

This item was submitted to Loughborough's Institutional Repository (<https://dspace.lboro.ac.uk/>) by the author and is made available under the following Creative Commons Licence conditions.



For the full text of this licence, please go to:
<http://creativecommons.org/licenses/by-nc-nd/2.5/>

Towards Internet Voting In the State of Qatar

By

Jassim Khalid AL-Hamar

A Doctoral Thesis

Submitted in partial fulfilments for the award of Doctor of Philosophy of
Loughborough University

2011

© Jassim Khalid AL-Hamar 2011

CERTIFICATE OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this thesis, that the original work is my own except as specified in acknowledgments or in footnotes, and that neither the thesis nor the original work contained therein has been submitted to this or any other institution for a degree.

..... (Signed)

..... (Date)

Abstract

Qatar is a small country in the Middle East which has used its oil wealth to invest in the country's infrastructure and education. The technology for Internet voting now exists or can be developed, but are the people of Qatar willing to take part in Internet voting for national elections?. This research identifies the willingness of government and citizens to introduce and participate in Internet voting (I-voting) in Qatar and the barriers that may be encountered when doing so. A secure I voting model for the Qatar government is then proposed that address issues of I-voting which might arise due to the introduction of such new technology. Recommendations are made for the Qatar government to assist in the introduction of I-voting.

The research identifies the feasibility of I-voting and the government's readiness and willingness to introduce it. Multiple factors are examined: the voting experience, educational development, telecommunication development, the large number of Internet users, Qatar law which does not bar the use of I-voting and Qatar culture which supports I-voting introduction. It is shown that there is a willingness amongst both the people and the government to introduce I-voting, and there is appropriate accessibility, availability of IT infrastructure, availability of Internet law to protect online consumers and the existence of the e government project. However, many Qataris have concerns of security, privacy, usability, transparency and other issues that would need to be addressed before any voting system could be considered to be a quality system in the eyes of the voters. Also, the need to consider the security threat associated on client-side machines is identified where a lack of user awareness on information security is an important factor.

The proposed model attempts to satisfy voting principles, introducing a secure platform for I-voting using best practices and solutions such as the smart card, Public Key Infrastructure (PKI) and digital certificates. The model was reviewed by a number of experts on Information Technology, and the Qatari culture and law who found that the system would, generally, satisfy voting principles, but pointed out the need to consider the scalability of the model, the possible cyber-attacks and the risks associated with voters' computers. which could be reduced by enhancing user awareness on security and using secure operating systems or Internet browsers. From these findings, a set of recommendations were proposed to encourage the government to introduce I-voting which consider different aspects of I-voting, including the digital divide, e-literacy, I voting infrastructure, legal aspects, transparency, security and privacy. These recommendations were also reviewed by experts who found them to be both valuable and effective.

Since literature on Internet voting in Qatar is sparse, empirical and non-empirical studies were carried out in a variety of surveys, interviews and experiments. The research successfully achieved its aim and objectives and is now being considered by the Qatari Government.

Key words

Internet voting, voting principles, transparency, anonymity, privacy, security, authentication, mix netting, blind signature.

Acknowledgements

After sincerely thanking Allah for all blessings and bounties, I would like to thank many people for their contribution, assistance, support and guidance during my PhD research. Special thanks are offered to my parents and family for their continuous encouragement along the joyful journey of knowledge which has brought this research to fruition.

I am also grateful to my home country of Qatar which is committed to education and the development of its people, and to my employer, the Ministry of Interior, for sponsoring my postgraduate education. I would like to thank my supervisors, Prof. Ray Dawson and Dr. Russell Lock, for their sustained support and valuable advice. I would like to thank as well everyone who has contributed and participated in this research including experts, participants and organisations who the authorisation and copyright clearance. Special thanks go as well to my wife for the support and encourage in difficult times.

Table of Contents

Chapter 1 Introduction	1
1.1 Background	1
1.2 Research Structure.....	2
1.3 Research Motivation.....	3
1.4 Research scope	5
1.5 Target Group	6
1.6 Research aim and objectives	7
1.7 Research Questions	9
1.8 Research contribution to knowledge	11
1.9 Originality of research contribution	12
1.10 Thesis structure.....	12
 Chapter 2 Background of voting	14
2.1 Introduction	14
2.2 Voters' characteristics	16
2.3 Voting systems	17
2.4 Election process.....	19
2.4.1 Absentee voting	21
2.5 Voting mechanisms	22
2.5.1 Paper ballots.....	22
2.5.2 Lever machines	24
2.5.3 Punched cards	24
2.5.4 Supervised electronic voting (E-voting)	25
2.5.5 Optical scan ballots.....	26
2.5.6 Direct Recording Electronic Systems (DREs).....	28
2.5.7 Internet voting (I-voting)	30
2.5.8 Conclusion on voting mechanisms	33
2.6 Summary	34
 Chapter 3 Literature Review and Current Systems Review.....	35
3.1 I-voting and e-commerce.....	35

3.2 I-voting experience	37
3.2.1 CyberVote project.....	43
3.2.2 Council of Europe's recommendation	44
3.3 Why move to I-voting?.....	45
3.3.1 Transformation to mobility	45
3.3.2 Transformation to automated system.....	46
3.3.3 Transformation to 'green' IT	47
3.4 Architecture of I-voting.....	49
3.4.1 Client-side attacks.....	52
3.4.1.1 Completely Automated Public Turing Test to Tell Computers and Humans Apart (Captcha).....	53
3.4.1.2 Code sheet voting.....	55
3.4.1.3 Clean Operating system and voting application.....	57
3.4.1.4 Special secure hardware for PC	57
3.4.1.5 Closed secure device	58
3.4.1.6 Secure PC operating systems	58
3.4.1.7 Test ballots	59
3.4.1.8 Obscurity/Complexity	60
3.4.1.9 External channel verification	61
3.4.1.10 Public bulletin board	62
3.4.1.11 Authentication	63
3.4.2 Internet-side attacks	64
3.4.2.1 Blind signature	66
3.4.2.2 Mix Networking (Mixnet).....	68
3.4.2.3 Homomorphic encryption	69
3.4.2.4 Other related cryptographic techniques	70
A. Public key infrastructure (PKI)	70
B. Certificate Authorities	71
C. Digital signature	71
3.4.2.5 Comparison of I-voting schemes	72
3.4.3 Server-side attacks	74
3.4.3.1 Server-related security issues	74
A. DoS attacks (indiscriminate or selective).....	75
A.1 DoS attack via bandwidth consumption.....	76

A.2 DoS attack via protocol attack	76
A.3 Denial of service attack via a logical attack.....	77
B. DNS attacks	77
C. Router attacks	77
D. No post-auditing.....	78
3.4.3.1.5 Insider attacks.....	79
3.4.4 Other implications.....	81
3.4.4.1 Legal issues	81
3.4.4.2 Transparency	85
3.4.4.3 Freedom	87
3.4.4.4 Equality	87
A. Digital and social divide.....	88
B. Usability	89
C. Accessibility	90
3.5 I-Voting Adoption	92
3.5.1 Trust of government and the Internet	94
3.6 Discussion	95
3.7 Conclusion.....	97
 Chapter 4: Research Methodology.....	99
4.1 Research Philosophy	99
4.1.1 Positivism	99
4.1.2 Interpretivism	100
4.1.3 Selection of Research Philosophy	100
4.2 Research approach	101
4.3 Research Design.....	103
4.4 Data Sampling Method	107
4.5 Research Process.....	108
4.6 Summary	110
 Chapter 5 Qatar Toward Internet voting.....	111
5.1 Background	111
5.2 Voting experience in Qatar.....	113
5.3 Corruption experience	115

5.4 Data collection method.....	116
5.5 Feasibility of I-voting in Qatar	118
5.6 Election procedure with or without I-voting	119
5.7 Qatar’s movement towards I-voting.....	120
5.7.1 Country size.	121
5.7.2 Economic development.....	121
5.7.3 Educational development.....	122
5.7.4 Technology development.....	123
5.7.5 The large number of Internet users	125
5.7.6 Transformation to e-commerce.....	126
5.7.7 Political	128
5.7.8 Election law	128
5.7.9 Culture	131
5.8 Barriers to I-voting	132
5.8.1 e-Law	132
5.8.2 Accessibility and Accuracy	133
5.8.3 Security, privacy and usability.....	134
5.9 Summary of expert interviews	135
5.10 Summary of candidate and voter interviews	138
5.11 Conclusion.....	139
 Chapter 6 Qataris’ Views on I-Voting	 140
6.1 Aim of survey	140
6.2 Survey design	140
6.3 Survey structure.....	142
6.4 Survey results and analysis.....	145
6.4.1 Demography.....	146
6.4.2 Willingness to participate in I-voting	148
6.4.3 Barriers to acceptance of I-voting.....	153
6.4.4 I-voting features	154
6.5 Analysis by respondents’ education	156
6.6 Chi-squared test	159
6.7 Conclusion.....	162

Chapter 7 Experimental Study: Comparison between Qatar and Estonia in Acceptance of I-voting	164
7.1 Experiment methodology	164
7.2 Experimental process	167
7.2.1 Plan and design	167
7.2.2 Test.....	169
7.2.3 Running the experiment.....	170
7.2.4 Analysis of results & discussion of findings	171
7.3 Reasons for the comparison with Estonia	172
7.4 Technical details	173
7.5 Results	177
7.6 Discussion of the results.....	183
7.3.1 Security of the theoretical approach	183
7.3.2 Election environment.....	184
7.3.3 Acceptance and trust.....	185
7.3.4 Usability and accessibility	185
7.3.5 Transparency.....	186
7.3.7 Quality	187
7.4 Conclusion.....	187
Chapter 8 Assessment of Client side I-voting Security	189
8.1 Introduction	189
8.2 Problem of awareness.....	191
8.4 Reasons for survey	193
8.5 Survey design	194
8.6 Analysis of Survey	195
8.6.1 Section 1. Background.....	195
8.6.1.1 Question 1. Gender.	195
8.6.1.2 Question 2. Age.....	195
8.6.1.3 Question 3. Education.	195
8.6.2 Section 2. Computer and Internet security.....	195
8.6.2.1 Question 1. Frequency of use of the Internet	196
8.6.2.2 Question 2. User reaction to a fake Internet security pop-up.....	196
8.6.2.3 Question 3. The best way for computer protection.	198

8.6.2.4 Question 4. Use of the same password.	199
8.6.2.5 Question 5. Remembering passwords.	199
8.6.2.6 Question 6. Method of choosing a password.	200
8.6.2.7 Question 7. Trustworthiness of a suspicious link.	202
8.6.2.8 Question 8. Use of P2P software.	203
8.6.2.9 Question 9. Checking file extensions before downloading.....	204
8.6.2.10 Question 10. Reaction to a warning of a virus attack that is imminent or on certain date.	205
8.6.2.11 Question 11. Opening e-mails from unknown senders	207
8.6.2.12 Question 12. Reaction to a firewall alert.....	208
8.6.2.13 Question 13. Switching off security applications in reaction to repeated alerts	209
8.6.2.14 Question 14. Responsibility for Internet security failure	210
8.6.3.1 Question 1. Training in IT security	211
8.6.3.2 Question 2. Computer security training for users	212
8.7 Conclusion.....	213
 Chapter 9 A proposed model for I-voting in Qatar	215
9.1 Introduction	215
9.2 Requirements of the Voting Process	216
9.2.1 Software requirements	217
9.3 The proposed model compared to the earlier experimental model	217
9.4 The Process of Voting	218
9.4.1 Introduction.....	218
9.4.2 Technical aspects of the system.....	219
9.4.2.1 Reception.....	223
9.4.2.2 Responding.....	223
9.4.2.3 Authentication and Authorisations.....	223
9.4.2.4 Audit trails.....	224
9.4.3 Authentication.....	225
9.4.4 Vote Registration	227
9.4.5 Anonymity preservation	228
9.4.6 Vote Casting	229
9.4.7 Vote Counting (Tallying).....	231

9.5 Prototype implementation of the model	231
9.5.1 Voting approach for secure I-voting architecture.....	231
9.5.1.1 Vote registration process for I-voting system.....	232
9.5.1.2 Vote on polling day by Internet	233
9.5.1.3 Counting ballot papers in I- voting architecture	234
9.5.2 Results and Discussion	235
9.6 Conclusion.....	238
 Chapter 10 Justification and evaluation	239
10.1 Introduction	239
10.2 Security assumptions and justifications	240
10.3 Justification of I-voting system based on the assumptions	243
10.3.1 Vote forgery	244
10.3.2 Voting by ineligible people.....	244
10.3.3 Multiple votes by eligiable voters.....	244
10.3.4 Large-scale exclusion of votes from a ballot.	245
10.4 How the requirements of I-voting are met by the proposed system.....	248
10.5 Evaluation.....	249
10.5.1 Expert evaluation on the proposed model design	249
10.5.2 Voter evaluation on the proposed model design.....	251
10.5.3 Expert Evaluation on the implementation of the proposed model.....	258
10.6 Summary of evaluation	260
10.7 Conclusion.....	261
 Chapter 11 Recommendations for introducing Internet voting in Qatar.....	263
11.1 Introduction	263
11.2 Recommendations	266
11.2.1 Recommendations 1: Reduction of Digital Divide in Qatar society	266
11.2.2 Recommendations 2. Enhance E-literacy in Qatar.	268
11.2.3 Recommendations 3. Enhance Internet Infrastructure Development	270
11.2.4 Recommendations 4. Provide laws to support I-voting	271
11.2.5 Recommendations 5. Ensure transparency of I-voting	272
11.2.6 Recommendations 6. Enhance the security and privacy of I-voting	273
11.3 Evaluation of Recommendations.....	275

11.4 Conclusion.....	280
Chapter 12 Conclusions and Future work.....	281
12.1 Research contributions.....	281
12.2 Research implications	281
12.3 Research achievements	282
12.4 Research limitations.....	282
12.5 Conclusion	283
12.6 Future work.....	286
1. Confirming research outcomes	286
2. Applying real trials.....	286
3. Establishing a research team	287
4. Investigating the cultural considerations of I-voting	287
5. Providing appropriate legislation	287
6. Assessing applicability of the proposed solution in other countries	288
12.7 Success of this PhD Research.....	288
Appendix A Interviews	289
A1 Consent Forms	289
A2 Example of signed consent Forms.....	290
A3 Interview questions.....	291
A4 Examples of interviews	292
Appendix B: Questionnaires	303
B1 Questionnaire 1: Exploring I-voting acceptance in Qatar	303
B1.1 First version of questionnaire.....	303
B1.2 Questionnaire after first review.....	306
Section 1 – Background.....	306
B1.3 Questionnaire final version (after pilot-test).....	309
Section 1 – Background.....	310
B1.4 Electronic version of questionnaire.....	313
B1.5 Questionnaire participants.....	313
B1.6 Questionnaire support	314
B1.7 Samples of completed questionnaire.....	316

B2 Questionnaire 2: Assessing client-side security awareness	322
B2.1 Questionnaire final version	322
B2.2 Sample of completed questionnaire	330
B2.3 Questionnaire results	335
Appendix C: I-voting Experiment.....	338
C1 Plan and Design	338
C2 Preparations	342
C3 Implementation	343
C4 Screenshots	346
C5 Unit Testing	349
C6 user manual	351
C7 Experiment evaluation	355
C7.1 Questionnaire first version	355
C7.2 Questionnaire final version	358
C7.2 Sample of completed Questionnaire	359
C7.3 Presentation of I-voting prototype	362
Appendix D: Proposed Model.....	364
D1 Requirements of the Voting Process	364
D2 Software requirement	367
D3 Presentation of the model	369
D4 Evaluation of the Model	380
D4.1 Questionnaire sheet.....	380
D4.2 Sample of completed questionnaire	382
D4.3 Questionnaire results.....	386
Appendix E: Recommendations.....	399
E1 Consent Form.....	399
E2 Example of signed Consent Form.....	400
E3 Recommendation evaluation.....	402
E4 Details of evaluator's interview.....	403
References	409

List of Figures

Figure 1.1 : Research General Structure	3
Figure 1.2: Thesis structure.....	13
Figure 2.1: Election Process (U.S General Accounting Office, 2004)	19
Figure 2.2: Lever voting machine displayed at National Museum of American History (RadioFan, 2010)	24
Figure 2.3: Precinct-Count and Central-Count Optical Scan Tabulator (United States General Accounting Office, 2004).....	27
Figure 2.4: DRE Push-button and DRE Touch screen (United States General Accounting Office, 2004)	29
Figure 3.1: I-voting basic requirements	49
Figure 3.2: Client-side malware attacks.....	52
Figure 3.3: Example of Captcha image Scantegrity (2008).....	54
Figure 3.4: Example of 3D captcha: Walking man attributes.....	55
Figure 3.5: Example of ballot and CodeCard	55
Figure 3.6: Improvement of code voting by using matrix table.....	56
Figure 3.7: Use of two channels (1) vote casting (2) vote verification.....	62
Figure 3.8: Internet-side malware attacks	64
Figure 3.9: Trial of ballot during decryption process	69
Figure 3.10: Server-side malware attack.....	74
Figure 4.1: Research process	109
Figure 6.1: Survey questions (Page 1)	143
Figure 6.2: Survey questions (Page 2)	144
Figure 6.3: Gender of respondents	146
Figure 6.4: Age of respondents	146
Figure 6.5: Final/current education level of respondents.....	147
Figure 6.6: Computer knowledge of respondents (Self-rated).....	147
Figure 6.7: Frequency of use of e-services	148
Figure 6.8: Confidence in elections in Qatar	149
Figure 6.9: Preference for I-voting.....	149
Figure 6.10: Voting method for citizens abroad	150
Figure 6.11: Comfortable feelings with I-voting	150

Figure 6.12: Confidence in privacy of I-voting	151
Figure 6.13: Ability to vote freely in I-voting.....	152
Figure 6.14: Confidence in security of I-voting.....	152
Figure 6.15: Reasons for not using Internet for e-services	153
Figure 6.16: Possible barriers for I-voting	154
Figure 6.17: Voter confirmation of candidate selected before vote recorded.....	155
Figure 6.18: Ability to revisit the voting website to confirm choice	155
Figure 6.19: Ability to verify votes through different channels such as SMS	155
Figure 7.1: Experimental process.....	167
Figure 8.1: IT security barriers, University of Minnesota (Kvavik, 2004)	191
Figure 8.2: Example of a fake Internet pop-up message.....	196
Figure 8.3: Perceived best way to protect computer	198
Figure 8.4: Remembering passwords	200
Figure 8.5: Methods used for choosing password.....	201
Figure 8.6: Suspicious link in instant messaging window	202
Figure 8.7: Respondents' thoughts on Instant Messaging window link	203
Figure 8. 8: Respondents using P2P software.....	204
Figure 8.9: Checking file extensions before downloading.....	205
Figure 8.10: Action on hearing about virus attack imminent or on certain date.....	206
Figure 8.11: Opening email from unknown sender	207
Figure 8.12: Example of Firewall alert	208
Figure 8.13: User behaviour on receiving firewall alerts.....	209
Figure 8.14: Turn off security application	210
Figure 8.15: Responsibility for Internet security failure.....	211
Figure 8.16: User training in IT security.....	212
Figure 8.17: IT security training for computer users	213
Figure 9.1: Qatar E-government roadmap	216
Figure 9.2: I-voting stages for the State of Qatar.....	218
Figure 9.3: Requests and response structure for I-voting	221
Figure 9.4: I-voting security engine architecture	222
Figure 9.5: Proposed IT Infrastructure for the central site for the I-voting.	224
Figure 9.6: Issuing a citizen card with personalisation.....	227
Figure 9.7: The process of issuing a Web certificate	229
Figure 9.8: Voter registration.....	232

Figure 9.9: Vote on polling day for voter	233
Figure 9.10: Example of voter registration using a web form	235
Figure 9.11: Example of letter	236
Figure 9.12: Identification on polling day	236
Figure 9.13: Example of candidates list.....	237
Figure 9.14: Example of outcome for counting the scores of the candidates list	237
Figure 10.1: Possible ways of large-scale vote rigging identified in the Estonian I-voting system. (EUDO, 2007; redraw by the researcher)	243
Figure 10.2: Do you agree that the Internet is safe and there are no legal issues concerned with I-voting?	252
Figure 10.3: Do you agree that you are comfortable with I-voting, that it is a good idea and that e-services are secure?	252
Figure 10.4: Would you agree to use I-voting with available support?	253
Figure 10.5: Do you agree to use your national ID, would you install software to vote and are you aware of phishing?	253
Figure 10.6: Would you agree to use biometric data to provide secure authentication for I-voting?	254
Figure 10.7: Do you agree that the proposed system is convenient?	254
Figure 10.8: Do you agree that the proposed system is easier, more secure than the existing system?	255
Figure 10.9: Do you agree that I-voting is desirable and beneficial for people?	255

List of Tables

Table 2.1: Comparison of voting methods against voting principles.....	23
Table 3.1: Global picture of I-voting experience	38
Table 3.2: Possible threats to I-voting	50
Table 3.3: Summary of possible computer attacks	53
Table 3.4: Comparison between blind signatures, mix-nets and homomorphic	65
Table 3.5: Comparison of schemes based on voting principles	72
Table 3.6: Possible security attacks associated with the server-side	75
Table 4.1: Three approaches to research (Iivari, 1991)	101
Table 4.2: Research design	103
Table 4.3: Relevant situations for different research strategies (from Yin, 1989).....	104
Table 4.4: Research design and research objectives	105
Table 4.5: Sampling methods.....	107
Table 5.1: Summary of expert interview responses	136
Table 6.1: Results by different education levels	156
Table 6.2: Factors constituting willingness and barriers towards I-voting	158
Table 6.3: Relationship between survey responses.....	160
Table 7.1: The technical details of Estonia experiment and Qatar case study	173
Table 7.2: Questionnaire results.....	177
Table 7.3: Comparison between Qatar and Estonia Results	179
Table 8.1: Views on computer crime and abuse (Furnell et al., 1999)	192
Table 9.1: Description of Requests and response for I-voting.....	221
Table 10.1: Fulfilling the I-voting requirements.....	248
Table 10.2: Summary of expert evaluation	250
Table 10.3: A summary of the voter evaluation.....	256
Table 10.4: Possible threats and solution of I-voting.....	261
Table 11.1: Summary of Outcomes and Implications of I-voting Research in Qatar...	264
Table 11.2: Recommendations 1 Reducing the digital divide	267
Table 11.3: Recommendations 2 E-literacy	269
Table 11.4: Recommendations 3. I-voting infrastructure	270
Table 11.5: Recommendations 4. I-voting law	271
Table 11.6: Recommendations 5. Transparency of I-voting.....	272
Table 11.7: Recommendations 6. Enhancing the security and privacy of I-voting	274

List of Publications

The following papers were produced during the course of this research project:

Al-Hamar, J., Al-Hamar, M. and Dawson, R.J., "Internet Voting in the State of Qatar: The People's Quality Requirements", Software Quality Management (SQM), Dawson, R.J., Ross, M. & Staples, G. (Eds.), Loughborough University, Proceedings of Software Quality Management XIX: Global Quality Issues, Loughborough, UK, April 2011, ISBN:978-1-907382-44-4.

Al-Hamar, M., Dawson, R.J and Al-Hamar, J., "The Threat of Phishing to Systems Quality in the State of Qatar", Software Quality Management (SQM), Dawson, R.J., Ross, M. & Staples, G. (Eds.), Loughborough University, Proceedings of Software Quality Management XIX: Global Quality Issues, Loughborough, UK, April 2011, ISBN:978-1-907382-44-4.

Al-Hamar, M., Dawson, R.J. and Al-Hamar, J., "The Need For Education on Phishing: A Survey Comparison of the UK and Qatar", International Process Improvement Research and Education (INSPIRE), Dawson, R.J., Uhomobhi, J., Ross, M. & Staples, G. (Eds.), Loughborough University, Proceedings of INSPIRE XVI: Educational Quality Issues, Loughborough, UK, April 2011, ISBN:978 1 907382-45-1.

Al-Hamar, J., "Business case study on Internet voting for the government of State of Qatar (Ministry of Interior), Doha, Qatar, Jan 2010.

Chapter 1 Introduction

This chapter sets the scene for this research project. The background to the problem area is described along with the motivation for the research. It defines the research scope, research questions, aim and objectives, contribution to knowledge and thesis structure.

1.1 Background

There has been an increasing demand around the world for replacing paper-based voting (Buchsbaum, 2004) with electronic-voting (e-voting) and several trials have been introduced (Aeby and Wiget, 2007; Buchsbaum, 2004; Krimmer et al, 2007). Internet-voting (I-voting) has attracted some debate on security vulnerability and large-scale fraud and most IT experts suggest the need to overcome these problems in the interest of ensuring accuracy and enhancing trust in such a voting system (Anane et al., 2007). The Netherlands is one of the countries which underwent a negative experience in e-voting and decided to stop in 2007, fearing that an intended secret vote may not be kept secret (Loeber, 2008).

Security requirements for e-voting and, in particular, I-voting have been defined as follows: (Cranor and Cytron, 1996, 2007; Nielsen et al., 2005):

Accuracy: to ensure accuracy of the system without interference or errors.

Democracy: to achieve democracy by allowing legal voters to vote only once.

Privacy: to keep all votes secret. No participant other than a voter should be able to determine the value of the vote cast by that voter. In other words, neither election authorities nor anyone else can link any ballot to the voter who cast it.

Verifiability: to provide individual and universal verification to ensure that votes are counted correctly.

Fairness: to ensure the system is available and accessible for all voters and free from possibility to declare results before the election closes.

According to Neumann (1993), availability, reliability, auditability, accountability and transparency were assigned as e-voting requirements by Cranor and Cytron (1996, 2007), and convenience, flexibility and usability were found to be crucial requirements for an e-voting system. In addition, I-voting has to meet political and legislation requirements (Council of Europe, 2004; Volkamer and McGaley, 2007).

1.2 Research Structure

The general research structure is shown in Figure 1.1. The thesis begins with an introduction which gives background information about voting, followed by an in-depth literature review of I-voting with an emphasis on examining the scope of the research based on I-voting experience and looking at filling the gaps in the literature and providing a contribution to knowledge. Subsequently, the research methodology is defined for achieving the research aim, including a review of the literature to illustrate the factors which make Qatar an appropriate place for introducing I-voting; surveys and interviews in Qatar to demonstrate the barriers for I-voting in Qatar in terms of technical aspects, government readiness and people's willingness and acceptance, along with defining the possible features of such technology.

Additionally, an experiment was undertaken to assess the feasibility and acceptance of I-voting in Qatar as a technical solution and for satisfying voters and election committees, through an effective prototype of I-voting developed according to Qatar's election requirements. Moreover, the results of the experiment were compared with a case study of Estonia, which shares many characteristics with Qatar (e.g. country size, readiness) to extract lessons from a successful I-voting experience. Accordingly, the findings are built on the research results, covering all aspects of the research and finally achieving the overall contribution of the research which is to define an effective framework for I-voting in Qatar to help the government in introducing such new technology in a general election. The framework involves formulating effective recommendations for the Qatar government and proposing an appropriate I-voting model for use in elections in Qatar. More details of the thesis are outlined in Section 1.8.

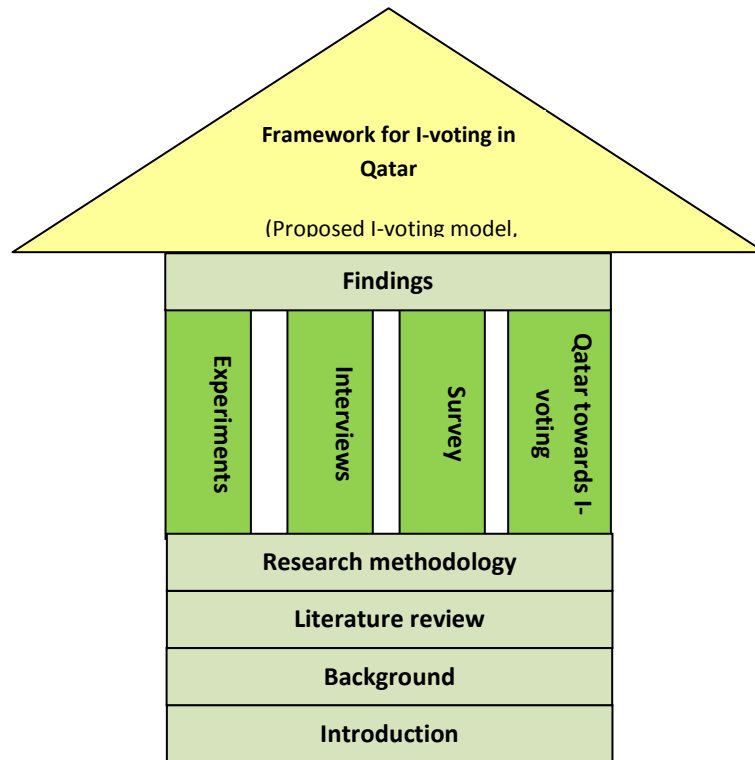


Figure 1.1 : Research General Structure

1.3 Research Motivation

Many democratic and modern countries have developed their own I-voting systems. These countries include the USA, Australia, Belgium, Brazil, Canada, Estonia, the European Union, France, Germany, India, Ireland, Italy, the Netherlands, Norway, Romania, Switzerland and the United Kingdom. The literature shows that I-voting was successful in many countries including developing nations, which made a start in such new technology (ACE, 2010).

The I-voting approach has been the subject of much research and it is clear that the experience of I-voting illustrates many advantages along with many concerns in terms of both technical and non-technical factors including security, privacy, transparency, social and the digital divide. Although many researchers focus on identifying solutions to I-voting concerns and on providing models and best practices, it is still a developing area of research (Jefferson et al., 2004). The experience of I-voting shows variations from one country to another, some show it to be positive and others negative in some

contexts. However, I-voting took different forms in each country, some proposed different I-voting models depending on the country-specific factors and requirements and consequently each presents different issues and shows varying willingness for I-voting (Boyd, 1990; Jan and Lin, 1995; Jan and Tai, 1995; Borrell and Rifa, 1996; Schneier, 1996; Fan and Lei, 1997; Abadi and Gordon, 1999; Adams, 1999; Kaldellis and Doumouliakas, 2000; Wu and Sankaranarayana, 2002; Meng, 2008; Purushothama and Pais, 2009).

This has motivated the researcher to further investigate I-voting and work on developing an effective I-voting model which satisfies essential voting principles and addresses the possible problems arising from I-voting. However, this would be hard to achieve since each country has its own requirements and characteristics and therefore implementing a standard model for all countries would be challenging. As a result, the researcher discovered an interesting case for research which is the State of Qatar for which there is a lack of literature on I-voting, which motivated him to shed light on one of the world's fast developing countries with a high GDP (QSA, 2008).

Qatar faces a rapid deployment in all sectors, including IT and democracy, especially since it is on the way to creating its parliament (Khalaf and Luciani, 2008). Furthermore, Qatar has developed e-government which could offer a usable IT infrastructure for I-voting (Al-shafi and Weerakkody, 2010). All of these factors provide an encouraging foundation for the introduction of I-voting in Qatar with the purpose of offering Qatari voters the possibility to vote over the Internet.

1.4 Research scope

This research focuses on eliminating the threats in introducing I-voting in general elections in Qatar. Since many challenges surround the adoption of I-voting, the research scope is narrowed to focus on designing a secure and effective I-voting model which satisfies Qatar's election requirements. The time constraint of PhD research has affected covering all the possible challenges (technical and non-technical), although the thesis provides a comprehensive solution for the State of Qatar government by analysing Qataris' willingness and government readiness and providing an effective I-voting model alongside recommendations for the Qatar government to assist in introducing such new technology in Qatar.

Although global solutions are essential to standardise I-voting, this research focuses only on the State of Qatar's requirement to motivate other countries to introduce I-voting. The research underlines the problem of introducing I-voting in the State of Qatar from both aspects of citizen and government, benefiting from experience in advanced countries, such as in Estonia, to introduce I-voting by taking advantage of Qatar's wealth and communications infrastructure without disregarding people's willingness to use such new technology.

The research also seeks to understand the factors which make I-voting successful in Qatar society and to propose a solution to the government to help in introducing I-voting through an effective framework consisting of an I-voting model along with a set of recommendations. Qatar was chosen as the case study for this research due to the convenience of access and the decision of the Qatar government to allow Qatari citizens to exercise their right to vote in parliamentary elections for the first time in 2012 (Tore, 2010). The lack of data on I-voting in Qatar makes it an original and interesting topic for investigation.

1.5 Target Group

The research will provide a contribution to scholarly research on I-voting. It addresses the challenges with cross-references to possible solutions to overcome obstacles, offers an effective model for I-voting and provides recommendations for the Qatar government to help in introducing I-voting in Qatar. It also provides an empirical study of I-voting adoption in the State of Qatar which has not been covered before in the literature.

Moreover, the findings of this research are intended to be of potential significance to a variety of groups such as:

1. Qatar government. The research focuses on identifying key elements which help in introducing I-voting and the importance of resolving problems. Also, a theoretical and practical solution along with a set of recommendations for the government with the main focus on providing technical solutions as a mean of eliminating I-voting threats. Moreover, other governments could benefit from the research outcome and the model proposed and the recommendations made in this research would be applicable elsewhere with certain variations, taking into account cultural and country-specific factors.
2. Qatar citizens. Since the problems associated with current voting methods affect all individuals, a solution for I-voting would be valuable for everyone, even those who do not have knowledge of using a computer and the Internet because the government would take the responsibility to educate people, which would help in enhancing computer literacy to benefit from an easy and convenient I-voting method.
3. Scientific goal. The research is expected to contribute to an enhanced understanding of what challenges are facing I-voting against the available solutions to establish comprehensive design theory and design methodology of an I-voting model, in order to improve I-voting development worldwide.

In addition, the research identifies the factors which make Qatar a suitable candidate for I-voting, including cultural, country-specific and other factors. This is a valuable outcome for all target groups which could be further studied. Although the discovered factors might be alike for other nations with certain variations, this would give clues as to what makes people in general willing to use such new technology which could therefore make I-voting more likely to succeed. The discovery of those factors would help to ease the introduction of I-voting and to develop effective I-voting solutions in both technical and non-technical aspects.

1.6 Research aim and objectives

The aim of this research is:

“To propose an effective Internet voting model for the State of Qatar to be used for future elections, taking into consideration technical and non-technical factors”.

Towards achieving the research aim, multiple objectives are required as follows:

1. To review the literature to determine the basic requirements for a democratic voting system and I-voting to support such a system and, hence, to form a set of criteria to act as a checklist to test the adequacy and acceptability of any existing or proposed system. Furthermore, to examine different ways of voting in a democratic environment and to assess each method using the criteria established to determine the strength of the case for using I-voting.
2. To review world-wide experience of adopting I-voting to highlight the successes and failures, and to address critical issues associated with their experience. Also, to review the literature to discover sociological and technical obstacles to adoption of such technology and to investigate potential solutions to overcome I-voting challenges.

3. To investigate and define the best practice research methodology to carry out this research.
4. To investigate the readiness of Qatar in terms of technical and non-technical aspects such as cultural, national and other country-related variables that might motivate the development or use of I-voting in Qatar by means of literature and interviews.
5. To assess, by means of a questionnaire and interviews, the confidence and willingness of Qatari citizens to take part in the initiative of I-voting, and to reveal the barriers that would inhibit I-voting in Qatar.
6. To further assess, by means of experiment, questionnaire, interviews and demonstrating a prototype of I-voting for Qatar elections, people's opinions and problems encountered while engaging in the voting process. Also, to test the effectiveness of the prototype solution in overcoming I-voting challenges and satisfying Qatar election requirements. Furthermore, to make a comparison between the Qatar experiment results and the experience of I-voting in Estonia to measure success or failure of the Qatar experiment in overcoming Estonia's problems.
7. To investigate the security risks that might appear due to lack of awareness of information security on the client side and to measure the level of awareness of Qatari people on the client side of I-voting in order to propose appropriate methods for solving the problem.
8. To design an effective I-voting model for the State of Qatar, by combining available technology and best practice to overcome I-voting challenges.

9. To test the applicability of the proposed model for overcoming the challenges of I-voting in the State of Qatar by means of simulation, experiments and expert opinion.
10. To propose, from the above findings, effective recommendations for the Qatar government to help in introducing I-voting in Qatar society

1.7 Research Questions

From the above aim and objectives, a number of research questions have been formulated for further investigation in this research, as shown in Table 1.1. These questions are answered in subsequent chapters as each of the main objectives are achieved.

Table 1.1: Research questions.

Objective number	Research Questions
1	<p>What are the different types of e-voting?</p> <p>What is the e-voting process?</p> <p>Can I-voting simplify the voting process?</p>
2	<p>What are the worldwide experiences of I-voting?</p> <p>What are the advantages and disadvantages of I-voting?</p> <p>What are the challenges to I-voting?</p> <p>What are the best practices and models or solutions proposed to meet the challenges of I-voting?</p> <p>Does I-voting comply with the current election law?</p>
3	<p>What are the research methodologies available to the researcher?</p> <p>What is the appropriate methodology for this research to achieve its aim and objectives?</p>

4	<p>Is the Qatar government prepared to introduce I-voting?</p> <p>Can I-voting be developed in Qatar using the available technology?</p> <p>How could I-voting be implemented successfully in Qatar while ensuring the fulfilment of voting principles?</p> <p>How could Qatar government take up and introduce I-voting?</p>
5	<p>Are the people of Qatar willing to take part in I-voting for national elections?</p> <p>What are the barriers to introducing I-voting in Qatar?</p> <p>What are the possible desirable features for I-voting?</p>
6	<p>Did the applied technology in the prototype overcome the challenges of I-voting?</p> <p>Did the Qatari people have the same level of acceptance of I-voting after using the prototype?</p> <p>What was the role of IT security and its management in I-voting?</p> <p>What are the real-world challenges for securing large-scale I-voting?</p> <p>What are the differences and similarities between the Qatar and Estonia case studies?</p>
7	<p>Does Qatar share the same problem of securing client machines?</p> <p>How far can this affect the voting process?</p> <p>Are the Qatar people aware of the need for securing of their computers and information?</p>

8	<p>What are the architecture and components of an I-voting model?</p> <p>What are the different types of protocol currently adopted?</p> <p>What are the international and industrial standards used for I-voting?</p> <p>How can smart cards and biometrics be used in I-voting?</p> <p>What anonymity protocols and standards are to be adopted?</p> <p>Will the proposed model gain acceptance of Qatari people?</p> <p>Does it meet the voting principles and accommodate Qatar's requirements?</p> <p>Was the model effective in the view of expert and public evaluation?</p>
9	<p>What are the technical measures taken to secure the I-voting?</p> <p>What is the software development methodology to be used for the implementation?</p> <p>Could a prototype application demonstrate sufficient security measures for I-voting using a smart card?</p> <p>Do the general security test, compliance test and performance evaluation results of the developed prototype validate a secure implementation of I-voting?</p>
10	<p>Was the proposed recommendation effective and feasible?</p> <p>Does it help the government of Qatar in introducing I-voting?</p>

1.8 Research contribution to knowledge

The contribution of this research is to develop a secure and effective I-voting model for the Qatar government as part of its e-government project, and also introduce the use of three factors of authentication for web application, which would encourage the use of this approach in applications such as Internet banking and e-government. It also measures willingness and acceptance regarding the introduction of such technology in

Qatar in terms of technology and sociology and proposes an effective I voting framework. This framework consists of an I-voting model that addresses the possible issues in I-voting and a set of recommendations to the Qatar government to help the uptake and introduction of I-voting in Qatar. It also provides a comparison of the Qatar experiment case study with the experience of Estonia with I-voting, looking for similarities and differences in each case. Furthermore, the research is beneficial to other researchers, as the lessons learned from the Qatari case study could be of use in introducing I-voting in other countries by considering the effectiveness of the developed model and recommendations proposed, taking account of the country-specific and cultural aspects of each country.

1.9 Originality of research contribution

The research is original since it sheds light on a part of the world that is largely ignored in the literature, the State of Qatar. This research fills the gap in the literature by exploring Qatar's possible move towards improving the current election system by adopting I-voting.

1.10 Thesis structure

This thesis consists of twelve chapters, as shown in Figure 1.2 below, beginning with an introduction to the thesis, giving background knowledge on the I-voting system, followed by a literature review of related work in the field of I-voting, reviewing the I-voting experience, advantages and disadvantages of I-voting along with the proposed models and solutions to overcome the problems in I-voting. A justification is then presented for the research methodology applied in this research towards achieving its objectives.

The following chapters assess the willingness to introduce I-voting in Qatar and people's acceptance of such technology, based on a review of I-voting in Qatar, surveys and experiments. Furthermore, an experiment is reported using an earlier version of I-voting to assess people's acceptance of such technology and provide a comparison of experimental outcomes with the case study of I-voting in Estonia.

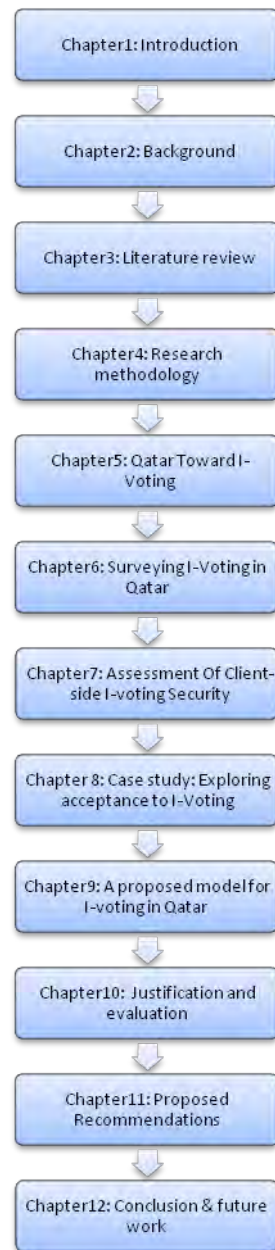


Figure 1.2: Thesis structure

Findings from the data collection reveals much willingness to embrace I-voting but also some barriers to I-voting in Qatar. This leads to the research contribution in proposing an I-voting model for Qatar to overcome the identified barriers, which was then assessed by a prototype I-voting system. Finally, recommendations are put forward to the Qatar government for the introduction of I-voting in Qatar. The thesis ends with a summary and proposals for future work.

Chapter 2 Background of voting

This chapter gives background information on voting, voters' characteristics and the types of voting systems. I-voting is introduced as a type of electronic voting.

2.1 Introduction

Voting is a process by which people express their opinions, commonly on selection of candidates or policies, and is a feature of a democracy (Dictionary.com, 2011). A healthy electoral system is one of the basic foundations of a free and democratic society as it acts as the main avenue by which the public exerts control over government, influences public policy decisions and holds officials accountable; although there are various signs which imply the unfavourable disposition of most voting systems across different countries (Amy, 2000).

The type of voting system which encompasses the overall voting process has often put stress on people. Frequently, voters face difficulty with registration and vote casting, and election officials and volunteers face a very strenuous process in vote counting (Amy, 2000).

According to Habermas (1989) (philosopher in the tradition of critical theory and pragmatism), an informed and engaged citizenry contributes greatly to improving a country's political process. When people participate more in the electoral process not only do they feel accountable for their political choices but it also adds further to the legitimisation of elections, hence mirroring a healthy democratic society (Kent, Harrison and Taylor, 2006). It is in this respect that Habermas noted that forces which can meaningfully contribute to the democratic society come from re-energised, activists and engaged groups who work together to create new small-scale communicative associative institutions (Shane, 2004).

Habermas claimed that decentralisation, which allows pluralistic decision making, comes from diverse societal groups, can pave the way to a healthy democratic electoral process. Decentralisation prevents the creation of mass loyalties normally brought forth by mass institutions such as political parties and states. According to Habermas, subgroups must break into smaller discourse communities which through elaborate interactions can create a discursive whole (Gibson, Nixon and Ward, 2003; Shane, 2004).

Habermas also claimed that civil society's role is very important as it creates a communicative power that influences political outcomes which are mainly about concepts of legitimacy. Practical discourse, according to him, is important to test the validity of norms that are being proposed and considered for adoption in the society (Shane, 2004). It is in this respect that it could be said that a society in which people live separately and maintain highly different views (i.e. anarchy) is a society which fails to legitimise its political, legal and government processes (Gibson et al., 2003; Shane, 2004).

Habermas's emphasis on the importance of discourse in legitimising the electoral process could be aided by other means which could further improve ways in which people collaborate with one another. According to Schwartz and Phoenix (2001), as cited by Shane (2004), technology will allow people a relatively easier process of discourse.

This section has shown the importance of voting in the democratic process and it is therefore important for people to engage with the voting process. This then provides the basic motivation for this research, as any improvement in the ease with which people can take part, together with an improvement in the security and reliability of the voting system can only help in legitimising the electoral system and, as a consequence, enhancing the democratic process.

2.2 Voters' characteristics

Theories on social choice have claimed that there are two types of voters: sincere and strategic. This categorisation capitalises on the value of the mental process in determining voters' decisions on who they should vote for. According to theories of social choice, sincere voters vote in accordance with their preferences, while strategic voters put much value on their voting strategies relative to the type and outcome of their calculations (Trechsel & Mendez, 2004; Kent et al., 2006).

Game theory is one of the branches of science which explains human decisions. According to game theory, there are four instances in which a voter can be constrained in making the right decision (Saco, 2002; Trechsel and Mendez, 2004;).

- 1) Procedural constraints. This refers to the difficulties encountered by people when they cast their votes, which are mostly procedural in nature. These constraints are often affected by the number of candidates competing for a particular situation in which voters are given various alternatives, which by virtue of their cognitive framework must be assessed and ranked. In voting situations, there are various constraints that voters have to face: the act of conducting, secretly or openly, the process of voting simultaneously, and the sequence or roll call decision (Trechsel and Mendez, 2004).
- 2) Information constraints. Voters find it difficult to decide who to vote for, or they consider it difficult to know if they are overloaded with information. Voters assess their preferences based on that information. In this case as well, voters can be categorised as having complete, partial or no information at all (Trechsel and Mendez, 2004).
- 3) Cooperation constraints. More informed and organised voters also face a lot of constraints, particularly when their decision lies on the binding agreements that they have within their group (Trechsel and Mendez, 2004). These types of voter have commitment to vote for whoever the party ask to vote for.

- 4) Compensation constraints. Money has always been involved in the decision of most voters. In some instances, voters among themselves offer compensation in exchange for support (Trechsel and Mendez, 2004)

All of the above constraints would act as barriers facing the voter while casting their votes. However, as the scope of this research is limited to the time and resource constraints of a PhD, only the barriers given in (1) will be considered to ensure the voters are provided with a voting system which is usable and satisfies the voters' needs.

2.3 Voting systems

Voting systems are important since there is a technical process which determines who is elected and eventually proclaims who runs the local, state and federal governments (Bimber and Davis, 2003). The people who are elected define the policies adopted and eventually determine who will benefit from them. Voting systems also determine the methods which can declare who among the candidates will win (Amy, 2000).

For instance, suppose Candidate A receives 42%, Candidate B 40% and Candidate C 18% of votes, respectively. Under Plurality Rules, Candidate A will win because he/she is the person with the most number of votes. However, if the voting framework only declares a winner by majority, Candidates A and B will be forced into a run-off in order to declare a winner with more than 50% of the votes (Amy, 2000; Gibson, Nixon and Ward, 2003).

A voting system is made up of procedures which people follow to elect their chosen candidate to a particular office. In this system, this includes the process by which the ballot is structured, together with the manner in which people cast their votes and this determines which candidate will win (Amy, 2000; Bimber and Davis, 2003).

There are two main systems in the voting system paradigm adopted by democratic countries in the West. The first is the *single-member district plurality system* in which votes are cast in single-member districts in which only one candidate for the legislative seat will be elected (Bimber and Davis, 2003). There are two structures of the ballot:

- 1) Simple, includes basically the list of all candidates from whom the voter will only have to choose one.
- 2) Complex, in which the voter ranks the candidates in order of preference.

On the other hand, the *proportional representation system* (PR) is the method adopted by most countries in the European region e.g. Austria, Belgium and Germany. This method is more elaborate as it uses different ballots and ways of vote computation (Amy, 2000). However, it must be noted that all PR systems share a common variable: they allow candidate election in multi-member districts (Bimber and Davis, 2003).

In addition, rather than having one member of the legislature elected in a small district, PR uses larger districts wherein more than one member is elected (Amy, 2000). Also, multiple seats are distributed in accordance with the proportion of votes won by a particular party or political group.

The voting system passes through phases, starting with preparation and registration, where eligible voters register, prove their identity, then authenticate themselves before proceeding to vote, where their votes are then cast and the results are calculated and published.

This implies that the more complicated voting systems require more time, firstly to carry out the voting process and, secondly, to calculate the result. The power of computer processing in electronic voting may make the system quicker and therefore more viable. However, the complications would increase the need for transparency as people would need to know how their vote had been handled (*e.g. Single transferable vote (STV) is a voting system based on proportional representation and preferential voting*). This section has therefore provided a motivation to research the potential of

electronic voting, but it has also established that the voting process, whether by electronic or other means, must be transparent in its operation.

2.4 Election process

Voting systems are one of many important components of the overall election process (Gibson, Nixon and Ward, 2003; United States General Accounting Office, 2004). Thus there should be an integration and cooperation between parties, including institutes, researchers and politicians in charge of the introduction of I-voting.

The entire paradigm is actually composed of several stages which are made up of people, process and other technological variables. Figure 2.1 shows the entire election process.

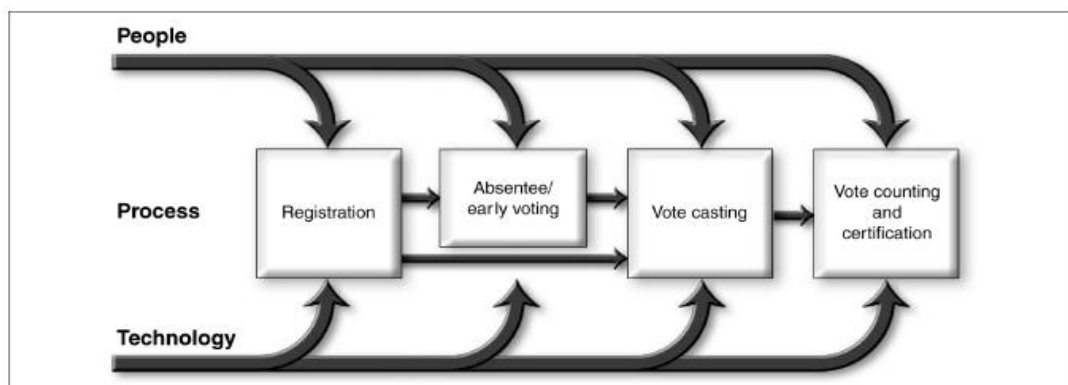


Figure 2.1: Election Process (U.S General Accounting Office, 2004)

The stages of elections are normally comprised of:

(1) *Voter registration*. Local election of officials requires voters to be registered and included in the official list of registered voters. In addition, their corresponding information must be presented, e.g. ID card or passport. A list of voters no longer eligible to vote must be maintained on a separate database (United States General Accounting Office, 2004). This implies that any new system must take into account the need for completeness, all eligible people must be allowed to vote, and uniqueness, each eligible person must only be allowed to enter his/her vote once.

(2) *Absentee and early voting.* For some people who have legitimate reasons such as illness, religious or educational commitment that prevents them from attending the polling station, voting must be allowed either in person or by mail before the actual day of the election. Voters who have legitimate reasons such as illness, religious or educational commitment that prevents them from attending a polling station would normally find mail voting a suitable option to cast their votes.

(3) *Choice of voting mechanisms.* Prior to vote casting, election officials must design ballots and other systems to allow that electorate to vote (United States General Accounting Office, 2004). This is required for completeness to ensure this group of voters is able to vote. However, it complicates the voting process and must therefore be considered when choosing the voting mechanisms that will be provided in an election. The ways of conducting absentee voting are examined in more detail in the next section.

(4) *Conduct of election/ Vote casting.* Election administration must be fully prepared before the Election Day. Polling places, recruiting and training of poll workers, designing of ballots, preparing and testing of voting equipment for use in casting and tabulating votes, together with the preparation of election day activities like opening and closing of polling places must be all specified (United States General Accounting Office, 2004). This level of care is to ensure the system is both robust and reliable. Officials will also need to be aware of procedures to ensure the privacy and anonymity of each individual's vote.

(5) *Vote counting.* Finally, the process of how to tabulate and count the ballots must be fully defined, together with those unable to be read by the voting equipment. A process of final votes' certification must also be established and any process of recounting must be laid down prior to the elections (United States General Accounting Office, 2004). This implies that the method of counting the votes and calculating the winner must not only be accurate and reliable, but it must also be seen to be accurate and reliable by allowing for recounts if required.

2.4.1 Absentee voting

Absentee voting is used for voters who can not attend the polling place for various reasons (unable or unwilling). Many countries have adopted this type of voting to suit the new life style of voters and to increase voter participation by providing a more flexible means of voting. Absentee votes are delivered using three methods, as follows:

(1) *Postal voting*. A voter would need to request this type of voting in advance, then the election council would send a referenced voting form to be filled in by the voter and sent back before the actual election according to country election law. However, this type of vote has experienced problems in the United Kingdom where voting anonymity, secrecy and delivery of the voting papers to the correct person could not be guaranteed (Isobel W, 2009).

(2) *Proxy voting*. Again, a voter would need to request this type of voting in advance. A proxy vote requires the voter to notify the election authorities of a trusted person who will vote on his/her behalf.

(3) *Internet voting*. A voter can cast his/her vote using the Internet network which is very cheap to access for voters and would be cheaper to administrate compared to postal and proxy voting. It would add the flexibility to vote at any time, anywhere, as long as it is within the defined election period. Furthermore, I-voting would have the beneficial side effect of pushing the government and organisations to use state of the art technology, such as smart cards, which could be used with a range of different applications. The one-off cost of the card would then benefit a range of security areas of concern.

Absentee voting can provide the ability for some voters to vote who would not otherwise be able to do so and would therefore increase voters' participation. However, the voters might lose secrecy as the lack of any supervision of the voting could mean they may be subject to pressure from others to vote for a particular candidate. With absentee voting in the form of postal voting, voters must vote in advance since the postal service takes time for delivery.

In 1956, absentee voting was introduced in Germany (Eckhard Jesse 2003) where voters met specific criteria with an acceptable reason for not being able to vote in a polling station, such as illness, age or disability. Still, absentee voting remains exceptional. In Germany in 1957, only 4.9% used absentee voting though this increased to 13% in 1980. In the 2002 election, a high percentage of voters (one in every five eligible voters) used absentee voting (Norbert Kersting 2004).

This shows that, over the years, absentee voting has become more popular with changes in life style, indicating that people would like to have the flexibility and convenience to vote remotely at any time. They may therefore be willing to turn to I-voting as a convenient and innovative method of voting that will fulfil this growing need.

I-voting could be considered as the best method of absentee voting in terms of flexibility, security and cost of setting up the election. However, many people currently regard I-voting as an insecure system, but on the other hand, technology is moving very fast and should soon provide a secure environment for I-voting.

2.5 Voting mechanisms

The ways of administering elections may vary with the voting system adopted by different countries and even in different elections within one country. Therefore various equipment has been developed by respective countries to cater for their voting needs. There are a few variables such as budget, culture and tradition, which would affect countries' choices of a particular voting technology (Shane, 2004).

2.5.1 Paper ballots

Ways in which people have voted throughout the years have changed from verbal expressions to the placement of small balls in a box to the use of paper ballots. Paper ballots were used during the mid-nineteenth century where voters were able to write the name of their chosen candidates on a piece of paper or use a pre-printed ticket from a political party where they just simply signed their names. Voters would then deposit their ballots in a designated area for counting (Bimber and Davis, 2003; Yang and Gaines, 2004).

Table 2.1: Comparison of voting methods against voting principles

	Paper Ballot	Lever Machines	Punch cards	Optical Scan	DRE	Mail voting	Proxy voting	I-voting
Eligibility	+	+	+	+	+	+	+	+
Privacy	Partly	+	+	Not for the disabled	Partly	-	Partly	Conditionally
Receipt-Freeness	+	+	+	+	+	+	+	+
Fairness	+	+	+	+	+	+	+	+
Accuracy	Partly	+	Partly	+	Partly	-	+	+
Individual Verifiability	-	-	+	+	-	-	+	+
Universal Verifiability	+	-	+	+	+	+	+	+
Reliability	+	+	+	+	+	-	+	+
Convenience	Partly	Partly	Can be ambiguous	+	Partly	+	+	+
Flexibility of the usability	+	Partly	Partly	-	+	+	+	+
Mobility	-	-	-	-	-	+	+	+
Transparency	+	-	+	+	Partly	+	+	Partly
Scalability	+	+	+	+	+	+	+	+
Efficiency	Partly	Partly	Low	+	+	-	+	+
Security	+	+	+	+	+	-	+	Conditionally
Cost effective	-	+	+	-	+	+	-	+

The paper ballot form of voting could be strenuous process for some voters, particularly during vote casting and counting. Illegible writing, the incapacity of voters to choose outside a certain party and lack of voting anonymity were a few of its main issues (Gibson, Nixon and Ward, 2003; Lock et al., 2007). To reduce the problems, the USA Government has standardised and printed ballots since the late 1800s. However, scandals and improper vote counting continued and this eventually mandated most USA states to abandon paper ballots (Yang and Gaines, 2004).

2.5.2 Lever machines

The lever machine is one of the earliest forms of mechanical voting which requires voters to pull selected levers assigned to their preferred candidate (See Figure 2.2). After each voter has made his/her choice, the levers return to their original position, while the internal counter in the machine advances immediately to record the vote (Gibson, Nixon and Ward, 2003; Yang and Gaines, 2004).



Figure 2.2: Lever voting machine displayed at National Museum of American History (RadioFan, 2010)

After the polls, the total number of votes for a particular candidate is produced by the machine. However, since lever machines do not produce a record of each individual vote, a recount would be impossible. Furthermore, lever machines are prone to breakdowns and tampering. As a result, lever machines are no longer manufactured and are in the process of being phased out in most countries which used them (Kent, Harrison and Taylor, 2006; Yang and Gaines, 2004).

2.5.3 Punched cards

Punched cards were used during the US Presidential elections in 2000. With punched cards, the voter inserts a card into a machine under a ballot label, then uses a stylus to punch through the space assigned for the preferred candidate, hence removing a 'chad' or the rectangular shape from the card (Saco, 2002; Yang and Gaines, 2004).

After this, a computerised tabulating device counts each result as represented by the hole. Through this process, vote counting speed is increased and recounts have become

possible and relatively easier (Bimber and Davis, 2003). However, various problems in using the punched card have been noted in several elections, particularly in the 2000 presidential elections in Florida. For instance, some voters did not punch their cards cleanly enough, hence preventing the machine's reading. As a result, the US Congress encouraged the phasing-out of punched card machines by 2006 (Yang and Gaines, 2004). These have generally been replaced by new voting technologies such as E-voting and I-voting (Kent et al, 2006).

2.5.4 Supervised electronic voting (E-voting)

There are generally two types of supervised E-voting systems adopted by modern countries in the West, such as the United States: optical scan and direct recording electronic (DRE). Other than this, there are also a few other, relatively older voting technologies, as used in the 2000 US elections: punched card and mechanical lever voting (United States General Accounting Office, 2004; Gibson, Nixon and Ward, 2003).

E-voting is an encompassing term referring to technologies adopted by countries all over the world which use advanced technologies as the core of the entire voting process. E-voting makes use of technologies from the basic punched cards up to the most advanced DRE systems and optical scan (Bimber & Davis, 2003). On the other hand, unsupervised I-voting makes use of a broad range of electronic telecommunication technology in which telephones, cables, satellite television and computers serve as the means by which citizens can cast their votes. Unlike E-voting, which requires citizens to vote in specific and designated areas of voting using stand-alone machines, I-voting allows citizens to vote using almost any means of technology made available: personal computer, mobile phone and even television sets (Trechsel & Mendez, 2004).

Increased voter participation is one of the primary arguments promoting the use of E-voting and I-voting. For instance, parliamentary elections across Western Europe, ever since the 1990s, have shown a downward trend in voters going to the polls (Bimber and Davis, 2003). Across the Atlantic, attention is also drawn to the problem of absence

from participating in election (Gibson, Nixon and Ward, 2003; Trechsel and Mendez, 2004).

In 1968, seven per cent of voters in the United States did not cast their votes and over time this figure had tripled by the year 2000. Low voter turnout among younger voters was also noted. In the US Presidential elections in 2000, only 36 per cent of those aged 18 to 24 participated (Kent, Harrison and Taylor, 2006). The same fate was experienced in the British General Election in 2001 in which voter turn-out dropped to its lowest levels since 1918, in which over 60% of voters aged between 18 to 24 did not vote (Gibson, Nixon and Ward, 2003; Trechsel and Mendez, 2004). Some countries counter this by making voting compulsory, e.g. Australia (Mackerras and McAllister, 1999).

Optical Scan and Direct Recording Electronic are two types of E-voting systems. However, E-voting can also be considered to include I-voting, for which Internet Voting at the Polling Place and Remote Internet Voting are the two main types (Kent et al, 2006). Each type of E-voting is considered as follows:

2.5.5 Optical scan ballots

The Optical Scan System is a technology developed almost three decades ago for scoring standardised tests. It was not until 2000 that this technology was used in US elections to tabulate paper ballots (United States General Accounting Office, 2004; Bimber & Davis, 2003). The optical scan system is made up of computer-readable ballots, marking devices, privacy booths and a computerised tabulation device (Bimber & Davis, 2003; United States General Accounting Office, 2004).

The ballot is designed so that it is capable of adjusting itself to various sizes, listing the names of the candidates and the like. During elections, voters record their choices by using an appropriate writing instrument to fill in boxes or ovals or in some cases put arrows indicating their choice of a particular candidate. This technology also allows a space for write-ins to be placed directly on the ballot (Kent et al, 2006; United States General Accounting Office, 2004).

Optical scan ballots work by having state of the art optical-mark-recognition equipment read ballots by sensing or reading the marks on ballot papers. Counting is then carried out either by a precinct-count optical scan or at a central location (Kent et al, 2006). For ballots counted at the polling place, voters or election officials put them inside tabulation equipment in which the votes are tallied. These tallies are captured in removable storage devices which are then transported to a central tally location or electronically transmitted to it from the polling place (United States General Accounting Office, 2004).

For ballots that are centrally counted, voters drop their ballots in sealed boxes and, eventually, election officials transfer these to the central location after polling for a particular area has been completed (Bimber and Davis, 2003; United States General Accounting Office, 2004). Figure 2.3 shows the optical scan ballot technology.

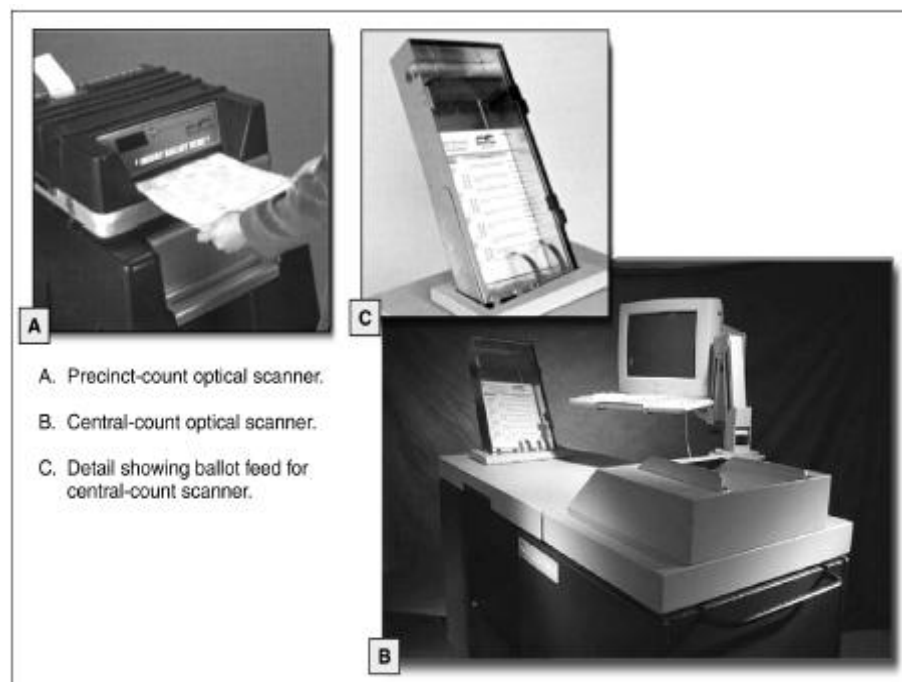


Figure 2.3: Precinct-Count and Central-Count Optical Scan Tabulator (United States General Accounting Office, 2004)

This technology instructs the tabulation equipment to assign each valid mark on the ballot to the chosen candidate. Such technology also allows the identification of

particular contests and candidates and configuration to capture a straight party voting and votes strictly to a particular number of contests. Over-votes (e.g. voting for two candidates where there should be one) and under-votes (e.g. voting for one candidate where should be more than one) can also be identified by using precinct-based optical scanners; in addition, a specific response can be provided for the two scenarios mentioned (Bimber and Davis, 2003; United States General Accounting Office, 2004).

Furthermore, this technology allows the use of vote-tally software which can count the votes from one or more tabulation devices. The benefit of this is also the immediate notification provided by the computer if an over-vote or under-vote occurs, hence allowing voters to fix their choices prior to leaving the polling place (Bimber and Davis, 2003). In instances where voters are unwilling or unable to correct their ballots, a poll worker can manually override the program and accept the ballot. Where ballots are to be tabulated centrally, mistakes cannot be corrected by voters. Clearly over-voting and under-voting affect the accuracy of a voting (Bimber and Davis, 2003; United States General Accounting Office, 2004). Alternatively, I-voting would overcome such a problem by minimising the number of people having direct access to the equipment.

2.5.6 Direct Recording Electronic Systems (DREs)

A DRE is a voting technology which captures votes without the use of paper ballots, but rather tallies them in an electronic manner. It was introduced in the 1970s and used in the 2000 US elections by almost 12 per cent of voters (United States General Accounting Office, 2004; Bimber and Davis, 2003).

Push-button DRE is a relatively older technology, somewhat larger and heavier than the touch screen. It also presents ballots in a full-face interface (where all choices are on one page) which, for instance, could have 50 buttons on a three by three foot ballot, with a candidate represented by each button (Gibson et al., 2003; United States General Accounting Office, 2004).

A touch screen DRE displays ballot information in colour and can also present pictures of the candidates. In addition, since the space on a touch screen ballot is relatively smaller than the push-button machine, voters who use this technology can navigate throughout the ballot information. Both touch screen and push-button DREs can also accommodate multilingual ballots (Kent, Harrison and Taylor, 2006; United States General Accounting Office, 2004). It should be noted though that push-button and touch screen ballot information is connected to electronic storage which eventually updates a central database with the votes cast (United States General Accounting Office, 2004). Figure 2.4 shows both the push-button and touch screen DRE.

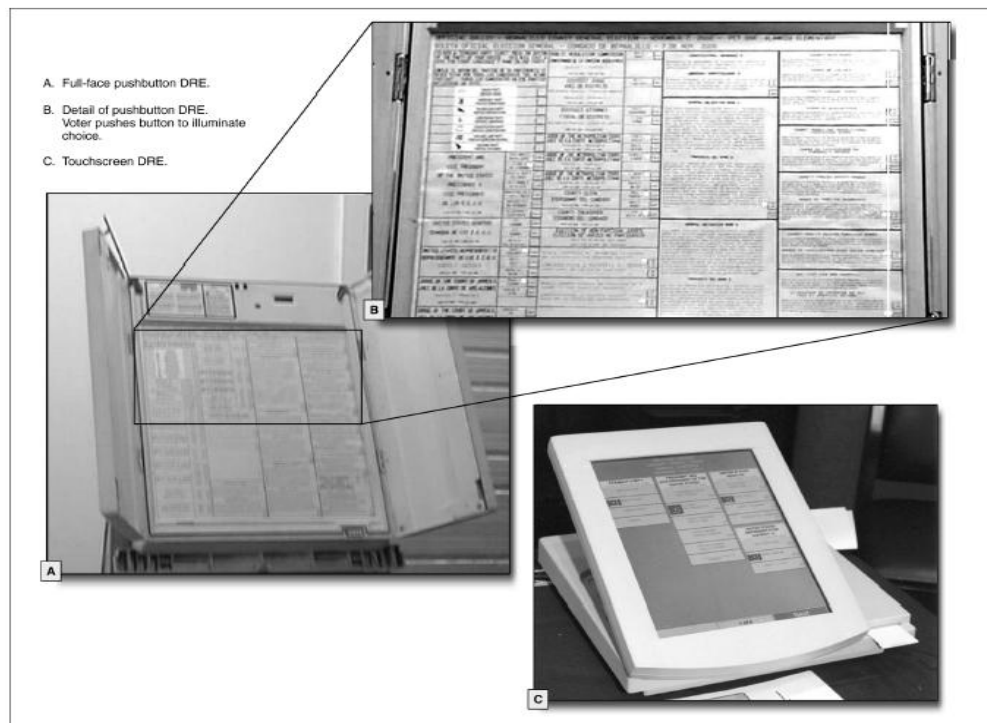


Figure 2.4: DRE Push-button and DRE Touch screen (United States General Accounting Office, 2004)

2.5.7 Internet voting (I-voting)

I-voting is a sub-type of electronic voting where votes are cast in a secure and secret electronic ballot and transmitted to the officials over the Internet. I-voting is therefore a technology which works through a broad range of electronic telecommunications technology using telephones, cables, satellite television and computers (Trechsel and Mendez, 2004; Kent et al., 2006;).

The Internet radically empowers people and creates new tools which allow people to communicate with one another and share their interests regardless of any distance barriers (Shane, 2004; Kent, Harrison and Taylor, 2006). The Internet also plays a big role in providing new links between the citizens and government where the government has initiated projects such as e-government, e-participation and e-democracy to increase participation in an effective, transparent, democratic system. According to Habermas (1964), the Internet, in its provision of new media for communication, draws power back to the public sphere and away from bureaucratic government systems. In addition, the Internet creates new virtual spaces where people can visit and express their opinions and this helps to “*guarantee freedom of assembly and association and the freedom to express and publish their opinions*” (Habermas, 1964, quoted in Pusey, 1987: 89). The use of democratised access to a new form of mass media allows more room for self-expression and makes people engage more in debate, which has created new forms of communities of discourse (Shane, 2004; Bimber and Davis, 2003).

The use of the latest hardware and software technologies, such as smart cards, biometrics and PKI (Public Key Infrastructure) allows easy information exchange which fosters discourse in healthy debates and arguments. As the base of Internet users increases, the utilities brought forth widen further. In addition, discourse-enabling tools are being developed and barriers such as cost, low computer literacy, lack of trust and unwillingness to use such technology that formerly hindered people from collaborating by electronic means are now being resolved (Kent, Harrison and Taylor, 2006). This increasing use of the Internet for communication and discourse means that the Internet is becoming more acceptable as a means of carrying out business and for interacting with government. A natural progression of this, therefore, is for citizens to accept the

Internet as a means to facilitate the most basic aspect of a democracy, the right to vote.

The practice of I-voting is less common compared to optical scan systems and DREs, in part because the Internet is a relatively recent phenomenon. In fact, one of the earliest political uses of this technology can be dated as recently as 1996, when the US Reform Party made its members cast a vote for their chosen president through their computers (Gibson, Nixon and Ward, 2003).

The first use of I-voting on a large scale and in a legally binding manner was by the Arizona Democrats in March 2000 (Trechsel and Mendez, 2004; Kent et al., 2006). The Republican Party of the USA also used I-voting in Alaska for the 2000 elections; however, the results were disappointing as only 35 votes were made online, less than one per cent of the eligible voters in the area.

The use of I-voting by the State of Arizona has stimulated interest of other countries all over the world to adopt I-voting. In fact, the Electoral Commission in the United Kingdom, together with the company responsible for the Arizona elections, and British Telecom, piloted a number of I-voting systems for 12 local elections (Bedford, Breckland, Broxbourne, Dover, Gateshead, Rushmoor, Sheffield, Shrewsbury and Atcham, South Bucks, Stratford-on-Avon and Warwick (joint pilot), Sunderland, and Swindon) between 2002 and 2007. This initiative allowed the use of interactive digital television, SMS by mobile phones, home personal computers and Internet-connected public kiosks in libraries and supermarkets (Saco, 2002; Trechsel and Mendez, 2004).

The result, of those trials shows a good degree of success, however the trial was held on a small-scale, which does not reflect the real threats of national elections. Moreover, some people found difficulties to cast their vote due to lack of standardisation in defining the election process.

As I-voting enables voters to cast their choices at any machine connected to the Internet, voters can log-on to an election website from their personal computers at home, work,

through their digital television or even mobile phone. Computers made available in other public areas such as post offices, libraries and shopping malls could also be used (Trechsel and Mendez, 2004).

According to Internet Policy Institute (2001), I-voting systems are categorised according to the siting of the voting terminals (Trechsel and Mendez, 2004; Kent et al., 2006).

(1) *Poll site*. The E-voting system is in a polling station in a safe, supervised environment. If implemented, it would replace existing voting equipment such as paper ballots or punched cards (Saco, 2002).

(2) *Kiosk*. The unsupervised E-voting system is located in specific locations such as shopping centre or libraries similar to ATM machines. However, such a system was found to be easily hacked if physical access to the machine is obtained even though it is protected and configured against security issues (Masnick, 2005). I-voting might suffer from hacker attacks targeting the weakest link, voters' computers, especially insecure ones.

(3) *Remote Internet Voting (RIV)*. This is a system where voters are allowed to vote online and remotely from any digital device connected to a network or to the Internet. It could be conducted from PCs, mobile phones, games machines and other technologies which can access the Internet. This requires less effort and cost from the authorities and provides more flexibility for voters to cast their vote.

2.5.8 Conclusion on voting mechanisms

This section has examined the different voting mechanisms used in government and other elections. Each of the methods has been shown to have its problems. Paper voting is labour intensive and is prone to some human error. It also means that voting remotely is only possible by using the postal service, which necessitates voting in advance. Lever machines work well for those present but the way they work means that any form of recount is impossible. Punched cards have some reliability problems when the holes are not punched properly, as was highlighted in the US Presidential election of 2000.

Electronic voting appears to be a step forward in that it eliminates human error in the counting process. However, optical scan ballots still involve paper and suffer from most of the disadvantages of paper ballots and neither this method nor the direct recording electronic systems enable absentee voting. I-voting is perhaps the mechanism that shows the most potential, but as the Internet is relatively new, its security is not as well tried and tested and it is uncertain whether the majority of the public will have the confidence to use it. However, the growing use of the Internet by the public for communication and business indicates that citizens may be coming to the point where they will use it for voting if the right conditions of security and transparency are provided.

2.6 Summary

This chapter gives background information about voting beginning with the importance of voting in a democracy. From this it was concluded that any voting system needs to satisfy citizens' requirements of being easy to use, secure and reliable in order to encourage the maximum number of people to take part in the voting process.

The chapter then examined the election process from voter registration, absentee and early voting to vote casting and vote counting. This showed it is a complicated process requiring expertise from different fields. Further characteristics of a good voting system were revealed: the system should be transparent in its operation; it must be complete so that it enables all people to vote but also offers uniqueness so that a person cannot vote more than once; it must allow absentee voting in a manner that is convenient, but also gives privacy; it must be robust as well as reliable; it must ensure privacy and anonymity for voters; it must be accurate and allow for recounts if required; and it should inspire confidence in the users that their vote is secure and properly handled. Ideally, the system should also be inexpensive and fast in calculating the winner.

The mechanisms for voting systems were then examined from the traditional paper ballot voting to advanced forms of electronic voting. All mechanisms of voting have some advantages and disadvantages, but the future technology of I-voting, which allows voters to vote remotely from their PCs through a secure channel, appears to offer the most promise if it can be made to satisfy all voters' requirements identified above.

The next chapter presents the literature review on the subject of I-voting, identifying the barriers to the implementation of such a system, the willingness of people to accept it and the experience of others who have introduced I-voting. This leads to specification of the research scope based on the gap identified in the literature in this area of research.

Chapter 3 Literature Review and Current Systems Review

This chapter summarises world-wide experience of I-voting, pointing to the successes and failures of such a system. Furthermore, it identifies the problems arising from I-voting and its introduction and the available potential solutions, models and schemes to overcome them. The literature review satisfies objective 2 of the research and assists in defining the research scope, aiming to add a contribution to knowledge and filling the gap in existing literature by shedding light on introducing I-voting in a country so far ignored in the literature, the State of Qatar. In the belief that I-voting could be introduced in Qatar, by designing the best of all I-voting models, it takes into consideration the relative I-voting experience around the world and the country-specific factors.

3.1 I-voting and e-commerce

For Internet voting (I-voting) and electronic commerce (e-commerce), some of the threats or characteristics might be similar. In this section, the researcher examines this possibility and argues that the similarity is more real than apparent. As a consequence, it will be necessary to explore novel means to support I-voting.

Jefferson et al. (2004) argued that it is important for people to understand the differences between I-voting and e-commerce in order to avoid possible attacks.

Elections are a link to democracy and any problem in the voting process would affect democracy. Therefore I-voting needs as high a level of security, if not higher, than e-commerce. In I-voting, the right to vote should not be handed over or sold (Jefferson et al., 2004). An occurrence of a denial of service (DoS) attack would cause consequent loss of confidence in the system since, if the election web server went down due to the huge volume of traffic, it would prevent voters from casting their vote. This could compromise the legitimacy of the whole election. Moreover, it is hard to protect against such an attack (Regenscheid and Hastings, 2008) and also difficult to recover votes since, as voting should be anonymous, no receipts are produced. This should be compared to e-commerce, where costs could be recovered through repayment and legal

actions. Moreover, offers of receipts after the commitment to I-voting might enable vote selling or pressure (Jefferson et al., 2004). Nevertheless, the story of successful e-commerce does not essentially make an I-voting system secure (Fairweather and Rogerson, 2005).

Some researchers anticipate the success and large-scale use of I-voting, as has happened for e-commerce. However, Ronald (2002) commented that the feasibility of e-commerce does not necessarily imply the feasibility of the I-voting since there are several different issues between the two, as explained in detail below (Jefferson et al., 2004; Schryen, 2004). In financial transactions, online and offline processes are provided, which might be referred for auditing, whereas in I-voting, it should be easy to do a recount but impossible to trace votes to individual voters. Moreover, in e-commerce there is the opportunity to dispute the transaction, whereas in I-voting, although this is possible, it requires many court appearances, yet the time for voting is limited. In e-commerce, the customer's identity is available, whereas in I-voting the case is different as the voter's identity must be anonymous and kept private. However, this might be subject to limitation. Even the characteristics of attackers are different: attackers of I-voting are more intelligent, can alter votes without notification and might be powered by foreign countries interested in affecting the poll results.

3.2 I-voting experience

This section reveals a large number of issues to be considered when deciding on the merits of I-voting and on the design of a system for this activity. In order to reduce the risks and produce a defensible system, it is necessary to identify the risks involved.

The section concludes with a brief description of previous experience with I-voting. As will be seen, various conclusions have been drawn about the process and its viability and it should be noted that the scope of these various experiments have been different. This reveals a large number of issues to be considered when deciding on the merits of I-voting. The testing of voting systems is a practical problem so the approach taken is to examine various methods for testing the correctness, security, usability, etc., of voting systems, starting with test ballots and verifiable protocols, code voting and so on. Quite clearly, these various testing methods can inform the design of new I-voting systems and models such as the one presented in this thesis.

Many countries have used I-voting, such as the USA, Netherlands and Belgium, using different technologies, such as touch screens, smart cards, tokens or machines similar to ATM engines, to cast votes (Gefen et al., 2005; Tan et al., 2005; Bonsor, 2004). However, others including Denmark, are still planning to initiate I-voting, although Danish election laws have already adopted the use of technology in elections to assist election practices.

Overall experiences of trial I-voting were different in different countries; however, the system security was generally not satisfactory. In addition, not every country employs open source systems which can be used by the public. Transparency was identified as an important aspect to enhance public trust in the Dutch, USA, Swiss and UK I-voting trials. Verification is necessary to avoid insider attacks. Evaluations of I-voting trials illustrate the importance of I-voting system testing, the possibility of Denial of Service (DOS) attacks and other attacks that might occur due to insecure platforms, especially on the client side, such as the DOS attacks on many government servers in Estonia. However, many countries have decided to stop using I-voting, including the UK, Germany and Italy (Ziegler, 2006) due to discovery of irregularities. The details of I-voting experiences in some countries are shown in Table 3.1.

Table 3.1: Global picture of I-voting experience

Country	I-voting experience	Main outcome
UK	<p>May 2000: 38 experiments in E-voting and counting in 32 local council elections.</p> <p>2002, 2003 and 2007: Several pilot tests of remote voting by mobile phones (UK Electoral Commission, 2003)</p>	<p>Security, integrity, availability and accessibility were the main challenges in I-voting (UK Electoral Commission, 2007a).</p> <p>Consequently, the Commission does not recommend continuing further pilots on I-voting (UK Electoral Commission, 2007b).</p>
France	<p>2001: I-voting from kiosk for municipal and cantonal elections</p> <p>May 2003: French citizens resident in USA allowed to vote online (voting participation 60%).</p> <p>March 2004: E-voting results declared for 33 cities, experience in general successful.</p> <p>2007: E-voting in French Presidential elections, but huge queues and equipment faults put some cities' systems out of action.</p>	<p>In spite of the support of some officials for the initiative of I-voting, some politicians wanted to stop I-voting.</p> <p>April 2007: more than 80,000 signatures were gathered in a petition against I-voting.</p>
Germany	<p>1999: Many pilot tests on E-voting technology at two universities (Osnabrück, Bremerhaven).</p> <p>2002: 1 million voters voted in Bundestag elections.</p> <p>2003: all polling stations connected electronically.</p> <p>2005 and 2006: E-voting in Bundestag elections and extra security measures adopted.</p> <p>2008: Optical-scan voting system based on digital paper used in Hamburg election since there had been numerous lawsuits about use of E-voting in Germany.</p>	<p>I-voting still illegal (Federal Ministry of Germany, Domestic Policy, 2007), it could be reconfigured easily by Erasable Programmable Read-Only Memory (EPROM).</p> <p>Consequently, the government removed approval for voting machines given in 1997 (Report of the Election Process Advisory Commission, 2007).</p>
India	<p>1982: First initiative on E-voting in experiment in North Parur, State of Kerala.</p> <p>2003: State elections by E-voting machines (EVMs): 1 million supplied for 700,000 polling stations around India.</p>	<p>Supreme Court of India ruled that E-voting does not contravene the law.</p>

Country	I-voting experience	Main outcome
Norway	2003: Pilot test for E-voting for local elections with touch screen technology.	Pilot shows system feasible, considering possible security issues. Furthermore, a specialised working committee assigned to E-voting drew up a report on issues and opportunities for E-voting and recommended continuing with pilot testing.
Spain	<p>Since 1995: Several E-voting pilot projects in polling stations</p> <p>November 2003 and March 2004: an I-voting pilot used to assess the efficiency of the I-voting system, especially regarding security. More than 23,000 residents abroad participated in I-voting.</p> <p>August 2004: the government considered some changes to the law on general elections to support I-voting.</p> <p>February 2005: I-voting held after changes applied in election law to support I-voting.</p> <p>July 2007: Experience repeated successfully.</p>	<p>Main challenge for I-voting was election law. However, in August 2004, the government considered some changes to the law on general elections to support I-voting.</p> <p>I-voting shows low participation: in February 2005 only 10,543 of two million voters cast their vote online by I-voting, using smart card technology.</p>
Brazil	<p>1994: Arrangements for an E-voting system set up</p> <p>1996, 1998 and 2000 elections: Direct Recording Electronic (DRE) voting system used, with significant increase in voting participation, reaching 100% in the year 2000.</p>	Brazil has experienced an increase in number of voters using E-voting by computers since introduction in 1990. Use exceeded 400,000 machines; data stored and transmitted on secure compact disk or by satellite modem.
Ireland	<p>February 2000, May 2002 and October 2002: E-voting launched in 2000 using modern technology in securing information, providing superior flexibility and facilitating voting process. Testing by independent authorities.</p> <p>May 2002 and October 2002: E-voting in General Elections proved its success</p> <p>June 2004: Initiated an E-voting system for European and local elections.</p>	<p>93% of voters found E-voting an incredibly simple practice; nevertheless, 87% favoured paper-based voting. Later, effort made to improve user interface and security.</p> <p>To examine confidentiality and accuracy of E-voting system, the government initiated an Independent Commission on Electronic Voting (CEV) in March 2004. In July 2006, CEV recommended use of E-voting for elections in Ireland, with some additional recommendations. Afterwards, a Cabinet Committee on E-voting examined E-voting issues and CEV's considerations.</p>

Country	I-voting experience	Main outcome
Austria	<p>Spring 2004: the Federal Ministry of Interior established a group to study E-voting.</p> <p>May 2003: Vienna University of Economics and Business Administration held a remote voting test in a Student Union election. Tokens consisting of an electronic National ID Card distributed for voting. April 2004 System used in Austrian Presidential elections.</p> <p>September 2006: System used for Austrians abroad; voters supplied with an electronic voting card to cast their vote online.</p>	<p>I-voting e-participation low, only 1,786 from 20,000 students from WU Vienna voted electronically.</p>
Belgium	<p>November 1991: E-voting was used in two electoral cantons.</p> <p>1995: 20% of voters voted electronically; later, in 1999, participation increased to 44%. Elections were broadened from regional, local, and general to European elections in 2000, 2003, 2006 through to 2007. In 2003, vote automatically stored in a database.</p> <p>April 2004: the government made some changes in election law to make E-voting promising in Belgium. However, in 1999, 2000 and 2003, an optical reader was used to scan ballot papers to provide an automated and reliable count.</p>	<p>E-voting software open sourced, opening polling station to voters triggered by Polling Station Chair and optical reader used to scan ballot papers towards providing automated and reliable count.</p> <p>However, some members of parliament displeased with E-voting system in which participation has not exceeded 44% since 1999. Also, there were many issues associated with the system in terms of security and secrecy. In July 2006, the Regional Parliament of Brussels asked for improvement of transparency of the E-voting system.</p>
Australia	<p>October 2001: First launch of E-voting in Australian parliamentary election, in 8 polling stations, where only 8.3% of voters cast electronic votes.</p> <p>October 2004: Experiment repeated: the need to provide an E-voting system for the next Federal election considered, to be accessible and usable by disabled people with poor vision or by blind persons.</p> <p>September 2007: E-voting tested on sample of disabled people with poor vision or blind persons after modifications of system to ensure they could cast their vote independently and</p>	<p>Barcodes applied to authenticate voters' votes. Computer used as a voting terminal, linked through secure local area network to a server in each polling location. Later, electronic counting combined all electronic and paper ballots.</p> <p>The Australian Electoral Commission (AEC) has worked on development of E-voting to enhance accessibility by providing audio, as well as enlarged screens and large telephone keypad to navigate and choose the preferred candidate and to cast the vote.</p>

Country	I-voting experience	Main outcome
	secretly in the 2007 Federal election.	
Canada	<p>Since 1990s: E-voting in use although there are no Canadian E-voting principles; voters have to obey some local principles but generally each city uses its own machines and principles.</p> <p>November 2003: 12 cities in Ontario used E-voting via the Internet and phone; as many as 100,000 voters participated. Authentication based on Voter Identification Number and password, given to voters. Some cities have used different technologies such as I-voting, touch screens, optical scan machines and some even still use paper-based voting in addition to E-voting.</p> <p>October 2007: VOTEX 'touch-screen voting machines' used in local election after its initiative in 2004.</p>	<p>E-voting has increased voting participation from 25 - 30% to 55% in some cities. Generally, growth of 48% experienced in the 2006 election.</p> <p>However, recent use of E-voting in main cities of Canada showed some issues, which indicates that E-voting needs to be improved. Main issues addressed included requests for re-votes, cultural barriers and lack of legislation, standards, management and security measures.</p>
Netherlands	<p>Since the late 90s E-voting began in the Netherlands. Since then, in 2000, the Netherlands' government experimented with I-voting for voters abroad. I-voting in European parliament and locally in 2004 and 2006. Experiments in June 2004 for I-voting and telephone voting for Dutch voters abroad. The Dutch Electoral Commission report suggested enhanced accessibility for people who found difficulty in accessing or using the system (Pieters and Haren 2007; Report of Election Process Advisory Commission 2007).</p>	<p>I-voting shows increase in voter participation from 5000 in 2004 to 21,000 in 2006.</p> <p>Secrecy and security were major issues identified by experts and this guided government to use certain computer voting machines in the 2006 national elections to avoid hacking and interrupting voting results.</p> <p>Currently, implementation of I-voting has been stopped</p>
Switzerland	<p>Since 2000: The government assessed the possibility of E-voting and conducted several trials to examine systems (Kersting, 2004) in which anonymity was guaranteed by use of anonymous mixnets channels. (Volkamer and Krimmer, 2006).</p> <p>January 2003: Geneva voters are the first citizens to vote electronically.</p> <p>December 2004: I-voting pilot tested in students' parliament election at University of Zurich where voters were allowed to vote by SMS. A secret key was sealed into the voter's polling card and votes were cast by selecting the</p>	<p>In Switzerland, voter turnout for elections is the lowest among democratic countries, dropping to 58% in 1945 - 1997 (Nohlen, 2007). Later, mobilisation suggested and seen to increase % of the turnout with interest in I-voting (Maur and Vontobel, 2007).</p> <p>Trials successful with no noticeable incidents, (Swiss Federal Council Report, 2002 and 2006) showed that securing I-voting is possible. However, some problems considered on authentication and securing of</p>

Country	I-voting experience	Main outcome
	<p>number of the candidates as represented on the polling card. Code voting was used to provide security from possible frauds on client side and anonymity ensured with mixnet technology.</p> <p>However, I-voting used as an alternative voting method (State of Geneva. E-voting, 2007; Sperlich, 2007).</p>	<p>client side, found hard to achieve, and possible appearance of vote selling and intimidation (Oppliger, 2002; Swiss Federal Council Report in 2006 commented on the risks associated with I-voting continuously increasing and therefore security measures should be improved. The Swiss government decided to continue E-voting pilot test and allow I-voting for citizens abroad in 2009 (Wili, 2007).</p> <p>The government still uncertain whether to consent to adoption of E-voting in Switzerland by 2012 as an alternative to paper and postal voting.</p>
Estonia	<p>2002: Legal provisions for I-voting assigned in Councils Elections Act (Office for Democratic Institutions and Human Rights, 2007; Breuer et al., 2006) aimed at increasing the participation rate in electoral voting, benefiting from availability of free Internet access for all citizens since 1999.</p> <p>2004: Development of E-voting system commenced; later, E-voting pilot in Tallinn for 703 voters. Following pilot outcome, some modifications applied to the system and, in 2005, Estonia introduced I-voting for local elections as an alternative method of voting (Thielbeer 2007). The encryption process also applied and ID-card authentication certificates for authentication; in February 2006 more than 900,000 ID-cards had been reported. In 2007 parliament elections used I-voting using the same technique and participation reached 30,275 voters.</p>	<p>The Council of Europe stated that I-voting has increased participation slightly but it is not motivating for people who do not participate in traditional voting schemes (Breuer and Alexander 2005). Their report indicates participation lower by 0.5% since only 5.4% voted electronically. Also, a survey by Alexander (2007) indicates only one tenth of E-voters prefer voting via the Internet.</p> <p>Although Estonia applied smart card technology, PKI and digital signatures to ensure the security of E-voting, the security of the system from possible attacks was a problem which might alter and affect the anonymity of the vote (Madise and Martens, 2006).</p>
USA	<p>2002: In the USA, Federal Help America Vote Act (HAVA) spent about \$4 billion to replace lever machines by stand-alone, touch-screen voting machines.</p> <p>February 2004: E-voting first used in South Carolina's Presidential primary election, but showed many security issues (Lemos, 2004).</p>	<p>An issue of I-voting was recounting votes through lack of voter verified papers; also, problems of transparency and security. In 2004, the US presidential election, there was a miscount of 18,000 votes in Florida due to electronic miscount (Krugman, 2007). Experience of I-voting in the USA shows the huge scale of vulnerabilities and risks of attack which requires redesign of hardware and software and</p>

Country	I-voting experience	Main outcome
	2007: USA certified to continue using E-voting (California Secretary of State) and initiate the Ballot Integrity Act to guarantee accuracy, integrity and security of the vote in federal elections (Top-To-Bottom-Review, 2007). Also, the US Department of Defense sponsored use of I-voting for US citizens abroad for the 2008 and 2010 presidential elections. Accessibility is an important issue that the election authority attempted to improve, where precise disabilities were concerned, such as visual and physical impairments, by using technologies such as a Braille-enhanced keypad.	continuous development of security measures to ensure security is under control (Jefferson et al., 2004). 2000: An experiment called SERVE (Secure Electronic Registration and Voting Experiment) by the US Department of Defense to support eligible overseas citizens and military to vote, showed issues were security, integrity, availability of Internet access and the possibility of sophisticated attacks (California Internet Voting Task Force, 2000; Report of National Workshop on Internet Voting, 2001; Jefferson et al., 2004; Camp and Bowman et al., 2005). As a result, the Pentagon recommended discontinuing the implementation of SERVE in 2004 elections.

In Europe, an emphasis was given to improving the current voting system with E-voting and, therefore, the CyberVote project was proposed with recommendations to study and assist the feasibility of E-voting and, in particular, I-voting. The CyberVote project and the Council of Europe's recommendations are described in the following sub-sections.

3.2.1 CyberVote project

In 2000, the European Commission (EC) launched the CyberVote project in collaboration with industries and universities across Europe (European Commission, CyberVote Report, 2003a). To study the possibility of using I-voting which ensures privacy of votes and contributes to the modern system of voting, the CyberVote project attempted to define a secrecy-integrated voting system, guaranteeing freedom, accessibility and usability for voters.

The voting system used homomorphic threshold encryption (a type of I-voting protocol) to hold multiple elections and cryptography. Smart cards with PIN codes were used for authentication. The system could be run on PCs, mobile phones and PDAs connected to

the Internet. The system was evaluated during elections in 2002 in France and in 2003 in Germany.

The experiment showed a low level of participation in E-voting. In a Swedish city, the trial was with elderly voters and about 200 took part, even though the testing was for a week. However, the experiment was successful, although some issues were raised about security (European Commission, CyberVote Report, 2003b).

3.2.2 Council of Europe's recommendation

With regard to voting, the Council of Europe (COE) aims to protect human rights and enhance democracy. In September 2004, the Council adopted a recommendation to develop an E-voting system (Council of Europe Recommendation, 2004). In the E-voting trial held by experts in the field, research by the Internet Policy Institute in 2001 showed the requirements of legislation, technology and users' familiarisation were essential for an E-voting scheme, with an argument over whether to process remotely through online voting or as stand-alone applications (European Commission, 2001). The recommendations state that I-voting should fulfil the fundamentals of democratic elections; it should be a reliable, secure integral system relevant to the law.

3.3 Why move to I-voting?

E-voting was introduced by politicians in the development of e-participation and e-government (Jan and Tai, 2007, pp.93-101). According to eGov Stakeholder Consultation (2005), 64% of people believe that e-participation and e-voting will help democratic philosophy by increasing turnout as result of simplicity. There are many advantages which motivate the introduction of I-voting, mainly its transformation to mobility, automated system and its support to 'green' IT. Each of these advantages is explained as follows.

3.3.1 Transformation to mobility

Saco (2002) and Alvarez et al. (2007) claim that the use advanced technologies could facilitate a successful voting process in remote or overseas sites. The rapidly expanding pool of voters from various locations, from cities, provinces, remote areas and even overseas, implies a need for creating ways to make the process of voting relatively easy, leading to a projected increase in voters' turnout. By these means, groups of people who are normally not found to participate in elections such as people overseas, young voters, elderly and people with disabilities can also be catered for (Alvarez, Hall and Roberts, 2007). Moreover, logistical challenges are one of the main variables to strengthen the need for I-voting.

Dictson and Ray (2000) claim that I-voting would enhance voters' convenience to vote remotely from any place and at any time through a secure channel. Also it is believed that the election committee could extend the voting period for a couple of days with minimum cost, unlike in paper-based voting which requires public service buildings as polling stations. In addition, voters can vote without the need to be restricted to attending their local polling station (Trechsel and Mendez, 2004; Kent, Harrison and Taylor, 2006).

Additionally, I-voting can cater for a population often less attracted to the elaborate traditional voting process, and capitalise on the use of technologies, gadgets and trends that mostly appeal to the young, hence significantly including them in the election process (Trechsel and Mendez, 2004; Kent, Harrison and Taylor, 2006).

3.3.2 Transformation to automated system

Administrative efficiency is also another advantage of I-voting. Ballot production and distribution will be eliminated in this process, hence removing previously inevitable waste of staff and money as a consequence of unnecessary production and, at times, over-production. In cases of I-voting, staffing costs for polling stations could be reduced, especially during the counting stage where computation is done electronically since voting areas will be populated by stand-alone voting machines (Dictson and Ray, 2000, p.4; Kent, Harrison and Taylor, 2006).

I-voting can also shorten the time needed to produce the final tally and reduce counting errors in the voting process as intelligent software is used to prevent over-voting or under-voting (Gibson, Nixon and Ward, 2003; Trechsel and Mendez, 2004;). Furthermore, I-voting would not allow ineligible voters to vote. (see Authentication, section 3.4.1).

According to Gibson (2001) and Grant and Chau (2005), I-voting is less costly than paper voting and it is accurate, easy to adapt to traditional voting techniques and expected to increase the level of participation since it reduces physical barriers which prevent voters from reaching polling stations and allows convenience to vote at any time and easily without the need to go to them (Dictson and Ray, 2000).

In contrast traditional voting in the USA has experienced a reduction in the level of participation from 63% to 50% in 1960 and 1996, respectively, and there were practical difficulties and annoyance with registration, long queuing and transportation, which might reduce voter participation (Bonetti, 2000; Bonsor, 2004). Voters who faced these problems did not find the voting process effective and precise.

3.3.3 Transformation to 'green' IT

Since technology is rapidly spreading all over the world, from the industrial sector to the basic home setup, this has, in turn, increased the demand for energy. However, ICT is among the fastest growing sectors of energy use and even though one of its main advantages was that it was an alternative to the more energy consuming industrial processes of the past, it has now become a danger to the energy sector also. Currently, it is estimated that the global carbon emissions of ICT industries are at 2 to 2.5% of the total world carbon emissions, very close to those of the airline industry (Green IT, 2010). This percentage rises in the developed countries to 5 to 6%. Also, the energy costs in many IT budgets are slowly rising from a previous low of below 10% to a perceived future peak of over 50% (Green IT, 2010).

This definitely warrants a closer look at green IT and its perceived green advantages. One of the obvious advantages of green IT is that it is clean and slows down the effects of global warming through the general reduction in CO₂ production (Harris 2008, p. 71). Thus, it has become necessary for the public to be educated on the real effects of these seemingly lifesavers when it comes to the environment and how society may take responsibility. Approaches to 'green' IT are many and can be broadly categorised into two main areas: optimisation in the IT software and management of power use by the various machines (Sam, 2008, p. 24). There are also other approaches that are less technology based, such as the recycling of materials and the enforcement of various employee regulations in IT companies. The above are just a few of the many strategies that may be used to achieve energy conservation and actually realise the true benefits of using 'green' IT as a means of saving natural resources.

Likewise, I-voting can support 'green' IT since it shifts the voting process from a manual system towards a computerised, remote voting system. I-voting will help to go green with the reduction of a huge amount of paper consumed in the traditional paper-based voting system. However, there comes the need to ensure optimisation in the IT software and power usage. This could be reduced either by human beings being responsible enough to carry them out, or there can be the alternative of installing special sensors that will be able to interact automatically with control systems that will shut down power when it is not in use or after a certain number of hours.

In the same vein, the management of individual IT companies should make the effort to purchase products that use advanced power management devices and software such as ASICs, PMICs and VRMs, among others (Kevin, 2003). Another alternative may be the use of energy-star equipment, popularly known as e-star, which maximises energy use and has very little wastage. When these steps are taken, there will not only be a reduction in energy use but also a reduction in CO₂ emissions per voter. This was a great motivation for the researcher to promote I-voting for a green, healthy environment for the future.

On the other hand, Gibson (2001) has commented that I-voting might reduce the number of voters because of a limitation of access for poor people, people with limited computer skills and other ethnic marginals. Hence, although I-voting should be accessible for all voters as far as possible, bearing in mind different disabilities (Boutin, 2004), ensuring accessibility might have some cost implication since it requires special equipment such as headphones and Braille keypads to assist sight-impaired voters to cast their vote without need for assistance. Consequently, use of both I-voting and traditional voting schemes would be effective where citizens would choose their preferred method to cast their votes (Mercuri, 2000). Although there are lots of arguments that support I-voting because of its advantages, some are against, since it has a lot of associated negative issues as described in the next section.

3.4 Architecture of I-voting

I-voting requires ensuring voting basic principles, including authentication, mobility, flexibility, accountability, anonymity, security and privacy (see Figure 3.1).

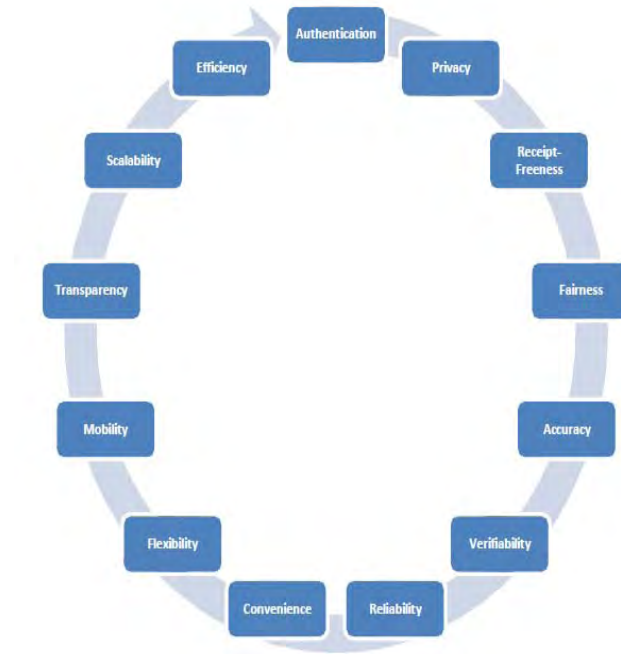


Figure 3.1: I-voting basic requirements

All of these requirements are defined as challenges for I-voting. There are a number of proposed voting schemes in the literature to overcome these challenges, each of which is addressed below, with possible solutions.

Hoffman (2005) and Rodriguez (2003) suggested the need for standards and regulations for I-voting to administer the whole voting process and guarantee fulfilment of the voting requirements defined earlier. On the other hand, the development of standards to certify I-voting would need to cope with rapid changes in the technology.

In general, I-voting has a number of arguable concerns, in particular the possibility of huge threats in the Internet world (Rubin et al., 2004a), such as denial of service attacks, malicious code attacks, spoofing, social engineering, server operating system vulnerability, authentication attacks and Domain Name System (DNS) attacks (Rubin et al., 2004b; Coleman, 2003). Table 3.2 shows the possible threats to I-voting, their consequences and countermeasures.

Table 3.2: Possible threats to I-voting

Threat	Skill needed	Impact	Realistic?	Defeat mechanism
Denial of Service (DoS)	Low	Disenfranchisement	Common on the Internet	No simple tools; requires hours of work by network engineers; launchable from anywhere in the world.
Trojan horse	High	Disenfranchisement	Common on the Internet e.g. spyware	Can mitigate risk with careful control of PC software
On-screen electioneering	Low	Voter annoyance, frustration, distraction, improper influence	Trivial with today's Web	Nothing a voter can do to prevent it, unless they have a clean Operating System
Web spoofing	Low	Vote theft, privacy compromised, disenfranchised voters	Common on the Internet	None exists; likely to go undetected; launchable from anywhere in the world.
Client compromising	High	Vote change or theft, privacy compromise	Common on the Internet	None exists for all possible mechanisms. Too difficult to anticipate all attacks; some likely never diagnosed.
Insider attacks	Medium	Complete compromise of the election	Most common, dangerous, difficult to detect of all security violations.	Need to restrict access and involve more than three people to perform any task.
Automated vote selling	Medium	Disruption of democracy	Very realistic, since voter willingly participates.	Over-write vote could solve the problem.
Coercion	Medium	Disruption of democracy	Man in the middle attacks makes it achievable.	If successful, likely to go undetected.
Specific virus	Medium/high	Vote change or theft, privacy compromise, disenfranchised voters	Some attacks require only experimenting with the system; others require leak of I-voting source code and a resourceful attacker	Virus scanning can detect known viruses, but not new ones; likely to be undetected.

These possible attacks have become common due to the availability of many free-of-charge tools which provide assistance even for people with novice computer knowledge in making malicious attacks (Coleman, 2003). DoS attacks might, in consequence, have a huge impact on the voting process because they send a flood of requests for the service which the server can not handle, leading to slowing down or shutting down of the server (Rubin, n.d.; Marconi, n.d). However, such attacks could be dealt with in two steps: (1) analysing the incoming packets, strip headers and trailers, looking for attack packet information, and (2) developing patch filter attacker packets (Xianju et al., 2000). Moreover, election committees could use redundancy of servers to handle a large number of requests. Another possible risk is physical attack on the Internet cable which could cause disruption in accessing the I-voting website; for example, in 2008 four undersea cables were damaged causing slow Internet access (BBC News, 2008). However, in a highly networked environment this may not be too serious as alternative routing would always be available.

In the last three decades experts strove to propose a cryptographic voting protocol to maintain a secure system, assuming that the client machine is reliable and secure from which to send ballots. However, those protocols were mainly considering securing ballots over the network channel and at the server side. In I-voting there are three main components which communicate to facilitate the voting process: the client, Internet and server. The client will send a ballot via the Internet network to the server which will then run the ballot through different protocols to ensure that it reaches its destination safely. The possible attacks associated with the client, Internet and server-side of I-voting are described as following sections.

3.4.1 Client-side attacks

Unreliable client machines create serious problems leading to compromising the integrity of the election (Gerck et al., 2001) (see Figure 3.2).

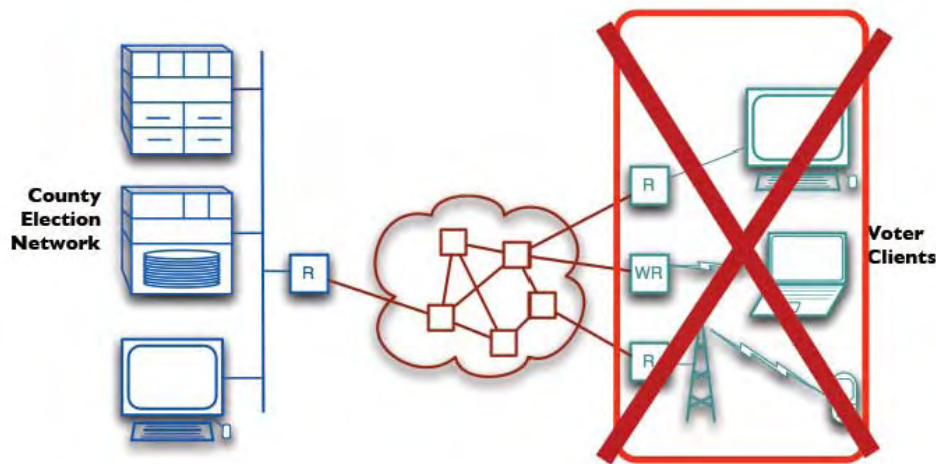


Figure 3.2: Client-side malware attacks

Computers connected to the Internet are known to become infected with viruses, worms, Trojans, spyware, malware, etc. (Gritzalis, 2002; Rubin, n.d.), although some studies on I-voting consider viruses and Trojans are acceptable threats (California Internet Voting Task Force, 2000). However, the extent of this threat is that it can change a voter's choice without their knowledge, before the ballot is sent to the server, so even if the Internet voting protocol is well designed and cannot be hacked, hackers can still make a major effort to tamper with some of the important voting principle of secrecy and integrity. Moreover, an add-on to the Internet browser which needs 20 to 30 lines of JavaScript code could be programmed to change or spy on a voter's choice (Chaum et al., 2010). Such an attack could be done in two ways: (1) a selective attack needs knowledge of a voter's choice to change it to the attacker's preference (2) a random attack, changing a voter's choice randomly. The first attack is considered to be hard to accomplish since the attacker needs to know the voter's choice which cannot be predicted or known with an automated attack. The random attack is widely used to disturb the election process (Jefferson et al., 2004; Kohno et al., 2003). Table 3.3 summarises some of the possible attacks to infect computers.

Table 3.3: Summary of possible computer attacks

Threats	Attack	Description
Automatic vote changing	Malware	Randomly alters a voter's choice without the user noticing. This type of attack could focus on a certain party or geographical area to change votes to the attacker's preference e.g. target Wales and change its votes to support London candidates.
Vote dropping	DoS, malware	Deludes the voter that vote has been successfully cast, whereas it might not have been.
Voter impersonation	Malware, Virus	This type of attack needs human agency. It needs to capture the user credentials' information and then send them to the attacker, who would cast the vote instead of the real voter. This type of attack is impossible if the Internet voting system is using two or three factors of authentication (see section 3.4.1).
Vote disclosure	Malware, Virus	This type of attack could tamper with secrecy by recording the voter name and choice to then be made public.

Chaum (2001) and Oppliger (2002) argued that a hybrid solution is the best to maintain client machine security by using another medium that is unavailable to computer malware (e.g. a smart card) along with one of the solutions described below. A hybrid solution would be ideal since each individual solution has advantages and disadvantages. Therefore a combination of a vote coding sheet with a smart card or clean operating system with a smart card would be a good solution to make vote changing harder or impossible. A survey of proposed solutions found in the literature to help maintain a reliable system is described below.

3.4.1.1 Completely Automated Public Turing Test to Tell Computers and Humans Apart (Captcha)

The aim of this approach is to have input from a human in which a virus could not determine what is the input. The Captcha development takes various forms (text, image and 3D Captcha). Text and image Captcha is the easiest approach to implement and to crack with high success rates reaching 100%. Some researchers describe the breaking of Captchas (Mori and Malik, 2003; Chellapilla and Simard, 2004; Chellapilla et al., 2005). In I-voting, different factors weaken this approach since the algorithm would be

limited by a number of candidates to compute the text or image to challenge the virus. However, malware or viruses would require part of the Captcha image to determine the candidate name. Also, the size of candidate name is an important factor in calculating the Captcha image. Captchas are widely used by Google, Yahoo and AOL to prevent viruses from automatic creation of accounts and in recent research by Websense, Sumeet Prasad (n.d.) demonstrates how easy automatic creation of accounts is using optical character recognition (OCR) with success rates between 10% and 35% within 6 seconds. Also, the size of candidate name is an important factor in calculating the captcha image. Figure 3.3 shows an example of Captcha image developed by Scantegrity (2008).

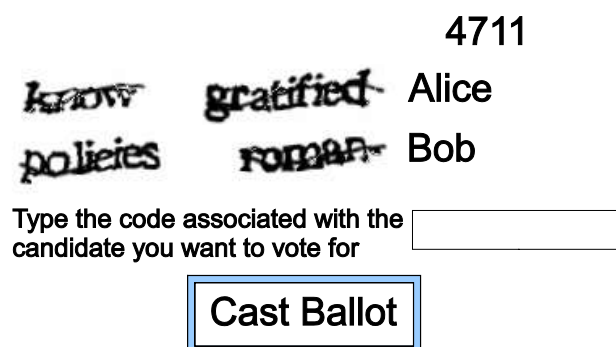


Figure 3.3: Example of Captcha image Scantegrity (2008)

On the other hand, multi Captcha images computed from different factors (mouse clicks, candidate name, voter data) would create a strong Captcha which the malware code could not determine, even if the attacker knows how the algorithm works. However, it would be difficult to include many Captcha images with good size on the voting page.

A better technique using 3D was introduced by Kaplan (n.d.), which depends on human differentiation of details in the image (see Figure 3.4). The image would be divided into parts and each part has some text or signal character. Users would be asked to type what is the text in some part of the image. Due to the dependence of the natural design of the algorithm on different user input there is no way to crack it, because it would require identification of each part of the image. This then suggests that each candidate should have 3D captchas on a complex background which can be easily identified by a human but with difficulty by a virus.

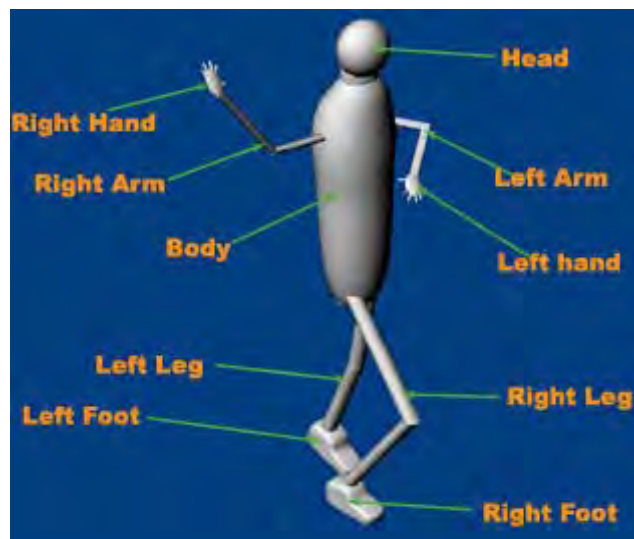


Figure 3.4: Example of 3D captcha: Walking man attributes

3.4.1.2 Code sheet voting

This approach was first observed by Chaum (2001a) to resolve the problem of privacy and integrity of voting by making the voter's PC secure from any vote manipulation. The idea of this approach is that each voter is given a code representing each candidate, the codes being randomly chosen from a wide range of numbers. The voter would be asked to type the appropriate code for the chosen candidate. This will prevent viruses and malicious software from detecting the voter's choice unless the voter has revealed the codes. The codes are sent by mail to voters and once they cast their vote, the voting server decodes the code to the related candidate. An example of a ballot and CodeCard is shown in Figure 3.5.

<p>Election for the most important figure in security.</p> <p>A - Alice B - Bob C - Eavesdropper D - Attacker</p> <p>Enter your vote code:</p>	<p>CodeCard</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Candidate</th> <th style="text-align: left;">Vote Code</th> </tr> </thead> <tbody> <tr> <td>Blank Vote</td> <td>SIT5Y</td> </tr> <tr> <td>A</td> <td>A3CR2</td> </tr> <tr> <td>B</td> <td>97RG7</td> </tr> <tr> <td>C</td> <td>GHFT1</td> </tr> <tr> <td>D</td> <td>WL764</td> </tr> <tr> <td>...</td> <td></td> </tr> </tbody> </table> <p>Confirmed vote delivery code: 6HKG2</p>	Candidate	Vote Code	Blank Vote	SIT5Y	A	A3CR2	B	97RG7	C	GHFT1	D	WL764	...	
Candidate	Vote Code														
Blank Vote	SIT5Y														
A	A3CR2														
B	97RG7														
C	GHFT1														
D	WL764														
...															

Figure 3.5: Example of ballot and CodeCard

Code voting would ensure voter privacy and integrity, since only the voter has the code. The applicability of the approach has been tested in a number of elections e.g. Swiss cantonal elections and in the UK. However, in the Netherlands, codes are used only for voter identification because it would be complex for multiple casting. Hellbach and Schwenk (2007) improved the approach by using a three-way-handshaking protocol which asks for a third code to confirm the vote. Moreover, some of the code voting approaches provide a verification number for voters to verify their votes. Helbach and Schwenk (2007) and Oppliger (2002) believe that code voting would maintain security of the client machine from vote manipulation. Moreover, Rubin (2002) added that code voting and trusted computing could achieve high security on the client side. However, improvement could be made by using a matrix table for the vote, an idea was inspired from the Entrust IdentityGuard. The idea behind it is that the voter would be asked to enter the randomly determined code, e.g. 1F 4D 7D 8S, using the matrix table which could be provided on the back of the voter smart card, and the voter would cross-reference the given value to determine the code. An example of the approach can be seen in Figure 3.6.

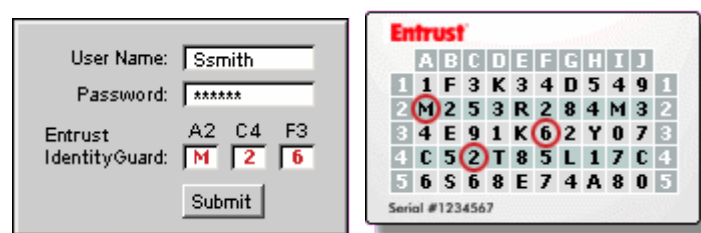


Figure 3.6: Improvement of code voting by using matrix table

3.4.1.3 Clean Operating system and voting application

This approach suggests use of a ‘clean’ and certified operating system and voting application, booted directly from a CD-ROM or other media such as a USB or hard disk drive. The voter would need to boot the clean operating system to access the voting application. Although it would ensure reliability of the voter machine, some drawbacks are:

- (1) Compatibility of client hardware.
- (2) Configuration of Internet connection e.g. BT has different configuration from O2.
- (3) Ensuring integrity of the CD to boot from.
- (4) The costly of the CD distribution.

The Trusted Computing Group (2007) do not believe that this approach could be successfully used to enable secure voting from any computer with an Internet connection. On the other hand, the day-by-day software development requires people to change their hardware to keep up to date with what is on the market, and regarding the Internet connection, programmers can include all the configurations for all telecommunication companies. Moreover, the configuration to access the Internet is done at the router side, so even dial-up requires simple configuration such as the Internet service provider username, password and domain.

3.4.1.4 Special secure hardware for PC

This approach suggests use of an external device, with secure I/O, connected to the voter’s machine, e.g. through a USB port. The device should display the ballot, allow a vote to be cast, carry out cryptographic computations and acknowledge the voter result. The voting protocol is carried out by the secure device which uses closed software that can not be changed or configured, therefore there is no chance of infection from malicious code. There are a few main drawbacks to this approach: (1) the cost of the device, (2) the manufacture and distribution of the devices (Saltman, 1988).

Z’uquete et al. (2007) used a secure smart card reader as a secure device which supports I/O and the ability to display the ballot and read the voter’s choice. The advantage of

using a smart card is that the PKI approach could be implemented for authentication and encryption, as used by Z'uquete et al. The advantage of using a smart card reader is that it is hard to tamper with. Also, another approach could be used along with the smart card reader, such as a vote coding sheet, to achieve maximum security on the client side. Bearing in mind both solutions could work perfectly together, since many countries use a smart card to authenticate to an E-government portal, such as Qatar, Estonia and UAE, it is therefore assumed that a card reader does exist. Regarding the vote code matrix table, this could be printed on the back of the smart card (see section 3.4.1.2).

3.4.1.5 Closed secure device

This approach is similar to special secure hardware for a PC (see section 3.4.1.4) and was suggested by the California Internet Voting Task Force (2000). The idea was the use of special closed software with Internet-capable devices, such as a hand-held PDA or mobile phone. However, mobile phones and PDAs allow users to access the Internet and install applications which make them open to malicious attack. The idea of developing a special device to access the Internet and cast votes works against the I-voting advantages of being an easy to use and cost effective system, so this approach is not considered further.

3.4.1.6 Secure PC operating systems

This approach suggests the use of secure PC operating systems composed of digitally-signed modules, that would then permit secure applications to exclude, as untrusted, modules of unsure source (i.e. potentially malicious programs). This approach was recently named “trusted computing” to offer secure platform support (Trusted Computing Group, 2007). It allows remote ratification of machines. In I-voting, it could be used to certify that a voter is using a trusted application or machine. It also secures the I/O process between the application and the devices and as result establishes a safe environment for an application to run. The ratification operation is based on measures carried out using software by a hardware module called a trusted platform module (TPM).

According to Rubin (2002) and Volkamer et al. (2006), a trusted computing approach guarantees trusted connection between the voter and the voting application, so that no malware can record the user input or modify it. The regency of this approach is considered as a barrier to deploy this technology (Sadeghi et al., 2006) and the withdrawal of cracked machines (Brickell et al., 2004).

The trusted computing concept ensures stabilising of voting application behaviour (Volkamer et al., 2006). This suggests that voters could access trusted computers via a Virtual Private Network (VPN) and a government would need to provide a clean and secure machine to be used for the VPN so voters could connect to this machine using the VPN to cast their vote using a trusted machine. Even if the client machine is compromised, users would not be affected by any virus or malware attack. This approach could be expensive but some operating systems provide free VPN. The real problem remains with the usability, since voters would need to learn how to access the trusted computer using a VPN connection which would create a private network between voter and the trusted machine.

3.4.1.7 Test ballots

Test ballots and voter verifiable protocols are examples of two methods of testing, where test ballots will examine the voting system before vote counting. A vote verifiable protocol is a method in which the test is conducted under real conditions, where receipts are provided for voters as a verification of their voting in case any problems are encountered during the election. In the test ballot, voters and voting administrators have the responsibility of testing the system for any malfunction and other risks. This is a kind of intrusion detection that helps in recognising attacks that might introduce viruses and malicious software, so that trust in the system is enhanced (Oppliger, 2002). Analysing the I-voting system involves establishment of a threat model, which defines and evaluates the possible risks associated with an I-voting system (e.g. viruses, DoS, phishing, etc.). However, there is a chance that attackers might know the ballot is a test and not real and therefore would not engage in their attack. Also, attacks are improving rapidly, which brings new risks for the future.

Vote-verifiable protocols provide verification to enable voter auditing when required without abuse of privacy, though some believe that it might be used as a proof of vote and thereby enhance vote selling and intimidation. However, there are four verifiable voting protocols: Neff's voting scheme (Neff, 2004a, b), Chaum's visual crypto scheme (Chaum, n.d), Ryan's voter scheme (Ryan, 2004) and Chaum's Scantegrity scheme (Chaum et al., 2008). Each tries to reduce the risk of vote selling and intimidation by providing receipts with less information. Individual verification ensures that votes have been cast and universal verification tries to ensure the correctness of the voting process through transparent tallying. This process requires a trusted bulletin board which shows the votes, so that every voter can check against the receipts; if it does not match, voters can dispute it.

Neff's, Chaum's and Ryan's schemes all provide receipts containing an identification number and verifiable calculation, an approach called End to End verifiability. In Chaum's and the Scantegrity scheme, voters are provided with their registered vote number. It could be argued that those schemes are vulnerable to security problems such as voter recording or changing vote attack which could be achieved by malicious software installed in the voter machine as it would motivate vote selling, since the voter could provide a confirmation of vote to the vote buyer. However, those schemes could be improved by allowing voters to over-write their vote. Furthermore, it should be noted that the Ryan and Scantegrity schemes are usually applied in optical scanning ballots and security issues might arise, dependent on authority, chain voting and illegal receipts. Even Neff's and Chaum's schemes are vulnerable to security problems (Neff, 2004a, b; Chaum et al., 2008).

3.4.1.8 Obscurity/Complexity

This approach, while not sufficient to guarantee the security of the system, raises the cost for potential attackers. Digital ballot formats and voting software may be kept secret prior to the election and possibly randomly changed during the election. In order to carry out an attack successfully and escape detection, malicious software authors must have a great deal of information about the internal format of the ballot and voting software. If these details are not available in advance, and/or if that information is

complex, the potential authors of attack software may not have enough time to develop and distribute it within the election window.

On the other hand, it is difficult to establish a lower bound for the time needed to write malicious software. Additionally, the system is still vulnerable to attacks that collect voters' authentication data and use them later in the real voting client software.

3.4.1.9 External channel verification

This approach aims to provide an additional communication channel to the server to make sure that correct votes reach their intended destination. Kutylowski and Zagórski (2007) designed a voting scheme which uses this approach to first “decrypt” the voter choice and then to verify with a probability of $1/2$ that the vote was cast successfully to its destination. The major drawback of this approach is the complexity of the verification process, especially when voters must deal with the encrypted ballots.

Skagestein et al. (2006) suggest verification of the clear cast vote, where voters could verify their vote using another machine. It would ask the voting server for the voter's vote, obtaining it using a secret encryption key to encrypt the vote to be stored in a secure medium at the time of vote casting, and display the vote to the voter. To solve the problem of vote selling and coercion, over-writing could be enabled so voters could re-vote at any time within the election time and only their last vote would be counted (Volkamer and Grimum, 2006). Volkamer and Grimum (2006) added that a decision on the voting channel could be made either before or during the election.

In multiple casts, fairness is an issue, since it is allowed only for online votes and not paper-based ones. Other issues might arise on assigning the final casting of votes, where a trusted timekeeper is required to ensure reliable timing. Although it might resolve intimidation issues, it will not prevent fraud. In addition, trusted computing is essential to enhance trust. However, this scheme has some weaknesses such as (1) it does not stop vote manipulation on the server side, (2) an insider attacker who has access to an encrypted vote can decrypt it using the secret encryption keys kept by the voters, (3) it

requires the voter to have two machines (see Figure 3.7), one for vote casting, the other for verification. This would not be convenient for some voters because verification is done after vote casting. However, the Skagestein et al. (2006) approach could be improved by sharing the secret key between parties using the Threshold encryption concept (see section 3.4.3.5).

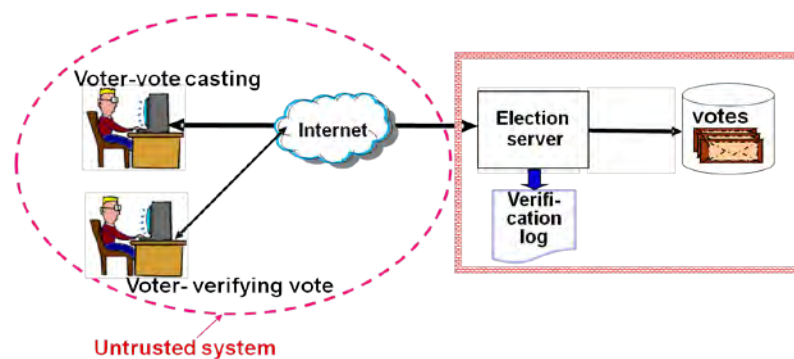


Figure 3.7: Use of two channels (1) vote casting (2) vote verification

3.4.1.10 Public bulletin board

The idea of public bulletin boards is to publish all voters' votes online, so voters could verify that their vote was cast and counted, without the ability to modify it. In this approach it is not clear whether the voter name should be listed with the vote or the serial number with the vote; however, in several voting schemes all options were suggested. However, since voting should be kept private, this implies the use of anonymous channels although this raises verification issues; hence the suggestion of providing a receipt for voters with only a serial number along with the voter choice to prevent vote selling.

3.4.1.11 Authentication

An authentication mechanism would ensure that only people eligible by law can vote but only once (Juang and Lei, 2006), as the entire election would be linked to a central database (Dictson and Ray, 2000). This could be ensured in I-voting through registration and authentication and linking to the central database (Cranor and Cytron, 2007). The purpose of keeping a voters' register is to guarantee that only people eligible by law are allowed to vote and that no one can vote more than once, unless the law allows multi-vote casting (Juang and Lei, 2006 pp. 339–348).

Authentication can be performed by a trusted authority to ensure its voter eligibility, electronically and/or manually, depending on election requirements. In the manual authorisation process, identification of eligible voters depends mainly on the person and authority responsible for validating voter eligibility before vote casting. This is a time consuming process and prone to human error in large-scale elections compared to electronic methods of authentication where this process is done automatically through advanced technologies such as digital signature, smart card and biometrics.

According to Schneier (1996), to attain an advanced level of authentication, votes should use numerous authentication processes: something they know (e.g. a username and password), something they are (biometric) or something they have (e.g. a smart card) (Adams, 1999). However, according to Newton (2007), there are still questions about the accuracy of biometric technology, e.g. labourers might find difficulties in reading their finger print. Moreover, use of a smart card can be costly, since it requires reader equipment and there is the possible problem of experience in terms of usability of the system and consideration of the human-computer interface (Quesenbery et al., 2003). However, the use of a smart card would enhance the security of the system since tampering is impossible (Joaquim and Ribeiro, 2007). This suggests having more than one level of authentication combining smart card, biometrics and PIN. The use of a virtual keyboard might prevent spyware from detecting keyboard actions. Also, a digital signature would be useful to ensure data accuracy and integrity while transmitting over the Internet, since it has an embedded special code by which the receiver can know if the data were read by a hacker (Fujioka, 1992).

3.4.2 Internet-side attacks

Concerns about security and potential violation of voter privacy have also been a major issue in using I-voting, which takes place in an insecure communication channel (Internet network) (Cranor et al., 2000; McGraw et al., 2000; Rubin, 2000, Weinstein, 2000; Oostveen and Besselaar 2004). The Internet-side of I-voting encounters many malware attacks (see Figure 3.8).

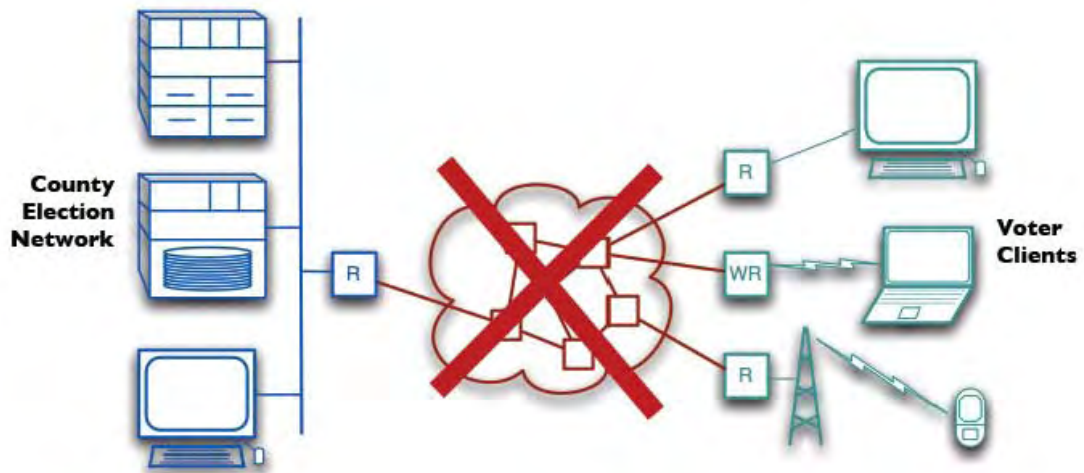


Figure 3.8: Internet-side malware attacks

These issues have been emphasised in a number of reports from government appointed agencies, together with independent policy institutes (Bimber and Davis, 2003). The use of I voting is strongly opposed, mainly due to its security constraints. With responsibility for voters and voting infrastructures removed from election administration and staff, there are many fears that they may be manipulated to cause unfavourable voting outcomes (Trechsel and Mendez, 2004).

In this section, three basic Internet voting protocols are discussed, each of which is improved by a number of researchers. Those protocols hide a voter's identification, making it anonymous so that no one can know the voter identity and decision. Both in traditional voting and I-voting, authorities are assumed to be fully trustworthy, even if they are not thorough. At least two authorities are involved, one for authorisation and one for vote counting (Wu and Sankaranarayana, 2002).

Concerns about privacy would be eliminated by the anonymity of a voter's ballot, also the election committee should not have control over the voting system and infrastructure (California Internet Voting Task Force, 2000; Rubin, 2001). Also involving more than one element with a secret key would solve the problem of an insider attack (Chaum, 1981; Danezis and Diaz, 2008). A comparison between different I-voting protocols: blind signatures, mix-nets and homomorphic encryption is shown in Table 3.4.

Table 3.4: Comparison between blind signatures, mix-nets and homomorphic encryption

	Blind signatures	Mix-nets	Homomorphic encryption
Improvements on Protocol	Fujioka et al. 1992, Sako 1994, Cranor and Cytron 1997, Herschberg 1997, Okamoto 1997, Ohkubo et al. 1999 DuRette 1999	Chaum 1981, Park et al. 1993, Sako and Kilian 1995, Ogata et al. 1997 Jackobsson 1998	Benaloh and Fischer 1985, Benaloh and Yung 1986, Benaloh 1987, Benaloh and Tuinstra 1994, Sako and Kilian 1994, Cramer et al. 1996, Cramer et al. 1997, Hirt and Sako 2000 Baundron et al. 2001
Remarks on protocol	Simplicity, low computational costs and ballot independent.	Requires less voter interaction, but would be complex to prove vote correctness	Very complex mathematically, therefore high computational costs. Used for one candidate elections (Yes or No)

With the requirements established, it is necessary to investigate the protocols explored in the I-voting literature. It is clear that protocols must be established in order to maintain secrecy. Exploration of these protocols will help in the present research to define the best practise Internet protocol to be used as a basis for the Qatari I-voting system. As will be seen below, blind signature plays an important part in the researcher's proposal as it is more flexible and with less computation (see Chapter 9).

I-voting might involve huge risks associated with functionality. Therefore, it can be regarded as an untrustworthy platform. Therefore, a way forward is to identify and clarify the risks and then produce methods of defence against the risks and testing their effectiveness.

3.4.2.1 Blind signature

A digital signature provides secure authentication and anonymous voting (Anane et al., 2007). Many voting protocols are based on blind signature since it is simple and efficient (Chaum, 1982, 1983). It is used to isolate the ballot from the voter's identity without the need for anonymous channels (Fujioka et al., 1992, 1993).

Blind signatures allow electronic text to be signed without exposing its contents. Valid legal voters will be given a blind signature for a token from the authorisation authority. From the blind signatures, the signed tokens are pulled out and then sent to the vote counting authority (Chaum, 1983).

Although this straightforward solution tries to resolve the anonymity issue, still it is difficult to ensure complete anonymity, especially with the involvement of all the authorities where hiding the link between voters and their votes becomes a challenge (Wu and Sankaranarayana, 2002).

Common implementations of blind-signature based on the Fujioka et al. (1993) scheme are: Sensus (Cranor and Cytron, 1996) which was found to be heavy and not balanced, EVOX (Herschberg, 1997; DuRette, 1999), and REVS (Robust Electronic Voting System) (Joaquim et al., 2003) an improved version of EVOX, which is an I-Voting System employing blind signatures. Joaquim et al. (2003) have improved the robustness of EVOX by associating vote weights; however, complexity of vote registration process was encountered in this proposal.

Some researchers propose cryptographic-based I-voting, such as in the Votopia project (Kim, 2002) which proposed I-voting for the Soccer World Cup of 2002 based on PKI using a Java applet to execute cryptographic processes. However, Votopia had problems with ensuring the anonymity of votes. Another well known project is the SERVE (Secure Electronic Registration and Voting Experiment) I-voting project (Jefferson et al., 2004) which proposed a practical I-voting scheme involving a PKI, however the project was cancelled due to arising issues (Schwartz, 2004), such as anonymity, where the web server knows the vote of each voter.

The Rijnland Internet Election System (RIES, 2009) developed for the Water Board elections in the Netherlands raises some issues such as the use of a single master triple-DES key. EVM2003 (Evm, 2003) is an example of open source I-voting which had some drawbacks due to not using any cryptographic voting protocols such as Blind signature or Mix netting. GNU.FREE (2004) proposed a stand-alone I-voting system using a Java program and BlowFish cryptographic algorithm, which showed security vulnerability.

Research by Wachowicz (2010) focused on introducing new ideas to voting, the so-called bidirectional voting and continuous voting to help in improving the quality of the democratic process by giving voters the chance to indicate their favoured candidates in bidirectional voting and consequently allow candidates to continuously review their grading. The Condorcet Internet Voting Service (CIVS, 2003) is an example of a bidirectional I-voting system which gives rise to security privacy issues due to lack of full cryptographic integration.

Ibrahim et al. (2003) proposed a secure e-voting using blind signatures, however the system requires preparation on the client side by installing a specific application to use the proposed I-voting system. Recent research by Purushothama and Pais (2009) overcomes issues identified by Kim et al. (2001) and Ibrahim et al. (2003) by proposing a secure I-voting system using an Identity Based Encryption System (IBES). The system ensures security of the client side voter without requiring the voter to download specific programs or browser. An Applets program was used and could be executed in a voter's browser that supports Java. The system shows its effectiveness in fulfilling many security requirements including privacy, anonymity, eligibility, accuracy, fairness, uniqueness and verifiability. This was proved using a security analysis process including calculation of the cost per request to vote and the cost of the PKG (Private Key Generator) server operations and database operations. Those calculations shows the speed of the proposed system where the voting process can be completed securely in a second. However, the system does not use PKI cryptography nor certificate recovery and confirmation. This suggests the use of an Identity Based Encryption System is not enough to ensure security and PKI and digital certifications would be better.

3.4.2.2 Mix Networking (Mixnet)

Mixnet establishes anonymity for the sender of the message by reshaping the communication. This technology can provide anonymity for voters (Chaum, 1981).

The process works as follows. Large messages are split into short ones and random bits are then added to obtain a specific length. These split messages are encrypted and mixed so that the identity of the message is mixed by more than one mixer to avoid recognition of the sender and receiver (see Figure 3.9). The output of the mixnet does not correlate with the input (Wagner, 2006).

The mixnet protocol was improved by a number of researchers to solve some of the problems occurring in re-encryption while shifting between servers. The re-encryption mixnet was improved by using threshold el-Gamal crypto in which all authorised parties run mixnet together. The message is decrypted only when all parties participate in the process (Ryan and Schneider, 2006). Furthermore, a verifiable mixnets approach achieves the integrity of the system since the plain-text input into the mixnet matches the decryption cipher-text output of the mixnet. However, this will not ensure anonymity. Zero knowledge interactive proof (ZKIP) is applied for each mix-server to provide verification (Buchmann 1981; Wagner 2006). For auditing, randomised partial checking is allowed (Jakobsson et al 2002; Chen 2007).

Research by Chun-Ta et al. (2009) proposes an I-voting protocol offering vote verification for voters to avoid vote selling. The proposed protocol was compared with similar protocols by Liaw (2004) and Chang and Lee (2006) and show their effectiveness in satisfying many requirements, including accuracy, simplicity, privacy, democracy and verifiability.

The research community have made important improvements towards providing a robust mixnets scheme in practice (e.g. Furukawa and Sako, 2001; Neff, 2001; Boneh and Golle, 2002; Golle et al., 2002). Common mixnet schemes are VoteHere VHTi (Neff, 2001) which emphasises voter verifiability, Scytl Pnyx (Riera and Brown, 2004) commonly applied in some government systems in Europe and SureVote (Chaum,

2004; Vora, 2004) a hardware improvement of the mixnet method introduced by Chaum (2004) which includes visual crypto to ensure voter verifiability.

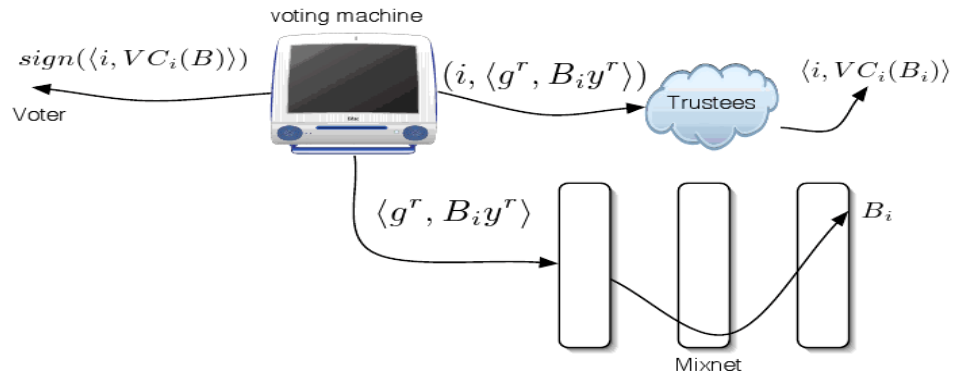


Figure 3.9: Trial of ballot during decryption process

3.4.2.3 Homomorphic encryption

This was introduced by Benaloh (1987). It can be used for I-voting to provide anonymity but is less common in practice (Benaloh, 1987; Sako and Kilian, 1994; Cramer et al., 1997), yet it ensures that individuals are unable to decrypt messages using only private decryption keys. However, it requires zero knowledge proofs and does not allow multiple candidate elections. However, for each protocol there are advantages and drawbacks, therefore some systems use a mixture of protocols to overcome the latter.

Homomorphic encryption was implemented in many European Union projects (e.g. CyberVote (2008) and E-Vote (Gilberg, 2003) which is based on Paillier homomorphic encryption (Damgård, Groth and Salomonsen, 2003).

3.4.2.4 Other related cryptographic techniques

This section gives the reader brief information about cryptographic concepts and techniques used to design I-voting schemes.

A. Public key infrastructure (PKI)

Küchlin (1987) presents the basics of the PKI public key encryption and RSA encryption algorithm which ensures secure transmission of messages over insecure channels where only authorised users with the appropriate key can decrypt the encoded message. Furthermore, Küchlin (1987) presents separate algorithms for generating encryption and decryption keys and an algorithm for encryption and decryption key pairs. In public key encryption, users will have to exchange public keys, after which the user will encrypt the data with the intended recipient's public key and then the recipient can decrypt the message with the private key kept secure under any circumstances (Küchlin, 1987).

The strength of public-key cryptography lies in the fact that the asymmetric algorithm is more valuable than symmetric secret key cryptography, allowing a safe transmission of data without the need to devise a secret way of key exchange (Küchlin, 1987).

On the other hand, there are some weaknesses associated with public-key cryptography which is more computationally costly and requires a longer key than secret-key cryptography to ensure equivalent security. Keys in asymmetric cryptography are also more vulnerable to various attacks than in secret-key cryptography, such as the man-in-the-middle attack (Küchlin, 1987; Halevi and Krawczyk, 1999). According to Halevi and Krawczyk (1999), RSA algorithms were found to be susceptible to attacks in less than brute force time. Also, Vacca (2004) identified key distribution issues of PKI. On the other hand, research done by Kim et al. (2001) shows redundant complexity elaborated in the PKI certification, certificate chain determination and certificate verification.

In I-voting, PKI is used to provide secure authentication to the voters (see section 3.4.2.4. B) or to establish secure connection between the voters and the server

B. Certificate Authorities

These act as trusted third parties that verify the identity of the sender of an encrypted message and issue digital certificates as proof of authorisation. These digital certificates comprise the sender's public key, which is then exchanged with the proposed recipients. Certificate authorities have been applied in the online environment in protocols such as Secure Socket Layer (SSL) and its successor Transport Layer Security (TLS), therefore issuing digital certificates can prevent transmitted data from man-in-the-middle attacks and enhance the security in web browsing, email and other means of data exchange. (Halevi and Krawczyk, 1999).

Although certificate authorities assist in enhancing security, they can be susceptible to attackers who can succeed in cooperating with the certificate authority to gain false certificates which could then be used to impersonate each member of the information exchange, acting as a legitimate trusted entity (Halevi and Krawczyk, 1999).

C. Digital signature

This performs as a verifiable seal to confirm the authenticity of the sender and the integrity of the message. To ensure identity and integrity of messages, the sender will encrypt the message with his/her private key, then the recipient will decrypt the message with the sender's public key (Booth, 1981). A digital signature will protect the message from a man in the middle attack where, if the message has been altered during transmission, the digital seal would be broken and the recipient would realise this when verifying the seal with the sender's public key. Furthermore, it ensures the identity of the sender since only the true sender would have been able to sign the message with his or her private key (Booth, 1981).

However, in a digital signature there is a lack of inherent time stamping, therefore it is difficult to essentially separate the fake messages created by the unauthorized entity from the real ones sent before the breach. By knowing someone's private key, the unauthorised entity could send fake messages and sign them with someone else's private key. Then, successfully posing as that other person, lead the user whose private key was stolen to trust the false messages without having to regenerate a new private key (Booth, 1981). In I-voting, private keys are stored in a smart card which makes them hard to tamper with.

3.4.2.5 Comparison of I-voting schemes

This section summarises available I-voting schemes, providing a checklist review for each scheme against voting principles (see Table 3.5). This checklist was initially created by Krishna and Radha (2006) and extended by the researcher.

Table 3.5: Comparison of schemes based on voting principles

Scheme	Eligible	Private	Verifiable	Accurate	Fair	Robust	Receipt-free	Scalable	Practical
Chaum, 1981	+	CP	IV	X	X	X	X	X	X
Chaum, 1988a	+	CP\MPV	IV	X	X	X	X	X	X
Boyd, 1990	+	CP\MPV	IV	X	X	X	X	X	X
Sako and Killian, 1995	+	CP	+	X	C	X	+	X	X
Chaum, 2004	+	CP	IV\C U	C	C	C	+	+	C
Cohen and Fischer, 1985	+	CP	+	+	X	X	X	X	X
Cohen and Yung, 1986	+	CP	+	+	C	X	X	X	X
Benaloh, 1987	+	CP	+	+	C	C	X	X	
Iverson, 1992	+	CP	IV	C	C	X	X	X	C
Sako and Killian, 1994	+	CP	+	+	C	X	X	X	+
Cramer et al., 1996	+	CP	+	+	C	C	X	X	+
Cramer et al., 1997	+	CP	+	+	C	C	X	C	C
Schoenmakers, 1999	+	CP	+	+	C	C	X	X	+
Hirt and Sako, 2000	+	CP	+	+	C	C	+	X	C
Baudron et al., 2001	+	CP	+	+	C	C	+	C	C

Scheme	Eligible	Private	Verifiable	Accurate	Fair	Robust	Receipt-free	Scalable	Practical
Lee and Kim, 2002	+	CP	+	+	C	C	+	+	X
Kiayias and Yung, 2002	+	CP\MPV	+	+	C	X	X	X	+
Damgård and Jurik, 2001	+	CP	+	+	C	C	+	C	C
Fujioka et al., 1993	+	CP	IV	X	C	X	X	+	X
Baraani-Dastjerdi, 1995	+	CP	IV	C	+	C	X	X	+
Okamoto, 1997	+	CP	IV	X	+	C	+	X	X
Juang et al., 2002	+	CP	IV	C	C	C	X	+	+
Golle et al., 2002	+	CP	IV\C U	C	C	C	X	C	+
Lee et al., 2003	+	CP	+	+	C	C	+	C	X
Kiayias and Yung, 2004	+	CP	+	+	C	C	+	C	C
Juels and Jakobsson, 2002	+	CP	IV	C	C	C	+	X	X
Acquisti, 2004	+	CP	IV	C	C	C	+	X	X
Proposed Scheme, Alhamar 2011 (see Chapter 9)	+	CP\MPV	+	+	+	C	+	+	+

+ : Satisfied	X : Not satisfied	C : Conditionally satisfied	CP : Conditionally private
MPV : Maximum privacy verifiable.		IV : Individually verifiable	CU : Conditionally universal

Source: Krishna and Radha (2006), extended by researcher

3.4.3 Server-side attacks

To avoid corruption of the ballot, cryptography must be employed in the network using the Secure Socket Layer (SSL). Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (http) (Rodriguez, 2003) to prevent attackers from ‘sniffing’ or hearing network traffic. Alvarez (2005) suggests using intrusion detection systems or firewalls to block unauthorised traffic. Figure 3.10 shows the server-side attack.

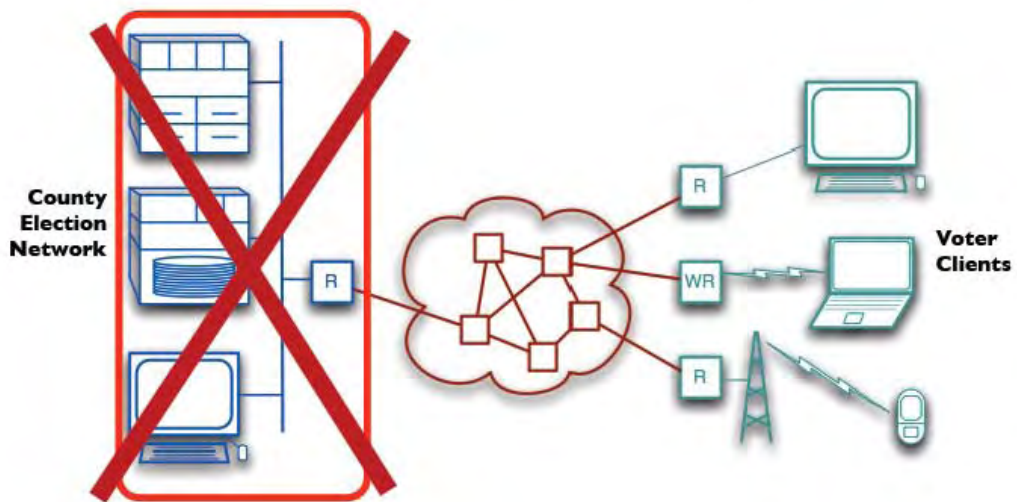


Figure 3.10: Server-side malware attack

3.4.3.1 Server-related security issues

Possible security issues arising from the server-side in I-voting are shown in Table 3.6.

Table 3.6: Possible security attacks associated with the server-side

Possible attacks	Risk	Description	Solution
DoS (Denial of service)	High	High demand on service with intention to overload the server, so legitimate users would find difficulty in or be prevented from reaching the voting website.	No effective mechanism known. However, this type of attack is done using PCs infected by viruses or malicious code with network name botnet. Solutions on the client side could eliminate the effects of this attack.
Router attacks	Medium	DoS attack on the router which forwards IP packets.	A solution to DoS attacks would also solve this attack problem.
DNS attacks	Low	DNS used to translate from IP addresses, which PCs use to reference each other (e.g. 145.132.142.15) to domain names, which people use to reference PC (e.g. www.aljazeera.net) Attacks targeting DNS could route voter to different route.	Researcher's approach (see 9.4) suggests using a customised operating system preconfigured with the voting IP address, therefore there is no need to rely on the DNS service.
Spoofing attacks	Low	The true IP address of domain name overwritten with a fake IP address.	Solved with protocol Domain Name System Security (DNSSEC) (RFC 2535 and 2931) since it allows dynamic update without online zone keys; that is, avoid storing private keys on the online server.
Insider attack	Low	A member of staff can physically have access to servers; the extent of this attack, if successful, could have full control of the election.	Solved with access control, sealed hardware equipment and use of a hardware security module (HSM) that needs more than one person key to gain access.

A. DoS attacks (indiscriminate or selective)

The idea of this attack is derived from the concept that the server has limited capacity to handle requests, where attackers use these techniques to demand more service than the server can handle. There are two main types of this attack:

A.1 DoS attack via bandwidth consumption

This attack aims to use all the server bandwidth, so voters would suffer from no bandwidth available for them. Attackers use the following protocols: UDP or ICMP ECHO packets, to reserve bandwidth.

“A simple bandwidth consumption attack can exploit the throughput limits of servers or network equipment by focusing on high packet rates – sending large numbers of small packets. High packet rate attacks typically overwhelm network equipment before the traffic reaches the limit of available bandwidth” (Householder et al., 2001).

“In practise, denial of service is often accomplished by high packet rates, not by sheer traffic volume” (Householder et al., 2001).

A.2 DoS attack via protocol attack

This kind of attack uses infected computers to start attacks on a particular source; however, installing the recent operating system patches would help minimize the problem. There are two types of attack:

(1) *“SYN (synchronised) flood is an asymmetric resource starvation attack in which the attacker floods the victim with TCP SYN packets and the victim allocates resources to accept perceived incoming connections”* (Householder et al., 2001).

(2) A Smurf attack generates network traffic on a victim network by flooding a target network via spoofed broadcast ping messages. An attacker would send an ECHO (Ping) message to be broadcast to network nodes, therefore nodes would reply to the ECHO message to the target network and as a result it would create high traffic on the targeted network (Householder et al., 2001).

A.3 Denial of service attack via a logical attack

“Logical attacks exploit vulnerabilities in network software, such as web server, or the underlying TCP/IP stack”. Examples of logical attacks are (1) Teardrop, (2) Land crafts, (3) Ping of death, (4) Naptha (Householder et al., 2001). However to overcome this problem it would be essential to ensure a reliable client machine. Users remain the weakest link in this chain of process to deploy I-voting, therefore a secure client using one of the discussed approaches would be worth trying even with the complication with usability or complexity (Householder et al., 2001).

B. DNS attacks

The extent of DoS could affect a DNS known to be vulnerable to many attacks. The company regulating the Internet DNS uses only thirteen DNS root servers. In 2002, a DoS attack successfully targeted some of the DNS servers and caused server downtime and degradation in the service. On the other hand, some companies mirror the DNS server to ensure that even if the DNS server is down, users could still access the website via a mirror server.

The extent of this attack is that voters would not be able to access the website using the DNS address so only those voters who know the IP address of their voting server could then vote. Another type of attack is DNS spoofing that over-writes the real IP address with a fake address, an attack regarded as difficult. Using DNSSEC (RFC 2535 und 2931) could overcome this problem; also, the use of digital certificates could distinguish between real and fake websites.

C. Router attacks

Internet routers are vulnerable to several attacks during forwarding of IP packets through the Internet to reach the voting server. A DoS attack on IP routers could affect a whole region from accessing the voting server; however, this would have low impact since the Internet protocol would re-route the packets to an alternative route to reach the voting server.

D. No post-auditing

In paper-based voting, secrecy of voting is guaranteed by physical protection, whereas in I-voting secrecy is susceptible to destruction by hackers. Therefore, in I-voting, secrecy should be ensured during the whole election process, no parties should be involved in the voting process or be able to manipulate the votes. Furthermore, the registration and authentication process should be defined clearly so that only eligible people can vote only once and, for secrecy, voters should not be able to verify their vote (Soder, 2002, pp.67-128). However, voters should have the ability to verify their vote casting through a print of a unique, randomly generated serial number which only shows the chosen candidate with the voter's unique signature; this will support secrecy of voting and will assist in auditing the ballot's results and prevent insider attacks (Kohono et al., 2004). Some argue that verification could reduce the risk of intimidation and vote selling. However, vote selling is actually a common and difficult abuse to control in any voting system (Anttiroiko, 2003).

Although electoral provision should ensure secrecy of vote, it is difficult to ensure that there is no external influence on it (Notton et al., 2008, pp.581-584). This risk is also high in I-voting systems. Therefore secrecy has to be related to a democratic philosophy for the election. To reduce the threat, encryption and authentication processes should allow only authorised persons to cast a vote which is then encrypted; subsequently, when gathering ballot results, only authorised persons should be allowed to gather them in a decrypted form after the voting period ends (which has the implication that voting should not be observed during the election process). Hence, in order to ensure secrecy in I-voting, the technology used for vote control should be feasible (Lazou and Papatsoris, 2000).

3.4.3.1.5 Insider attacks

This threat is considered as low risk if the election committee uses best practice methods to protect the servers from insider attack. Possible solutions are (1) sealed servers so no unauthorised physical backup or access to equipment is allowed, (2) use of physical access control to prevent unauthorised access, (3) allow a trusted third party to observe the election, (4) harden access to the server using Threshold encryption, This encryption process will guarantee the strength of the I-voting process by reducing the chance of an unauthorised person gaining access to confidential information since the private key is reconstructed and shared by several parties instead of a single person (Boneh et al., 2005).

In conclusion, this section indicates that the greatest threat is from a DoS attack on the voting server which could result in it being cut off from the Internet, for which no effective protection mechanism is known, although some of the good practice could be used to reduce the chances of this type of attack. Also, the use of a vote receipt without mentioning the voter choice would help in preventing some of the attacks described above. The client machine could act as a DRE (Direct Recording Electronic) to prevent the impact of the voting server being down due to a DoS attack, although this is not likely to be effective due to the unreliability of the client machine (Internet Policy Institute, 2001).

According to Xianju et al. (2000), some of the good practice solutions to avoid a DoS attack are as follows:

1. Filter all the packets in the network which are entering and leaving the network to prevent attacks from the neighbouring networks. *“This measure requires installing ingress and egress packet filters on all routers”* (Xianju et al., 2000).
2. Upgrade the client machine with the latest security patches and techniques to prevent, for example, the SYN flood attack. Increase the size of the connection

queue, decrease time-out waiting for the three-way handshake and employ vendor software patches to detect and circumvent the problem.

3. Disable IP broadcasting, so that the client machine will not be used as an amplifier in ICMP Flood and Smurf attacks. To prevent this attack all the neighbouring networks need to disable IP broadcasting.
4. Disable unused network services to prevent tampering and attacks.
5. Monitor traffic patterns on the network to indicate when the system is under attack, to enable protection from the attack.

The above points help in eliminating the DoS attack impact on the I-voting process. It would, therefore, be important to follow this best of practice advice in any proposed I-voting system.

3.4.4 Other implications

There are many other implications of the I-voting system, other than the risks associated with client, Internet and server-side. The following are other issues which might arise in I-voting.

3.4.4.1 Legal issues

Since I-voting was first considered, several writers have made their contributions on the legal viability of this idea. According to Carley (2008), election issues are in every way legal issues and any slight breach of the electoral law renders the election null. This claim is, however, challenged by the fact that there have been cases of breach of electoral laws without nullification of the results (Carley, 2008). In other words, it may be possible, in some cases, to manipulate results, regardless of the existence of electoral laws, and get away with it. According to Strassman (1999), the traditional way of doing things, including voting and elections, has been greatly challenged by the advent of the Internet. He further says that the delays witnessed in the implementation of technological changes in the area of voting are actually due to the legal issues surrounding it. Thornburgh and Celeste (2006), Rubin (2006) and Niemi (2008) seem to agree that there are four main areas which present the greatest concern. These are privacy, security, availability and authentication. Additionally, policy and logistics have also been identified as needing to be addressed before I-voting can be considered a success (Schaffer 2008). Some legal experts (Strassman, 1999; Friel, 2006 and Gritzalis, 2006) have advanced the view that it is actually more difficult to handle these two than the four others combined. In some parts of the world, giant steps have already been made towards an Internet-based voting system. A classic example is the first trial held in New Zealand where over 21,000 people participated in voting for shadow representatives using the Internet (Niemi 2008). The interesting thing is that due to the security-related concerns surrounding this activity, hackers were actually invited to try and get into the system in order to help identify the possible threats.

As indicated, the laws of every single country across the world have set a particular standard within which voting can and must be done. The four areas discussed form the basis of any voting system and actually constitute the major barriers that must be

overcome before I voting in any part of the world can actually be realised (Alkhelaifi et al., 2009).

Generally, the legal requirement is that privacy be accorded to every citizen during the voting process, so that voters have the opportunity to exercise their conscience ‘behind the curtain’, so to speak (Mehdi, 2001). The aim in this case is to eliminate any possibility of manipulation or coercion from interested quarters and this is done through maintenance of voter anonymity. For Metz (1996), the legal determination of privacy is that no-one should be in a position to identify a vote with a particular person and that the voters themselves should be unable to prove that their vote was cast in a particular way. However, it seems that this can only be possible in countries with a mature democracy. The challenge in this case is that anything that is done through the Internet, including voting, cannot be fully guaranteed to be free of interference (Metz, 1996). This can however be addressed by an automatic authentication and validation system which allows for automatic encryption of information to ensure that no interference is possible (Mehdi, 2001).

The security of an electoral system seeks to ensure that only voters who are eligible can actually participate. However, the Internet does not always accord the highest level of security needed (Metz, 1996). According to Gritzalis (2006), there are, therefore, possibilities of threats such as sabotage, for instance through Trojan horse software that is highly sophisticated to the point that it could actually divert the votes or change them, while viruses can be created to cause crashes of the computerised voting systems, creating a possible legal crisis, even acting as serious challenges to democracies around the world. According to Thornburgh and Celeste (2006), for a vote cast through the Internet to be valid, it must necessarily satisfy three criteria. First, it should be free from any possible alteration. Secondly, it should be impossible for anyone to eliminate a validated vote from the final tally. Finally, invalidated votes should be automatically excluded from that final tally.

For an I-voting system to be generally accepted, the uncertainties of people regarding authentication of votes cast through the Internet must be addressed. It should be

possible to identify a vote as being a real one (Glass, 1999). However, this is not an easy task, considering that the computer systems are designed by human beings and as such are capable of manipulation (Rubin, 2006).

Another major barrier that makes I-voting a challenging affair is availability. The technological infrastructure as well as the infrastructure needed for this undertaking is still largely unavailable. Everyone should be able to have reasonable access to Internet services (Thornburgh and Celeste, 2006).

Californian laws on I-voting offer a classical example of what can be considered a model I-voting system. There are a number of legal requirements that must be fulfilled before any individual can be allowed to vote through the Internet. For instance, voters are required to make a request in writing every time they wish to vote. It is illegal to request both I-voting and an absentee vote (Mehdi, 2001). The system of voter authorisation must be designed in such a way that it is possible to link the actual vote cast to the voters' register for verification. Each voter must be issued with an authentication code combined with his/her PIN in order to allow voters to authenticate themselves. Additionally, any form of advertising is disallowed on the I-voting system screens. The system should allow easy navigation while at the same time preventing any cases of over-voting (Mehdi, 2001). Generally speaking, the features of the I-voting system borrow heavily from the absentee ballot system features, making possible voters' trust in the system. The Internet voting laws in the State of California can therefore be considered best not only for California, but for other countries as well (Mehdi, 2001).

The current electoral law, namely absentee ballot system, has gained acceptance over time. This is perhaps due to its features that guarantee free and fair voting (Gritzalis, 2006). In other words, the issues discussed here as constituting the challenges of I-voting have been adequately addressed by the current legal system. The new system must therefore take an approach that is evolutionary, rather than revolutionary. This will enable it to learn from the existing laws and avoid creating vacuums in the voting process. Therefore, if the shift is to be a successful one, it ought to be gradual, but all

the principles of an absentee ballot system must be applied and maybe improved in the new system (Gritzalis, 2006).

The bringing e-transaction laws into force in Qatar was meant to open up previously unexploited possibilities. The structure and principles of these new laws have a lot to offer to the debate on the possibility of an I-voting system (Alkhelaifi et al., 2009). It would be important to understand what these laws require in order to assess whether they can actually address the challenges of I-voting. These laws can be applied successful to I-voting, because they actually address most of the challenges discussed earlier. For instance, issues of integrity, digital signature and digital signature certification, of the transmission and storage of data, of consumer protection and, more importantly, of the offences and penalties applicable to defaulters can all be successfully addressed (Alkhelaifi et al., 2009). These are provisions with extreme significance for the prospects of I-voting and, if used, can easily make it possible to vote through the Internet without raising the current challenging questions (Alkhelaifi et al., 2009).

It is concluded, therefore, that although the age of I-voting is here, it faces many challenges which must be addressed before the process can be considered to be up to the expected standard. Some of the challenges are actually not technical. Most of the already existing electoral laws need to be amended so as to accept electronic aids to the process. This can be a valuable start but the entire process must at all times be guided by integrity. The example of Qatar is a good one for setting up the technological as well as the legal infrastructure for a successful implementation of such a process.

3.4.4.2 Transparency

Although I-voting provides faster, less costly and more accurate results, people still do not trust the system. Furthermore, since the process is not clearly available, people rely on experts' evaluation of the source code.

An I-voting system should involve a high level of security, usability and trusted infrastructure, and software should be open source (Ata et al., 2004; Kitcat, 2004). The process should allow voting monitoring by trusted authorised parties and experts who carry out inspections to ensure voters' trust in the voting system and that votes are not interfered with or manipulated (Muselli, Notton and Louche, 1999; Trechsel, 2005). However, existing I-voting systems hardly ever provide an open source system (Kohono et al., 2004).

In I-voting, successful fraud could be perpetrated remotely by a single person and might have a large scale effect, whereas in paper-based voting it is hard to commit an attack on a large scale (Jefferson et al., 2004). Since, in I-voting, there is a huge chance of fraud, and since the process of voting is anonymous, it is harder to investigate cases of crime. In e-commerce, proceeds of e-crimes could be easily recovered by legal actions (Marconi, n.d). The most threatening attacks are malicious programs since they might result in a considerable damage to client machines because they can alter votes (despite the system security and compressed encryption or authentication) without being detected, since they act before the encryption and authentication are applied to the data, thus leaving no proof of fraud (Rubin, 2002). Between the client and legitimate website, attackers can act as a man-in-the-middle (Phillips and von Spakovsky, 2001), but the risk of this could be reduced by use of the secure socket layer (SSL) and digital certificates available in the website.

No detection of incidents does not necessarily mean that no successful attack has occurred, since most attackers will have carefully hidden their attacks (Rubin, 2002; Jefferson et al., 2004). They are good at tricking people, they usually exploit vulnerabilities in their victims in order to engage in an attack and, once this is achieved, the secrecy of voters could be infringed, votes could be manipulated, and even the

integrity of the election itself could be destroyed (Statements about Internet Voting from Experts, 2008).

The principles of I-voting must be categorised. Phillips and von Spakovsky (2001) state that there should be a paradigm of terms of infrastructure, communication protocols, software and a hardware platform for I-voting which guarantees people's right to vote freely and fairly through guidelines provided for all entities to follow to implement the I-voting system (Bouras, 2003), since there is a lack of understandable guidelines (Joe and Glidden, et al 2001)

According to the California Secretary of State (2000), research states that it is currently hard to replace the existing traditional voting with I-voting system since it is yet not legal or practical to develop it due to many issues associated with such a system, for example, secrecy, trust, culture, usability, etc.

Other research (US NTIA, 2000) suggests that I-voting in its first launch should be implemented along with the existing traditional voting and the use of supervised I-voting in polling stations would provide an idea of people's acceptance of such technology and the experience of it. However, supervised I-voting would reduce voters' convenience to vote remotely since it only allows voting in a supervised environment in specific polling stations (US National Telecommunications and Information Administration, 2000).

According to Trechsel (2005), open source applications are not welcome since they provide attackers with detailed information about the system design which they can use to commit their crimes by determining system weaknesses. The Netherlands reported that their I-voting had been hacked within 24 hours. Experts claimed that the open source had assisted in conducting the attack. However, Larman (2008) claims that open source systems should have a high level of security so that no one can use it maliciously although it is publicly available (Phillips and von Spakovsky, 2001). Open source can be considered good practice because security experts and the community could help

detect and correct errors, since all actions are recorded in log files (Gordi and Gosep, n.d.; Marconi, n.d.). Jan et al. (2001) noted that I-voting source code should be available through the Internet to be evaluated by experts.

Transparency can be achieved not just by technical solutions but also by enhancing government trust (Leontine, 2008).

3.4.4.3 Freedom

Voters should have the full freedom to vote without stress, interference or manipulation (Okamoto, 2007, pp. 25-35). I-voting creates significant problems regarding fraud and vote selling, which might limit the freedom and integrity of voters, whereas in postal voting they are required to sign a declaration.

Freedom of voter decision could be ensured by providing privacy for voters to vote remotely from any place, using the Internet (International for Data Protection and Telecommunication, 2001, p.86).

3.4.4.4 Equality

Since voting is a practice of democracy, equality is important, where all candidates are treated equally and all eligible voters have the right to vote. Equality is one of the main challenges for I-voting as it is a broad concept. To achieve equality many aspects have to be assured, such as eliminating the digital divide and providing usability and accessibility. Each of these aspects is now described.

A. Digital and social divide

The use of the Internet as a voting channel is argued to be available to some people who are of a relatively better standing through their access to the technology (i.e. Internet, computers and the like). Belanger and Carter (2010) concentrated on reviewing the influence of the digital divide on I-voting and proposing a model to limit digital divide issues. The model was examined against a large sample of citizens identifying that age, income, education and Internet experience have an impact on the I-voting process. Trechsel (2004) pointed out that I-voting is not yet a truly public medium. According to studies, only a small percentage of the population have access to and are regularly use the Internet (Gibson et al, 2003; Trechsel and Mendez, 2004). Moreover, Arab et al. (2001) added that this would lead citizens to face difficulties in exercising their right to vote, if such limitations were experienced in postal voting (Notton, 1999; Cramer et al., 2007). However, these studies are quickly becoming out of date as more and more people are connected to the Internet with some countries now having high speed Internet access at low cost. For example, Qatar has more than 50% of Internet users, 436,000 out of 840,926 (QSA, 2009).

One of the main difficulties facing I-voting is the social divide and the ability to adapt to new technology alongside the legacy methods; this requires effort and would be costly and time consuming, since human nature resists change and some people do not know how to interact with such new technology (Gordi and Gosep, n.d.). Also, some claim that I-voters will miss the voting experience of the traditional voting system (Barrat, 2004a; Reniu, 2005). The TruEVote project (Bruschi et al., 2002) explored people's acceptance of I-voting, focusing on technical and social matters. Workshops with various groups of citizens and politicians showed a clear acceptance of I-voting technology though there were some worries on the technical aspects of I-voting and very minor concerns on possible security risks.

Hence, this research project has aimed to consider digital and social divide issues, which describe the gap between what technologies people have and do not have. Accordingly, I-voting should be an option so voters would have the choice to vote at the polling station or through the Internet with I-voting.

B. Usability

ISO 9241-11 identifies usability as the degree to which a product can be used easily by users and attain its goals efficiently (Quesenbery et al., 2003). A user guide of how the voter would vote should be provided for voters, especially in I-voting to facilitate the voting process. Although the system should be user friendly, it would still be useful to provide easy to follow guidelines to ensure all voters would understand it, even those with novice computer knowledge (Quesenbery et al., 2003).

Since the act of voting is not frequent (e.g. in the USA, it occurs once a year), voters might be novices in dealing with the system, therefore it is important to provide one that is usable (Nurmi et al., 2001). Studies by Strassman (2000) and Larman (2008) on the usability of I voting concluded that the design should consider usability in terms of ability to start the vote, read the screen, navigate, change, review and verify votes. Moreover, Hoffman (2005) argued that I-voting should be carefully designed and implemented to assist citizens to exert their right confidently and easily. In general, applying usability in an I-voting system will develop voters' trust (Quesenbery et al., 2003). Dictson and Ray (2000) suppose that if usability issues were resolved, IT would facilitate the voting process for people.

Usability involves ease of navigation, understandability, simplicity and avoidance of complexity (Rogers, 1995; Hirt and Sako, 2000; Marche and McNiven, 2003). The structure of the system should be well defined, there should be a clear and reasonable number of options on the ballot, the paper should have a clear layout, request for verification before committing the vote, allowing citizens to be aware of the I-voting process with the ability to cast their vote efficiently with minimum skills and equipment required (Mote, 2001; Storer, 2004). An I-voting system should include a candidate description, since it plays a big role in voters' decisions about candidates (Kaldellis and Sotiraki, 1999; Komnimglou and Kaldellis, 2001). In addition, it is important to consider the relative advantages for the I-voting process in improving the standing of the existing voting system, considering accessibility and usability of vote casting (Gimpel and Schuknecht, 2003; Thomas and Streib, 2003; Chen, 2008). According to Chaum (2002), training is required for I-voters to facilitate the voting process,

especially for voters who find it difficult to vote. As a result, it is crucial to discover the views of the Qatar government and citizens before adopting the I-voting innovation (Rogers, 1995). Compatibility defines the suitability of innovation in relation to needs, principles, knowledge and beliefs. This was considered in this thesis to illustrate Qataris' awareness of the pleasant nature of I-voting in their society.

According to Hall and Alvarez (2004), young citizens in the age group (18-27) found I-voting more comfortable to use compared to older age groups. Also, it was discovered that citizens who use the Internet regularly for communication and electronic transactions appreciated the simplicity of I-voting (Carter and Belanger, 2005).

The research community have assumed that, in general, young and educated people have more enhanced computer knowledge than less educated and older people (Manna and Smith, 2003; Smith et al., 2003; Bonsor, 2004; Smith and Manna, 2005). Moreover, to enhance participation in I-voting, the system should be cheap, fast, usable and as accessible as possible, especially for people with disabilities (Alvarez, 2005).

C. Accessibility

I-voting should ensure equal accessibility, without differentiating between candidates. It should treat all candidates equally and should ensure transparency and guarantee that voting results are not interfered with (Kaldellis et al., 2004, pp.187-203). Voting system should provide an equal accessibility, where the system is easy to use regardless of voters' computer knowledge, education, age or disability. In 1965, the USA Voting Right Act required the avoidance of discrimination between people (Bonsor, 2004), but this might prevent establishment of I-voting since it uses Internet technology which might be inaccessible to some citizens and this is a kind of discrimination.

According to Kaldellis and Doumouliakas (2000) the opportunity for equal access in I-voting is not ensured, while in online access only those who benefit from it and who have some computer knowledge can vote, leading to unequal accessibility to the voting

system. Norris (2001) noted that this limitation of access would increase the issues of digital and social divide (see Section 3.5.4.1).

Since accessibility is one of the main advantages of I-voting, it must be ensured that voters can vote from anywhere as long they have access to the internet whether through Ethernet, dial-up connection or wireless networks. Accessibility should be defined earlier according to the election requirement for internal access within network organization, national or international access. Furthermore, I-voting provides flexibility where some elections might give voters the ability to use varies devices (e.g. PC, mobile phones, PDA) and to use different ballot formats.

Additionally, the usability of I-voting systems is a main concern especially for disabled voters where a special tool and/or software might be included to help them to cast their votes. The use of a virtual environment could give voters the feel of the voting experience, but this would require a high Internet speed for fast browsing (Morgan et al., 2001).

Dictson and Ray (2000) suggested providing a public Internet access in the country to enhance I-voting participation, especially for people who find it difficult to have Internet access. However, there is still another limitation, the level of literacy of people in general and computer literacy in particular. Some experts advocate I-voting based on the number of Internet users within their country without taking into consideration users' knowledge of how to use such technology (Demunter, 2005).

3.5 I-Voting Adoption

Many organisations provide electronic elections, for instance the IEEE and governments such as the United States and Australia. Despite the successful and unsuccessful experience and challenges and limitations of I-voting, still many organisations are inspired by e-voting. I-voting is a new process and will be extremely strange to almost all voters. It is necessary to consider how such a system and in particular how a system can be constructed according to the prescriptions of the model proposed in this thesis, should be introduced into general use. This section is concerned with that question.

The need for acceptance by the population suggests I-voting should be introduced gradually, for instance starting with poll site voting and then kiosk I-voting, until it is accepted by the community and people get used to it. When associated legal certification issues are resolved in the future, I-voting can start.

The technology of smart card compressed encryption and authentication can be used in I-voting since it provides a higher level of security, contains a huge amount of data and enables services to be integrated (Simons and Graham, 2008; Rivest, Shamir and Adleman, 2008). The use of the smart card reduces time and cost associated with huge amounts of paper work and labour involved in elections (Lin, Hwang and Chang, 2003). Hence, it is estimated that the revenue of the smart card would be increased by 30%.

A survey of UK voters in 2002 concluded that a huge percentage of voters (87%) believed online voting would be preferred for the next general election so people can vote remotely from anywhere (Touch Plc, 2002)

According to Carter and Belanger (2005), the proposed e-government adaptation model depends on the TAM (technology adoption model), DOI (diffusion of innovation) and the trust of the Internet and government. Although this model provides a valuable contribution for e-government, it is practical for I-voting adaptation, since I-voting can be considered to be part of e-government.

Davis (1989) uses TAM to examine the adoption of e-commerce and e-government. TAM involves Perceived Usefulness and Perceived Ease Of Use, which affect users' acceptance of the system, whereas the DOI consists of compatibility, relative advantage, image and complexity (Davis, 1989).

The aim of this thesis is to develop an I-voting adaptation framework for Qatar employing the proposal of Carter and Belanger's (2005) e-government adoption model, considering the cultural and country-specific factors for the State of Qatar.

In the context of I-voting, Perceived Usefulness defines Qataris' insight of the efficiency of process in election practice, also Perceived Ease Of Use describes the offer of a usable system for users. This is important to consider, especially for I-voting, since the users of the system are people with different backgrounds, some with insufficient computer literacy.

All of the above factors, if considered, will assist in enhancing citizens' interest in e-government (Carter and Belanger, 2005) and this suggests they will have the same effect for I-voting.

3.5.1 Trust of government and the Internet

If I-voting is to be employed in deciding matters of national importance, for example the constitution of the next legal government, it is necessary for the Internet to be trusted (because it is the medium through which I-voting is conducted) and for governments to be trusted. This is the subject of this section.

Trust is an initial requirement for I-voting adaptation. A survey by Los Alamos National Laboratory in 1999 concluded that 1,000 adults trusted businesses more than government (ITAA, 2000).

Sofia (2009) claims that e-government will enhance the trust between citizens and government if transparency is applied. However, McKnight (2002) commented that there is no clear evidence that e-government is associated with trust having found that visiting government websites to retrieve contact or information has no relation to trust. However, it can be argued that usage of e-government services with transparency would increase trust in government.

According to Sofia (2009), any mistakes occurring within the e-government service will have a negative influence on citizens' trust in government. Therefore, government should move gradually towards developing the trust of its citizens and, once this is achieved, it will play a big role in adoption of I-voting. To establish trust should involve trusted parties, such as government officials, politicians, legislators and expert system developers, to support the I-voting system.

Jillbert and Musaruddin (2003) argued that it is easier to use I-voting in developed rather than in developing countries, since it requires a huge amount of effort and time and most developing countries have an inadequate national budget to adopt I-voting. Also, it would require training and education of people on how to use the system. Carter and Belanger (2005) reported that the client platform was an untrusted entity which is hard to secure with current malicious software and viruses.

In general, most voter verifiable protocols still fail to resolve the intimidation that voters might experience. Helbach (2007) suggests multiple vote casting is a good method to protect against intimidation. However, social and political scientists are still doubtful about using I-voting. Thus, Ewert et al.(2006) stated that election-voting participation would not necessarily be increased when voters have the flexibility to vote remotely from anywhere and they also added that reduction of cost is not an issue.

3.6 Discussion

I-voting has attracted a great attention as a result of growth in e-government and digital communication. The main characteristics of successful I-voting are security, privacy, accuracy and mobility. Internet voting still suffers from insecure computer networks. However, the literature shows that the major problem with I-voting is that the client machine is not supervised, therefore it might be infected with malicious code or viruses which can affect voting, although there are some ways to avoid this but until now it has been considered too costly. One method would be connect each voter's machine through a VPN (virtual private network); this is considered secure but requires a large budget and computer literacy. However, one of the simple methods distributes voting responsibility and functions to the voters.

Transparency in I-voting has received considerable attention, using a voting verification method as one way of solving this problem. Verification should show voting success or failure when proving correctness of voting. Moreover, this builds trust in a system, since voters can verify the integrity of system functions and contribute to election observation; although the goal of coercion resistance cannot be guaranteed. On the other hand, Helbach (2008) has argued that multiple vote casts could be used to eliminate vote selling by allowing voters to vote again and again; however, this could yield many fraud cases in which someone could sell his/ her vote many times. In practice, current law does not promote multiple casts. There may also be the effect that, instead of taking a decision on the basis of accurate long-term and personal perspectives, voters may begin to respond to current affairs and the results of surveys. The practice of multiple casts is not common for democratic elections, so for these reasons, its use is not further considered in this research.

The code voting method has shown its worth in achieving integrity and privacy through secret ballots, where an attacker would need to get hold of the code sheet to translate voter choices. Furthermore, the use of smart cards and voting coding together guarantees a reasonable degree of security where, instead of storing voting code sheets in a central database, smart cards have the necessary storage capability.

Adopting both code voting and vote verification in future Internet voting is desirable. Vote verification needs appropriate platforms for secure use but trusted computing guarantees increasing confidence in the platforms' integrity and faithfulness. Moreover, trusted computing could simplify voting adoption since it provides trustworthy clients. However, the trusted computing approach does not seem to be good practice for now, since accurate performance cannot be verified on its own.

Election law is an Achilles' heel in I-voting, since the existing law was written for paper-based voting. There is a huge difference in the legal requirements between traditional and I-voting methods. For example, traditional voting would give the voter the ability to participate in an election without selecting a candidate and an important addition in Internet voting is that the voter would have a receipt to be used for appeal whereas traditional voting does not provide one.

The secrecy aspects remain challenging, although researchers suggest some best practice methods, but it still remains impossible to fully guarantee end-to-end protection. In order to vote in absence, confidentiality may have been infected because it is a form of additional vote and officially associated with strict regulations. Here, the benefits are more important than the losses. If I-voting offers a complement to absentee voting, it must be measured according to the same rules.

The uncertainty of people's acceptance of I-voting suggest that more needs to be learned about voters attitudes and acceptance of the plans, including methods for fraud protection and for verification. Experiments and trials need to be carried out, preferably during elections that are not legally binding (such as workers councils, universities, boards or councils of social security institutions). Here, the methods proposed for further evaluation are within the limits of adequate control and the risk is limited.

Future work can be summarised into three main phases:

- 1) First, determining people's acceptance of I-voting using a variety of methods (survey, interview and experiments).
- 2) Second, measuring the voter's security awareness to provide an accepted solution to bribery and coercion problems.
- 3) Third, real time and practical testing outside the laboratory of the released version of the system in order to report on its performance and reliability.

3.7 Conclusion

Although there are many advantages of I-voting, some disadvantages appear to influence negatively on voting experience. Gerck (2000) states that the main concerns with I-voting are limitation of access, requirements for training people to use the system, lack of a paper examination review to ensure integrity of voting process and political risk. The lack of paper-examination review could be resolved by examining the log files in which all actions are recorded. According to Wolosik (2004), in a personal interview, I-voting candidates were not able to observe voter practice, and this prevented them from exercising their right. Moreover, he commented that I-voting might be implemented in the future only if issues associated with I-voting are resolved. Therefore, those disadvantages and possible issues and attacks in client, Internet and server- side have to be considered carefully.

The issues reported varied from country to country according to the country specific factors. There is no research in I-voting in the State of Qatar, this identifies the need to do some research to discover the possibility of having I-voting in this part of the world. Each country has used a different model to introduce I-voting, and this shows that each country has its own criteria and characteristics which have an effect on the design of I-voting system based on resources available. Consequently, issues associated with I-voting in Qatar might be different to those experienced in other countries and, therefore, there is the need for investigating how to reduce all possible issues and for developing an effective I-voting model for Qatar taking into consideration the country factors and cultural effect to introduce an effective I-voting experience.

This identifies the need to identify possible I-voting protocols and solutions and build a combination of protocols that suits Qatar. The majority of research on I-voting has not taken account of user input in introducing I-voting which will create a problem in getting people's acceptance of such new technology. Therefore, in this research, cultural and community factors will be investigated to provide an effective introduction to I-voting in the Qatar community.

Chapter 4: Research Methodology

This chapter summarises best practice in regard to research philosophy, strategy, approach and data collection methods. Hence, a justification of the suitable research methodologies for this research is presented in this chapter to satisfy the aim and objectives stated in Chapter 1.

4.1 Research Philosophy

Any researcher needs to address a project from a particular philosophical stance. An information system (IS) project thus requires a research philosophy based on the nature of the project, whether it constitutes research in natural or in social science. According to Crossan (2003), research philosophy helps in clarifying research design and in evaluating different methods so that the appropriate choice is made. On the other hand, research philosophies employ two different approaches: epistemology (what is known to be true) and doxology (what is believed to be true). Positivist/scientific (positivism) and anti-positivist/interpretivist (interpretivism) are the common research stances encountered in research in the natural and social sciences (Galliers, 1992).

4.1.1 Positivism

Many researchers have found that the positivist position fits best for IS research (Galliers, 1992; Miles and Huberman, 1994; Yin, 1994; Walsham, 1995; Themistocleous, 2002). According to Orlikowski and Bardoudi (1991), about 97% of IS research is based on such a stance. Positivism started to become more popular in the late 1970s (Dickson and DeSanctis, 1990, cited by Jackson and Scott, 2001) and is inspired by the fact that reality is independent of the individual's thoughts. In another sense, positivists consider that knowledge can be developed through the observation or experience of real world events. Positivists deal with proven facts based on measurement and experiments; mathematical and scientific theory thus provide good examples.

4.1.2 Interpretivism

In contrast to positivism, the interpretivist approach is *'aimed at producing an understanding of the context of the information system, and the process whereby the information system influences and is influenced by the context'* (Walsham, 1993, pp. 4-5). Interpretivism underlies studies of phenomena based on empirical observation and social interaction with the community (Myers, 1997). Interviews and surveys are common methods of data collection in this approach. In addition, interpretivism could influence the researcher and lead to definition of a solution to the phenomena (Galliers, 1992; Miles and Huberman, 1994). On the other hand, people's opinions and observations reflect their views and beliefs which might not reflect the reality, so research should be interactive to enable the researcher to get to know the interviewees opinions better. Social research is a wide-open subject where researchers can obtain totally different results for the same subjects.

4.1.3 Selection of Research Philosophy

Some researchers advise the use of both approaches in order to achieve quality research because of the complexity of real world problems where facts and social context are a control variable (Benbasat, 1984; Kaplan and Duchon, 1988; Galliers, 1992; Pervan, 1994).

I-voting is a topic of increasing interest in the research field and therefore researchers should consider technological developments along with social aspects of the community (government or citizens) (Sarker and Lee, 1998).

This research examines the possibility of implementing I-voting in Qatar, considering whether people would accept such new technology and whether resources are available to implement it. Therefore, positivism and interpretivism are both invoked in this research to investigate its feasibility in terms of technical facility and social acceptance of I-voting.

4.2 Research approach

Research approaches adopted in the light of the researcher's philosophical position are essential in any research since they are used for planning the research methodology. Iivari (1991) identified three such approaches: constructive, nomothetic and idiographic, as shown in Table 4.1.

Table 4.1: Three approaches to research (Iivari, 1991)

Constructive Research	Nomothetic Research	Idiographic Research
1. Conceptual development of frameworks	1. Formal mathematical analysis	1. Case studies
2. Technical development of frameworks	2. Experiments: laboratory and field	2. Action research
	3. Field studies and surveys	

Constructive research is concerned with developing and refining frameworks by means of conceptual and technical methods (Cornford and Smithson, 1996). Nomothetic research is described as a tendency to generalize and it is a common approach within the natural sciences for the natural sciences. It investigates objective phenomena in general through field studies in order to achieve the research objectives (Burrell and Morgan, 1979; Iivari, 1991).

Idiographic research is described as a tendency to specify and it is typical for the humanities. It explores a particular case study or phenomenon, which might be supported by action research in the field to provide an effective outcome. It also describes the effort to understand the meaning of dependent, unique, and often subjective phenomena (Cornford and Smithson, 1996).

Myers (1997) has described research approaches as objective and subjective. The former involves prediction of the case instead of control over the situation in the field, which is what subjective research aims to do. In objective research, the researcher is independent of the fieldwork but in subjective research the researcher is involved

directly in the fieldwork. Basically, objective research studies the case from the outside whereas subjective research studies it from the inside, leading to a more effective outcome. In addition, Myers described quantitative research as appropriate for natural sciences' research where quantity and numerical data lead to valuable findings, whereas qualitative research suits social sciences' research where qualitative data and information gathered lead to effective results.

Miles and Huberman (1994, p.40) state that qualitative methods usually lead to direct outcomes such as one/zero or true/false; qualitative research is more investigative and leads to more informative outcomes and it therefore forms the basis for many research projects.

According to Firestone (1987, 14-19), *'Quantitative studies "persuade" the reader through de-emphasising individual judgement and stressing the use of established procedures, leading to more precise and generalizable results. On the other hand, qualitative research persuades through rich depiction and strategic comparison across cases, thereby overcoming the "abstraction" inherent in quantitative studies.'*

Dedrick and West (2003) propose the use of qualitative study for developing an effective framework. In contrast, Miles and Huberman's (1994) view is that researchers should use quantitative methods for investigating and proving a particular hypothesis. Furthermore, Sieber (1973) has reported the effectiveness of using both quantitative and qualitative methods to provide in-depth analysis of the topic.

In this research, a combination of constructive, nomothetic and idiographic research is applied subjectively as appropriate and in response to available resources. Since I-voting in Qatar is a new topic, not covered before, this inspired the researcher to investigate it through a combination of various approaches, which enrich the research and provide comprehensive findings. Both quantitative and qualitative methods are used in analysing the data gathered to provide a superior research approach where the ultimate benefit of each method is derived and each is used to support the others.

4.3 Research Design

Research design describes and identifies the process of data gathering in any research (Gallier, 1992). Many researchers have identified different methods of research design which could be used to create richer research. A summary of the methods is given in Table 4.2. (Galliers, 1992; Alavi, 1994; Cavaye, 1996; Remenyi and Williams, 1996; Hussey and Hussey, 1997; Leedy and Ormrod, 2001).

Table 4.2: Research design

Research Design	Explanation
Field Study	Researcher acts as observer involved in field of study and aims to achieve defined research objectives by applying specific techniques of data collection in the organisation.
Action Research	The researcher both observes and contributes to the organisation to investigate and solve a phenomena in field experiments and by shared partnerships having control over variables (Denscombe, 2002; Rapoport, 1970). It has the following characteristics: Practical, Change, Cyclical process and Participation.
Ethnographic Research	The researcher attempts to investigate phenomena through the understanding of society and human activities. Ethnographic research could involve various methods of data collection such as interviews and questionnaires. It is based on observing patterns of human activity and societies where the researcher could draw conclusions from participants' activities and views.
Case Studies	The researcher aims to investigate existing phenomenon embedded within a specific context, and utilizes various methods, usually a social phenomena using various methods of data gathering such as experiments, surveys, and archival analysis (Stone, 1978; Benbasat, 1984, 1985; Kaplan, 1985 cited in Benbasat et al., 1987 ;Yin, 1989).
Survey	<p>These are one of the most common methods of gathering data (Weisberg and Bowen, 1977). Creswell (2003) states that surveys include cross-sectional and longitudinal studies using questionnaires or structured interviews with representative sample of population.</p> <p>Sekaran (1992) defined cross-sectional surveys as data collected just once over a given period of time, whereas in longitudinal surveys data are collected more than once at regular intervals.</p> <p>Surveys involve several stages, from identifying the sample and developing the survey questions to administering them and analysing the data gathered qualitatively and quantitatively and finally drawing conclusions about the population under study (Thomas, 1996).</p>
Experiment	This is a common method of data gathering which could be applied both in natural and social science. Experiments involve practical processes and

Research Design	Explanation
	specific measurements applied under certain conditions, either in a controlled laboratory or as a real world event, aimed at the study of a specific subject, theory or phenomenon.
Modelling	This involves creating and/or investigating a specific model in order to improve it to enhance performance and obtain beneficial results, or could be used just to understand the situation.
Grounded Theory	This research is based on in-depth analysis of a combination of data gathered using a series of methods to identify and conclude with theory based on all findings.
Operational Research	This is based on examining operational activities in order to optimise them in the pursuit of set objectives. This type of research is common in economics (Leedy and Ormrod, 2001; Saunders, 2000).
Archival Research	This is based on archival data gathered from historical events

Yin (1989) summarises some empirical studies based on interpreting real world events (see Table 4.3).

Table 4.3: Relevant situations for different research strategies (from Yin, 1989)

Strategy	Form of research Question	Requires Control Over Behavioural Event?	Focuses on Contemporary Events?
Experiment	How, why	Yes	Yes
Survey	Who, what, where, how many, how much	No	Yes
Archival analysis (e.g. economic study)	Who, what, where, how many, how much	No	Yes
History	How, why	No	No
Case study	How, why	No	Yes

In this research, a mixture of research designs is chosen to achieve the research objectives. The thesis is based on a case study of I-voting in a particular part of the world, the State of Qatar, and to investigate this case, a wide variety of methods will be employed including experiments and surveys, and interviews and questionnaires were based on specific and representative participants. In addition, the thesis involves developing a model to study a method to improve the existing voting process (paper-based) in Qatar by adopting I-voting technology. Furthermore, it contains action research not only to develop I-voting but also to apply it in reality by getting support from responsible organisations. However, it was hard for the project to be applied fully in Qatar owing to the sensitivity and the confidentiality of voting as a democratic process, so a demonstration of I-voting was used to examine the effectiveness of I-voting and people's acceptance of such new technology.

Table 4.4 details the research objectives and the research design applied towards their achievement.

Table 4.4: Research design and research objectives

Research objectives	Research design
1. To review the literature to determine the basic requirements for a democratic voting system and I-voting to support such a system and, hence, to form a set of criteria to act as a checklist to test the adequacy and acceptability of any existing or proposed system. Furthermore, to examine different ways of voting in a democratic environment, and to assess each method using the criteria established to determine the strength of the case for using I-voting. 2. To review world-wide experience of I-voting adoption, to highlight the successes and failures, and to address critical issues associated with their experience. Also, to review literature to discover sociological and technical obstacles to adoption of such technology and to investigate potential solutions to overcome I-voting challenges. 3. To investigate and define the best practice research methodology to carry out this research. 4. To investigate the readiness of Qatar in terms of technical and non-technical aspects such as cultural, national and other country-related variables that might motivate the development or usage of I-voting in Qatar by means of literature and interviews.	Literature review
5. To assess, by means of questionnaires and interviews, the confidence and willingness of Qatari citizens to take part in the initiative of I-voting, and to reveal the barriers that would inhibit I-voting in Qatar.	Case study, Literature review, Surveys, Interviews, Experiments

Research objectives	Research design
<p>6. To assess by means of experiment, questionnaire and interview of the Qatari people a prototype of I-voting for Qatar elections, to obtain a rich picture of people's opinions and problems encountered while engaging in the voting process. Also, to test the effectiveness of the prototype solution in overcoming existing I-voting challenges and satisfaction of Qatar election requirements. Furthermore, to make a comparison between the Qatar experiment results and those of Estonia's experience with I-voting to measure success or failure of the Qatar experiment in overcoming the Estonia's problems with I-voting.</p> <p>7. To investigate the security risks that might appear due to lack of awareness of information security on the client side, to measure the level of awareness of Qatari people on the client side of I-voting to propose appropriate methods for solving the problem.</p>	Surveys, Interviews, Experiments
<p>8. To design an effective I-voting model for the State of Qatar, by combining available technology and best practice to overcome I-voting challenges.</p> <p>9. To test the applicability of the proposed model for overcoming the challenges of I-voting in the State of Qatar by means of simulation, experiments and expert opinion.</p>	Modelling Findings based on qualitative/quantitative analysis
<p>10. To propose, from the above findings, effective recommendations for the Qatar government to help in introducing I-voting in Qatar society.</p>	Action research

4.4 Data Sampling Method

To provide a robust piece of research, data needs to be gathered from a representative sample of the population. Therefore it is important to define the appropriate data sampling method applied for the research. Sekaran (1992) has classified sampling methods into probability and non-probability sampling. A summary of the methods is given in Table 4.5.

Table 4.5: Sampling methods

Probability sampling	
Simple random sampling	Samples selected randomly
Complex probability sampling	<p><i>Systematic sampling</i>: Random selection of samples of population, every nth element.</p> <p><i>Stratified random sampling</i>: Population divided into groups known according to defined criteria (e.g. geographical areas or age groups) and then random selection of a sample from each group.</p> <p><i>Cluster sampling</i>: Population divided into groups based on different criteria (e.g. hobbies, religion, etc.), then a random selection of the sample from each group.</p> <p><i>Area sampling</i>: Associated with regions, involves random selection of samples from different regions (e.g. countries and villages).</p> <p><i>Double sampling</i>: Sub-sample chosen from the first sample for further investigation to clarify results.</p>
Non-probability sampling	
Convenience sampling	The researcher takes advantage of his/her convenient and available resources (e.g. contacts and position) to gather samples of participants for research.
Purposive sampling	The researcher chooses participants carefully to obtain the best sample able to provide the required information.

In this research, both probability and non-probability sampling are used as appropriate in different data collection methods. In particular, stratified random sampling is used for questionnaires and experiments, whereas purposive sampling is used for interviews. Convenience sampling is used mainly in experiments where obtaining participant consent was a challenge and therefore the researcher took advantage of colleagues and friends to obtain consent to participate in the evaluation of the I-voting demonstration.

4.5 Research Process

Since literature on I-voting in Qatar was found to be lacking, there was a need to define a planned research methodology to satisfy the research objectives. A review of I-voting in Qatar was therefore based on reviewing voting experience in the country using a questionnaire and interviews with domain experts to study the possibility and willingness to introduce I-voting in Qatar. The entire outcome from all data collection methods was analysed qualitatively and quantitatively. Consequently, an experiment was used to explore people's acceptance of I-voting technology by demonstrating to them a standalone I-voting system. Later, an I-voting model was proposed, a prototype of which was evaluated by a sample of experts and the general public to ensure its effectiveness and fulfilment of voting principles. Finally, based on the conclusions drawn from the data collected, some effective recommendations were proposed for the Qatar government to adopt I-voting. These recommendations were then reviewed by experts in the field and were also assessed for their applicability in other countries. Figure 4.1 depicts the research process.

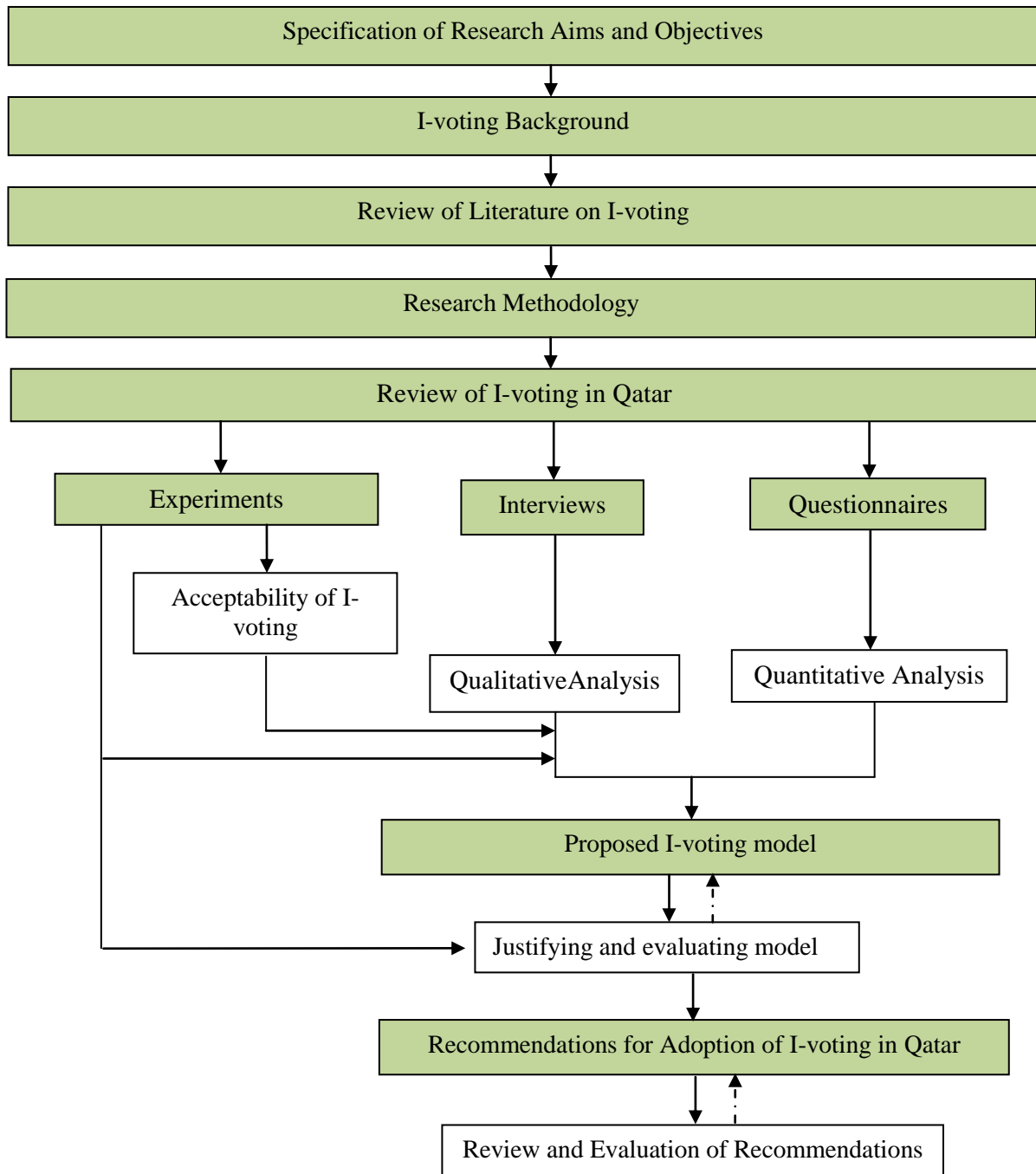


Figure 4.1: Research process

4.6 Summary

This chapter has summarised the research methodology which forms the basis of the research. The research philosophy, approach and design were reviewed and selected carefully to suit the research and achieve its objectives effectively. Positivist and interpretivist philosophy both underlie this research in its investigation of the technological and social aspects of I-voting in Qatar. In addition, a combination of research approaches, constructive, nomothetic and idiographic, are applied subjectively.

To achieve the research objectives effectively, various research designs are found to be appropriate, including a case study of I-voting in Qatar, modelling the present paper-based voting system electronically and, finally, applying I-voting in Qatar based on action research. Moreover, different methods of data collection are applied, including surveys and experiments in which participants are chosen to represent the population by means of stratified random sampling, purposive sampling and convenience sampling. Finally, the data gathered are analysed qualitatively and quantitatively to derive valuable and effective findings.

Chapter 5 Qatar Toward Internet voting

This chapter provides an empirical study on the feasibility of I-voting in Qatar taking into account the country and citizens' readiness along with possible barriers for I-voting. This chapter satisfies Objectives 4 and 5.

5.1 Background

Qatar is a very small Middle East Arab country which is also recognised as the State of Qatar and, in official terms, as an Emirate. It occupies a small area of approximately 11,500 sq. km, about double the area of Lincolnshire, on the northeast coast of the Arabian Peninsula and on the border of Saudi Arabia to the south, and is otherwise surrounded by the Persian Gulf (QSA, 2009). A passage from the latter separates Qatar from the nearest island, the nation state of Bahrain. Although Qatar is a small nation with a population of approximately 1.4 million (about double that of Leeds), it is estimated that native Qataris comprise approximately 200,000 of the population, it has the third largest gas reserves and highest per capita income in the world (QSA, 2009). It has been ruled by the Al-Thani Family since the 18th century (Bahry, 1999; Ministry of Foreign Affairs, 2007a).

Qatar has gone through enormous changes in the past few decades. There was a huge expectation of modernisation in the country but the western values have inundated Qatar with all kinds of modern technology. This became a major reason for a gap between the generations and also for losing some traditional values, especially among the younger generation (BTI, 2010). Qatar was once counted among the poorer countries of the world with a very small population but, with the discovery of its oil in the year 1940, it started on its way to modernisation. Along with economic growth, there has been much progress in human rights and politics. Qatar became independent from the UK on 3 September 1971 and opted to continue with the hereditary form of government maintained by the Al-Thani family for many years (Bahry, 1999; CIA, 2008a).

The Emir is considered as a supreme leader of the nation and of any institution or individual, though in practice his rule is not so absolute. He is bound completely by Islamic perceptions and all his decisions regarding his public and private life are affected by the religious and ethical values of Islam (BTI, 2010). There is a separate advisory body named the Al-Shura Council, which is partially elected and holds the right to debate government decisions before they are approved.

There were 16 Council of Ministers' posts in Qatar in 1992 and around 10 were occupied by the Al-Thani family. Qatar generates the highest per capita income in the world and, for this reason, there is no state tax for individuals and, at the same time, health care and education are provided free of charge for all Qataris (Ministry of Foreign Affairs, 2007a).

All the major decisions over the executive and legislative affairs in Qatar are made by the Emir. All political parties and labour unions were banned in 1976 and no elections were held until 1999 when the first municipal elections took place for the 29 member Central Municipal Council. For the first time in the history of the Gulf countries, women were allowed to vote and also to stand for office (Khalaf and Luciani, 2008).

The ruling Al-Thani family continued to hold power even after the declaration of independence in 1971. The Emir was to be considered as the head of state but all rights to rule Qatar were to reside with the Al-Thani family. This was the time when Qatar started developing its political abilities and moving from a traditional society to being a modern welfare state. Later on, government departments were established to meet the needs of social and economic progress (BTI, 2010). The basic Law of Qatar (1970) was rooted in the Wahhabi Heritage and the provisional constitution allowed the existing system of traditional rule to continue and granted extensive powers to the Emir to rule the country. He was also granted the right to appoint and dismiss any of the Council ministers (Ministry of Foreign Affairs, 2007a).

The first political elections took place in 1999, and subsequently in 2003 and then in 2007. Later on, in March 2003, the Emir, Sheikh Hamad bin Khalifa bin Hamad Al-Thani, wanted Qatari society to get further involved in politics as this could help the state to achieve a modernised democracy and also create strength and leadership skills in Qatari employees. A new constitution, accepted in a public referendum with 96.6% participation in 2003, proposed parliamentary elections with two-thirds of the members (30 out of 45) elected by citizens and the remaining 15 assigned by the Emir. Involvement of the people would provide training in all the areas important for parliamentary elections which were originally scheduled for 2004 but have been postponed to 2012 due to administrative issues. However, a new election law was approved in May 2008 which should address all problems delaying the election. To the author's knowledge from personal contact, the government has started working on developing an E-voting system (Khalaf and Luciani, 2008; BTI, 2010). Although parliamentary elections have not yet taken place, this would be significant progress to real democracy in Qatar.

According to Amiri Diwan (2009), Shaikh Hamad Bin Khalifa Al-Thani stated, *"We are on the threshold of a new epoch overlooking the 21st century where we aspire to attain the status befitting us."*

5.2 Voting experience in Qatar

In order to understand the voting system in a country, it is useful to first understand its political system and its governing criteria. Qatar is a politically stable nation. It does not have a well-defined democracy or a democratic government where the people choose their leaders, but follows a system of governance where a single head or a single leader controls the entire country and its affairs (BTI, 2010). The head of the country, the Emir, has complete control over the country and is solely responsible for the running of the nation. He is answerable only to a few, now 15 in number, of his close associates who constitute his cabinet or council (Bahry, 1999).

In the first municipal council elections in 1999, 248 candidates have participated, including six women, who were contesting for a 4-year term. These elections witnessed a participation of approximately 22,000 people (55% of eligible voters) who exercised their voting rights for the first time in Qatar's political history. The success of these elections built the foundation for a strong political base in the country (Bahry, 1999) which experienced its subsequent municipal voting in the years 2003 and 2007.

In contrast to the 248 candidates in the first elections in 1999, the second municipal elections on 7 April 2003 saw only 78 contestants for the 29 seats. Four of them were unopposed, out of which three were female candidates who ran for top positions. The elections of 2003 thus saw the country's first female contestant to occupy a seat. Shaikha Yousef Hassan Al-Jufairi won the elections when her counterparts withdrew. However, one major setback which became the highlight of these elections was the poor voter turnout ratio. In contrast to the earlier or the first municipal elections which showed a voter participation of around 55%, the second elections of 2003 saw a voter turnout ratio of a mere 30% of the voting public (Bahry, 2010).

A few variables could be behind the low turnout: (1) municipal elections do not change things in national government, (2) the inconvenience of the voting method, and (3) complacency. Complacency is a characteristic of Qatar culture (BTI, 2010), and this would mean voters are willing to vote only if it is easy, without having to queue for a long time or having to take part in a sequence of procedures to record their vote. Internet voting could, therefore, be useful to encourage voter participation.

Voting in the third municipal elections took place on 1 April 2007 and saw an increased performance from the election point of view. These elections could be regarded as more successful than those of 2003 due to the increased number of candidates who stood, in addition to the increased percentage of voters who exercised their voting rights. The 2007 elections had around 120 candidates in contrast to a mere 78 in 2003. Two contestants were unopposed in the elections which also returned three of the female candidates who contested the 29 seats. Shaikha Al-Jufairi became the only female contestant to occupy a leading position in the country for the second time when she

defeated her male counterparts with a huge margin of 90% of the vote. These elections also witnessed a greater voter turnout ratio of more than 50%. The government of Qatar played a prominent role in supporting the smooth running of the elections and special teams were formed to supervise the elections in accordance with the law of the country (Khalaf and Luciani, 2008).

5.3 Corruption experience

According to the *Oxford Advanced Learner's Dictionary* (Hornby, 1995), 'corruption' means 'corrupting or 'being corrupted'. In any sphere of influence, this implies dishonest interference with the intended agenda of the matter or creating illegal defaults in the process, often with concealed financial inducement. Corruption is a widely present phenomenon in many fields and in many countries, as revealed by journalistic and other more formal investigations. It can take various forms, such as political corruption, data corruption, corruption in the various public services, etc., typically based on bribery and the granting of favours. Any type of corruption is harmful for the process or service which is intended to be carried out for the benefit of individuals or the general public. The Qatar constitution, in Articles 129-131 and 134, declares assurance of independence of the judiciary and of each single judge; accordingly, in 1999, a Court of Cassation and the Supreme Judiciary Council were established. Later, in 2002, an independent public prosecution system was established, followed by an Administrative Court and a Constitutional Court in 2007, thus emphasising a clear development in the independence of the judicial system. In contrast, in 2002, Foreign Minister Sheikh Hamad bin Jasim Al Thani was accused of accepting irregular payments from a British defence company; however, the investigation was terminated and the case was most likely settled out of court. Furthermore, in 2005, three senior figures including two ministers were dismissed from employment as a result of fraudulent activities. This provides strong evidence of improving transparency and accountability and an example of separation between public funds and the royal family.

Despite all challenges, Qatar has defeated corruption by a series of actions, such as being a signatory member of the United Nations Convention against Corruption in 2005. Also, in 2008, Qatar hosted the "Corruption-free Asia Conference", to fight corruption and to improve transparency and accountability. As a result of Qatar's hard

work towards being a democratic country, Qatar received global recognition, demonstrated in comments made by the Managing Director of Transparency International, Cobus De Swardt, with regard to successful implementation of “first steps” in the state’s fight against corruption. (Aljazeera, 2009)

According to the Corruption Perception Index 2010 (CPI, 2010), Qatar was recorded in the top 20 least corrupt countries in the world, where Transparency International ranked Qatar first among the Arab nations and 19th instead of 22nd recorded in 2009 among all 178 listed countries and reported that Qatar made significant improvement over the 2009 score. Furthermore, MENA reported that Qatar scored 7.7 among 178 countries, where 0 signified highly corrupt while 10 signified low level of corruption.

Qatar has not had a major problem at the grass-roots’ level although some corruption was alleged, involving just a few senior figures of the political system (BTI, 2010), which is not very common in the history of Qatar. However, such instances of corruption are found very rarely in Qatar, and this facilitates the introduction of I-voting, which would be helpful to the population of the nation to overcome the digital divide where each voter has the equal access to services from the government (InfoDev, 2002).

5.4 Data collection method

This section examines the barriers to I-voting in terms of technical and non-technical aspects and the willingness of the society to introduce I-voting in Qatar. Towards this aim, a combination of data collection methods were used: (1) a literature review focused on discussion of the key findings and future directions for the I-voting initiative in Qatar, and (2) interviews with a sample of experts, voters and candidates used to support the literature and to obtain more recent findings on the aspects which could make the State of Qatar willing to introduce I-voting.

Three groups of respondents (voters, candidates and experts) were interviewed to explore the current voting system in Qatar and the difficulties faced with voting, along

with the feasibility of introducing I-voting, its opportunities and threats, how it would be implemented effectively and whether it could replace the current system. The first group of respondents were seven experts in the field of Information Technology (IT) and Information Systems (IS) within relevant organisations in Qatar. These interviewees provided a purposive non-random sample and were thus recruited by direct personal contact. The purpose of the interview was explained to each interviewee who was also provided with a list of the topics which it was hoped to cover. Confidentiality was assured in person and also in a covering note. Each interview was therefore semi-structured, was held individually and lasted 45 – 60 minutes, depending on job role, with notes being taken by the researcher. The interviewees preferred note-taking rather than digital recording, so they could feel comfortable and secure and could also review and comment on a copy of the notes taken.

The seven representative experts interviewed were as follows:

1. Head of IT department, Ministry of Foreign Affairs (MOFA)
2. Manager of Patient Care department, Ministry of Health (MOH)
3. Head of IT, Ministry of Interior (MOI)
4. Manager of E-services, IBQ Bank (IBQ Bank)
5. Head of ISP, Q-Tel (Q-Tel)
6. Manager of Incident Management, Supreme Council of Information and Communication Technology (ictQATAR)
7. Head of Prosecution, Supreme Judiciary Council (SJC)

Due to limited resources the researcher was only able to interview a small proportion of candidates and voters. A random sample of 4 candidates from the 2007 election and 6 voters, from different backgrounds was recruited using personal connections and convenience. These interviewees were briefed and interviewed individually, face-to-face. They were asked 20 questions on the following 10 topics:

1. The feasibility of I-voting in Qatar
2. Election procedure with or without I-voting
3. Willingness to participate in and barriers to I-voting
4. Government opinion and readiness
5. Legislation and laws regarding the e-project (I-voting)
6. The ability of the IT Infrastructure in Qatar to adopt I-voting
7. Political opinions on introducing I-voting
8. I-voting implications on security, privacy, accessibility, vote selling and the digital divide and recommendations to overcome those problems
9. Increased turnout of voters
10. The results of the survey conducted earlier in this research (see section 6.4).

These interviews aimed to review public opinions on I-voting in comparison with the experts' view to see whether people would accept I-voting technology and whether they believed it would be effective. Consequently, the information gathered from the interviews was then analysed qualitatively to identify the main outcome.

The sections below discuss the responses to the ten question topics.

5.5 Feasibility of I-voting in Qatar

The head of IT in the Ministry of Foreign Affairs (MOFA) claimed that rapid development in the country might make I-voting feasible and acceptable, especially since Qatar aims to lead the development in technology in the region. Similarly, the Ministry of Health (MOH), Supreme Judiciary Council (SJC), Q-Tel and IBQ bank experts believed I-voting was feasible and could increase participation and fulfil voting principles if it was designed with a solid and secure infrastructure.

The Ministry of Interior (MOI) and ICTQatar experts stated that it was not possible to introduce I-voting in the short term but maybe in the future, when people would be more capable of using such technology. Also, the issues associated with I-voting would have to be reviewed or maybe overcome, especially security, privacy and usability. They added, I-voting would be even more feasible if e-government infrastructure was used to provides very secure authentication using a Smart card and a digital signature as the person's signature (see section 3.4.1).

5.6 Election procedure with or without I-voting

The Head of IT in MOFA stated that in the current voting system, Qataris abroad vote for their preferred candidates safely and securely through the embassy of Qatar in the country and their votes are sent to Qatar in a diplomatic bag. Running the election in the embassy would meet all voting principles since all embassies are going to be provided with a very secure system where all the information is encrypted and transferred into a Multiprotocol Label Switching (MPLS) line or satellite communication, covering all Qatari embassies around the world. In addition, all communications are monitored and controlled by the MOFA in Qatar. He added Qatar is not yet prepared for ensuring reliable and secure voting from abroad until the project for connecting embassies is completed. In the cases where there is no embassy in the country, the State of Qatar collaborates with some other countries' embassies to cover some of the Qatari embassy duties. For example, in Kazakhstan there is no Qatari embassy but the Oman embassy provides such collaboration. The Qatar approach to solve the problem of citizens abroad by establishing a polling station per country would be costly. This implies the need to use an I-voting system, so citizens abroad would be able to vote without the need to be physically at the embassy. Qatar would save time and cost since it would not require any polling station to be established abroad.

The MOI and ICT Qatar interviewees stated that I-voting could be used alongside paper based voting, but there is a need first to make a study of I-voting and look at experiences with it elsewhere and then to carry out a feasibility study to look at the country-specific factors and whether it fulfills voting principles. They believed that

verification of voting and ensuring security, transparency and privacy are the prime considerations for I-voting and that accessibility and usability also have to be ensured.

The MOH and SJC interviewees mentioned that voters unable to attend polling stations with valid reason could delegate someone to vote on his/her behalf (Proxy voting). This approach has some implications for ensuring privacy of voters, however it is legal and voters are responsible for assigning a trusted person to vote on their behalf.

5.7 Qatar's movement towards I-voting

Qatar history of voting system has various levels, such as the municipal elections in the years 1999, 2003 and 2007 and the legislative elections during 2009. Thus, for a country which engages in the voting processes, it would be advisable to enhance the voting system to suit the convenience of the people and to carry out further development activities in the nation. I-voting would, therefore, be a potentially useful development for voters and for Qatar to be the first nation to introduce such a system for elections. Since Qatar has encountered rapid development for the last few years, developing its most important system of voting could maybe further raise its performance levels, according to the survey reported in Chapter 6. According to an interview held with Head of the IT department in MOFA, a large number of Qatari citizens living abroad exercise their rights by casting their votes for elections in their own country. He added, in such cases, Qatari citizen have to present themselves at the embassy of Qatar in the respective country and make their votes which are then carried to Qatar in diplomatic bags. Furthermore, he believed that technological developments in Qatar could pave the way for I-voting but it also needs all people to be aware of the technology, especially older people. However, he believed I-voting to be a superior and more favourable option for the Qatari citizen living abroad than for those who reside in the country.

There are various aspects that should be considered before adopting I-voting. The following sections give a summary of the different aspects that make Qatar ideal for adopting the option of I-voting according to the literature and the experts that were interviewed.

5.7.1 Country size.

As mentioned earlier, Qatar is a very small country with an area of approximately 11,500 sq. km, with a population of approximately 1.4 million (QSA, 2008) of whom, however, approximately 350,000 were believed to be Qatari citizens (United States Department of State, 2005). The small size of a country such as Qatar provides an advantage for the implementation of any new country-wide initiative. Most interviewees believed the smaller country size makes it easier to make or bring about changes in the functioning of a particular system. Hence, it will be simple to introduce the concept of I-voting in this country. Moreover, the introduction of I-voting in Qatar would be more economical and cheaper due to the smaller population size, thus facilitating the success of the concept of I-voting.

5.7.2 Economic development.

The economic development of a country plays a very important role in the all-round development of the nation reducing the opportunities for corruption in governments (Hazlett, 2003). Qatar is an economically developed country and has rich reserves of oil and gas. Being an oil-rich nation, it has an enormous amount of financial resources to support and develop its economy (Sambidge, 2009a). Qatar has been ruled by a single family since it gained independence from British rule, and this provides a major advantage to the nation in being politically stable, where its reserves are well-maintained and taken care of by the ruler of the country.

Qatar enjoyed a growth of 14% yearly compared to the UK's 0.7% since 2003; according to GDP it was ranked third highest in the world and per capita income reached \$72,634 in 2007 compared to the UK which reached \$36,600. The population growth was estimated to be 4.5% annually. Furthermore, Qatar had the lowest percentage of unemployment with 0.60%, compared to the UK's 5.5% (QSA, 2008). Qatar aims to make best use of its resources and financial abilities. It manages its resources and its developmental processes by investing the returns on oil, gas and petroleum into developing its infrastructure (Sambidge, 2009a).

One interesting development for Qatar is the presence of Internet connections in all its hospitals, thus facilitating the use of the Internet. Moreover, the hospital is equipped with a telephone line at the end of each patient room that can be connected to the Internet. According to the Manager of the Patient Care department in MOH, this facility can be useful for sick and disabled people who often vote from the hospital. Moreover, the Head of IT in MOI stated there are plans to use the network of self-service kiosks in public areas for election voting. Thus, a country such as Qatar with strong monetary and IT infrastructure and with a vision of transforming itself into a knowledge-based society is capable of building a more participative form of government by encouraging I-voting, debating and sharing of information (Reynolds and Regio, 2001; Bonham et al., 2001; InfoDev, 2002; Davison et al., 2005).

5.7.3 Educational development.

The State of Qatar has a very strong and educated base of citizens. The country has a sound education system that focuses on the quality of education imparted to its people. It has a good relationship with the topmost educational institutions of the world including those of the US and the UK. Under the guidance of H.H Sheikha Mozza, the wife of the Emir, the government has developed well-planned educational facilities for its female population. The government has educational plans for its people according to which every child has to attend classes from kindergarten till high school (H.H. Sheikha Mozah Bint Nasser Al Missned, 2009).

During recent years, Qatar has seen a large improvement in its educational system, in 2005 3.3% of GDP was invested in the education sector (CIA, 2009a). The Educational Foundation of Qatar has collaboration with many universities of the USA such as Texas A&M University, Virginia Commonwealth University and Georgetown University. Many leading American universities have opened branches in the State of Qatar which contribute towards providing quality education. As a consequence, recently Qatar became attractive for students, mainly from GCC Countries, due to the world-class universities in one place (QSA, 2008). In addition, various medical colleges and research centres have also been developed which attract students from all over the world to the world-class education system provided by the country. There is also a sound IT

curriculum and use of the Internet is provided for students at school and university levels (Ministry of Foreign Affairs, 2007c). According to UNDP (2009), Qatar has improved its literacy rate to reach 93%. On the other hand, although Qatar is showing great improvement in the education sector, the literacy rate is still below the average of 95% in the developed nations (AME info, 2004). Interviews with the ictQATAR experts claimed that all schools have computer classes and a majority of employees are asked to join various forms of computer courses to be better skilled with computer programs, thus making it easier for people to readily accept any computer-related change in the country.

In conclusion, educational development has not only improved people's general literacy but also their computer literacy, making ICT a compulsory subject taught at all education levels, and has encouraged an increase in Internet users, thus making it easier for people to readily accept any computer-related change in the country. This has raised Qatar's suitability for I-voting.

5.7.4 Technology development.

The ictQATAR interviewee stated that I-voting is part of an existing E-government project in Qatar and the MOI expert stated that Qatar has the IT infrastructure needed for I-voting. This was supported by the Qtel expert who claimed that as an ISP, Qatar has state-of-the-art technology to develop I-voting. The MOI and ictQATAR experts stated that there is currently a plan for e-voting by using an ATM machine, but it is not yet running because of technical and political difficulties and the need for more research and approval. However, the MOI expert claimed that Qatar is now capable of introducing an I-voting system both politically and technically.

Moreover, Qatar has a very strong network of telecommunications, roads and transport, seaports, postal services, airports and various other services to support communication links (Ministry of Foreign Affairs, 2007b; INTELSAT, 2010). In addition to this, the country has effective national and international communication services. the government has taken steps to set up individual bodies to regulate air transport, postal services and seaport affairs. These areas are regulated by the Civil Aviation Authority,

the Postal Service Authority and the Customs and Port Authority, respectively (Ministry of Foreign Affairs, 2007b).

One of the most important aspects is the evolution of the telecommunication system in the State of Qatar. In 1987, Qatar Telecom (Q-tel) was established as the major provider of telecommunication services for the people of Qatar. The services include a Global System for Mobile Communications (GSM) network, Internet access, e-commerce and the launch of the fibre optics cable between Qatar and Saudi Arabia (Ministry of Foreign Affairs, 2007b), thus fulfilling its role as the major telecommunication partner in Qatar. Q-Tel is solely responsible for improving the standard of telecommunication in the country and has introduced various mobile services such as short messaging service (SMS), voice messaging and a pre-paid card service. In addition, according to the CIA (2009), Q-tel reaches 2,472 million mobile subscriber and 285,300 thousand customers by landline. Moreover, it played a very prominent role in developing the Internet technology to fulfil and improve the communication criteria by introducing a fast Internet service, broadband facilities, etc. (Greenway and Robinson, 2000).

In August 2004, the Supreme Council for Information and Communication Technology (SCICT, ictQATAR) was established, acting as the main regulatory authority in Qatar (Ministry of Foreign Affairs, 2007b). IctQATAR aims to build an advanced knowledge-based research centre to extend the use of IT, developing and leading the national strategic vision relating to ICT initiatives in government, business, education, health, cyber security, market development and knowledge management. In 2006, a new telecommunications law was launched, mainly for organising competition and dominant service providers (ICT Qatar, 2009a; ICTQatar, Decree Law No. (34) of 2006).

In addition, the country has invested in ship-to-shore communication that helps to carry messages between land and sea and also in satellite communication. IctQATAR announced, in 2007, the licensing of Vodafone as a second telecommunication company operating in Qatar. Vodafone launched its service in 2009 and acquired an 18% share of the mobile market in less than a year (AME Info, 2008; ICT Qatar, 2009b). Vodafone in

Qatar currently provides only a mobile network. Fixed lines and the Internet are not yet not offered, but delivery is expected in the near future (Vodafone, 2009).

As result, Qatar has been ranked in the top 30 in the world for governmental readiness and usage of ICT (Global Information Technology Report, 2008-2009; ICT Qatar, 2009f). Also the ICT infrastructure is one of the regional broadband leaders in the Arab world (Sofiane 2005, cited in Al-shafi and Weerakkody, 2007). The interviewees from Q-tel and ICTQatar expressed the belief that there is a solid infrastructure that can support the introduction of I-voting technology with the massive improvement in the telecommunication sector and the government readiness to invest in technology.

All these considerations support the idea of introducing I-voting in Qatar with its development of IT and communications which could form a reliable infrastructure for an I-voting system.

5.7.5 The large number of Internet users

There has been a substantial growth in the number of Internet users in Qatar in the past few years. The number had reached 436,000 by 2008 and this was expected to reach the 500,000 mark by the year 2011 (CIA, 2008a). With the increase in technology and telecommunications, the Internet is making its own space in this country for carrying out different operations in various fields such as E-government, Internet banking and e-commerce. It was estimated that the Internet user rate increased from 2000 to 2009 by 1,353% due to the rapid rate of development in Qatar (Internet World Stats, 2009b). which positioned Qatar as the second highest growth of Internet usage in the Gulf region after Saudi Arabia (Internet World Stats, 2009b). Though the speed of the Internet provided to the people in Qatar is only 8 Mbps as a maximum, which is below the normal levels used in the major developed countries such as the US and the UK which use at least 20 to 50 Mbps, this medium has succeeded in attracting people to use it. However, the price for use of the Internet is high in Qatar (from 200 to 600QR, about 33 to 100GBP, depending on Internet speed) when compared to the other countries. However, the cost issues are likely to be resolved in the near future due to competition

between Q-tel and Vodafone. Qatar people have already benefited from a decrease in mobile service prices and have received a better quality service. Such an example was in April 2009, when Q-Tel Business users benefited from Free Internet Broadband Business ADSL Speed Upgrade (Qtel, 2009d).

Also, the Secretary General of Information and Communication Technology launched the I-park initiative through ictQATAR in collaboration with the Ministry of Municipal Affairs and Agriculture in March 2007. I-park is a free wireless Internet service to increase the use of the Internet by the people of Qatar. This Internet service, in accordance with the ictQATAR standards, is provided in public places such as parks, etc., thus making it accessible to a large number of people at an economical price (ICTQatar, 2007). Most interviewees believed that I-park will facilitate the process of I-voting, but it is still not accessible to all people, as some might not have a computer or even the knowledge required to operate such a system. Furthermore, the expert from the MOH mentioned in the interview that Internet technology is available in Qatar hospitals for patients to vote, free of charge, so I-voting would become accessible to all patients.

Moreover, the expert from ICT commented that providing this service free of charge has succeeded in attracting the general public to use the Internet. Such steps taken by the government play a major role in enhancing and improving the role of the Internet in the lives of the people of Qatar, giving them the benefit of this technology. This then provides support for the proposal to introduce and establish I-voting in this country (Al-shafi and Weerakkody, 2010).

5.7.6 Transformation to e-commerce

e-commerce is a rapidly evolving area wherein businessmen can fulfil their various objectives and can simplify their businesses with the help of Internet. With the increase in technology and communication, the GCC countries have considered e-commerce as a major priority for enhancement (GCC Secretariat General, 2001). Interviewees from IBQ, Q-tel, ICTQatar and the MOI claimed that Qatar is making an effort to transform business to e-commerce and is coping well with the development and, today, most business transactions in Qatar are carried out electronically (Al-shafi and Weerakkody,

2007). With ever increasing development in the field of technology, most of the companies in Qatar are transforming their operations to e-commerce (QSTP, 2007). Qatar is in the first stages of e-commerce adoption (Ashrafi et al., 2007; QSTP, 2007) but the experts expect ongoing uptake of e-commerce with the continuing development of the Qatar economy and enhancement of computer literacy.

In addition to e-commerce, another upcoming area of advanced technology, paving their way in the business world of Qatar, are e-services. This area of development uses the Internet to provide services to people which were originally provided in person. The Qatar government has been keen to provide e-services, including e-education, e-health and e-government (ICT Qatar, 2009d)., Most developing countries are planning to implement e-government services comparable to those implemented in most developed countries (Accenture 2006; Chircu and Lee, 2005; World Markets Research Centre, 2001). In Qatar, e-government called Hukoomi, was introduced in July 2000 by the Ministry of Interior, offering many government services (e.g. paying for traffic violations, applying online for visas and permits). In 2005, the success of the Qatar E-government was considered in a UN Global e-government readiness report, being ranked as number 62 worldwide and as a best practice for western Asia (UN, 2005). High growth in the number of visitors and transactions reached QR 428 in million in 2009 compared to QR 237 million in 2007, with total revenues reaching QR 930 million in 2005 (ICT Qatar, 2009e).

According to the interview with the Head of IT in the MOI, Qatar has a wide usage of secure e-services such as those using smart cards, biometrics, and digital signatures in E-government services, thus facilitating the addition of more and better e-services. This step further enhances the global position of Qatar as one of the emerging and developing nations, thus facilitating new companies to invest their money in developing their businesses in the country. The interviewee from ictQATAR believed there is a high acceptance from the people of Qatar of various new and improved e-forms such as the e-passport, E-government, e-gate (for airport immigration control), etc., hence accepting that the system of I-voting would not be a cultural hindrance in the country. This is also supported by literature (ictQATAR, 2009).

This fast transformation has led to the growth in the number of Internet users communicating online with organisations, motivating the introduction of I-voting technology as an enhancement for the e-democracy plan.

5.7.7 Political

The Head of IT in MOFA discussed the political point of view on I-voting. He believed I-voting will affect the monitoring of voting practice and the voting experience, including media coverage. In his view, it will affect voting practice where a lot of people will not go to polling stations to vote. Basically, the country and people will thus miss the voting experience, including media coverage of voting practice. He added that the law and transparency still remain the main political considerations and barriers to implementing such a system. Regarding transparency, he believed the Qatari government has developed strong relationships with its citizens and there is a coherent trust of the government.

The ictQATAR expert said that as a political consideration, there is a fear of failure of such a system which might have negative consequences for government trust. However, the MOI expert stated that the political system would encourage development of I-voting as it could ensure transparency. Nevertheless, most interviewees pointed to the political fears regarding security associated with I-voting and the possibility of a rising vote selling problem which might affect government trust.

5.7.8 Election law

Voting rights are seen in countries that follow a strict democratic form of government. In countries such as India, which is known as the world's largest democracy, all citizens attain the right to vote at the age of eighteen, as in the UK. Similarly, every country practising democracy has its norms and policies regarding the power conveyed to its citizens to exercise their voting rights.

The Head of Prosecution of the Supreme Judiciary Council claimed the state of Qatar does not follow a strict form of democracy and has certain rules that govern its political system. For example, since the country has been ruled by the Al-Thani family since its independence, formation of any kind of political party is considered illegal. However, candidates can contest elections to occupy different positions in various departments of the government institutions or government centres. He added, one major rule that governs this policy is that members of the police force or the armed forces cannot be contestants or exercise their voting power to select any contesting candidate. Voting rights are granted to the people of the country on attaining the age of 18, when they are legally considered to be an adult and can, therefore, exercise their voting power.

The State of Qatar has strict regulations regarding its political security. The government has various rules and laws in practice that govern and prohibit the formation of any political parties. However, a law was passed in May 2004 that granted permission to form private institutions and professional centres but which were given restrained powers, so as to have minimal influence over the politics of the State. In addition, all the managerial activities and official appointments dealing with the private institutions were required to gain approval from the Ministry of Civil Service Affairs and Housing (Khalaf and Luciani, 2008). An improvement in this law came about in May 2005, which relaxed the imposed restrictions dealing with managerial affairs but which restricted these operations and rights to the citizens of Qatar aged 18 and above and forbade any affiliation to groups outside the country.

A survey by the Worldwide Press Freedom Index ranks Qatar in 79th position in a list of about 170 countries, thus highlighting the liberal operation of mechanisms inside the state. This gives a positive hope for the concept of I-voting to be introduced in the country with high chances of success (BTI, 2010).

Since Qatar is an Arab country which follows the Muslim religion of Islam, the law operating in the State of Qatar is based upon the 'Shariah' which is the set of rules and justice followed according to the Islamic religion. Qatar has various laws for all the processes relating to the national interest and follows a varied view of rule

implementation. The laws are neither too strict nor too liberal so as to harm the dignity of the nation. However, Qatar has a few sets of rules and laws which are totally distinct from the other nations of the Gulf which follow the same religion.

The first and the foremost law regards the nationality of the people. The State laws forbid the practice of dual citizenship, i.e. a citizen of Qatar is not allowed to hold citizenship of any other country at the same time. Apart from this, it has various liberal laws which are not found in other Gulf nations (BBC News, 2009). These include the permission to open public bars and night clubs; however, these operate only in expensive and luxurious hotels (Greenway and Robinson, 2000).

Based upon this analysis, Qatar possesses a liberal set of laws which can be amended for modernisation and advancement of the country and this can be used in promoting the concept of I-voting. The interview with the Head of Prosecution in the Supreme Judiciary Council claimed the government of Qatar would not raise objections to this concept on condition that the voting process retains the manual voting that has been practised in the country since voting began. It should be clear, transparent, secure and private. The interviewees from the MOI and ictQATAR mentioned there is a new e-law developed by ictQATAR in collaboration with MOI which has been prepared but has not yet been approved by the government. Both added that the government of Qatar has built a strong relationship of trust with its citizens over a period of time. Ironically, the interviewees believed the political willingness and the absence of a strong law regarding Internet voting might benefit introducing this system in Qatar. However, with no protection for Internet users because of the lack of any e-law in Qatar, Qatari voters would have concerns on ensuring their security through electronic channels. Research by Al-hamar et al. (2010) has pointed to the effect of Qatar culture and country-specific factors in making citizens vulnerable to online crimes with the clear absence of Qatar e-law. Therefore, protecting online voters should be considered along with cultural and country factors to assist in the introduction of I-voting.

5.7.9 Culture

Culture refers to the set of values and traditions followed by the people of a country in their day-to-day life activities. Culture defines the use of principles and processes to deal with everyday situations and to confront problems in a well-defined manner according to the rules of their religion. Since Qatar follows the Shariah or the Islamic set of rules and regulations in the governing of the country, it is essential that any new processes or proposals introduced in the country should be within the acceptable limits of the national culture. However, a country is not only a home to its nationals but is also a destination for people from all over the world who stay in this country for education, tourism, employment, etc. Around 80% of the population is Muslim, 6.5% Christian and the remaining 13.5% belong to different religions (CIA, 2008a; [QSA, 2008](#); U.S. Department of State Diploma in Action, 2007). Qatar culture is influenced by the Islamic religion and traditions which have a major impact on people's daily life behaviour. However, even with the rapid development encountered, Qatar has maintained its culture with the support of the Ministry of Culture and the Arts which aims to preserve Qatar culture and heritage (Ministry of Culture, Art and Heritage, 2008; Al-hamar et al., 2010).

The government of Qatar has liberal laws when compared to other Islamic nations of the Gulf and, despite the varied diversity of the Qatari population, the Qatari people still seem to be trustful, helpful, generous and good willed (Al-hamar et al., 2010). The ability of the culture of Qatar to adapt to the multi-ethnic living of Qataris (CIA Facts, 2008; Al-hamar et al., 2010), rapid developments and modernisation means the introduction of a new concept such as I-voting would not prove to be a hindrance for the culture of the country. Recently, Qatar was the first Arabic country to win the bid to host the 2022 FIFA World Cup (FIFA, 2010). All interviewees pointed out the government's outstanding achievement in keeping itself updated with the continuously evolving technologies across the world in all sectors and in supporting the nation's development. As I-voting is considered to be a simple technological process, it should not face any major objection from the government of the country and should be easily and effectively introduced in the nation if it is correctly designed. This implies considering the cultural and country specific factors while designing I-voting, taking into account people acceptance to such new technology.

5.8 Barriers to I-voting

Although, there is an obvious Government readiness and willingness for I-voting in terms of politics, technology and accessibility, I-voting still faces concerns over security, privacy, accuracy, getting people's acceptance and eliminating the possibility of vote selling. Still, government approval of such a system and ensuring trust in the system are essential to achieve success. This implies that although there is a lot of willingness towards I-voting, there are still many barriers which need to be addressed to introduce I-voting in Qatar in the near future.

5.8.1 e-Law

The majority of interviewees claimed the e-law discussed in section 5.7.8 is on the way to approval. The law involves all topics associated with electronic communications and is being developed by ictQATAR in cooperation with other related bodies including the SJC and the MOI. The law will protect online consumers' rights. The law does not permit verification for voting because it may be used for vote selling. The Head of IT in MOFA stated that the approved Internet law would encourage I-voting. In contrast, the interviewee from the MOH's view was opposed to voting through the Internet as he thought there is no need to change the law and provide an e-law since voting in elections in Qatar runs smoothly. The MOI expert, however, suggested there should be development of an e-election law to assist the introduction of e-voting.

The Head of Prosecution of the SJC claimed that in Qatar law there is nothing to say that I-voting is not allowed. If it is proved that it fulfills all of the voting principles, then why should it not be applied? However, it could be applied as an experiment to assess its effectiveness alongside the traditional voting system, and also to assess people's acceptance. He added that override voting (allowing a person to change their vote within the voting time frame) is a complex feature which the current law does not allow because it could be used for vote selling as voters might change their vote several times in order to sell it to different candidates. Although some might say the override is a valid option, especially for people who might be intimidated and forced to vote for a

specific candidate, this is, however, difficult to prove and therefore he still believed overriding is not a valid option. Moreover, he pointed out that Qatar law does not allow for source-code to be made available to the public to avoid it being used by malicious people who wish to hack into the system and manipulate voting results. However, work still need to be done on e-law to facilitate I-voting, this implies the need for collaboration with information security expertise and election committees towards identify all the possible threats might face election process and embed them in the E-law. Furthermore, having a separate section covering e-election is advisable to protect election process from possible electronic threats.

5.8.2 Accessibility and Accuracy

All interviewees stated that I-voting would increase voting turnout by providing accessibility. The sample of four candidates and six voters interviewed believed I-voting would aid accessibility, especially for voters unable to come to polling stations, as they could vote over the Internet at any time. The MOI and ICT experts claim that it facilitates the efforts of the voting committee, since votes are counted automatically through the website and this might reduce human errors and save the time and effort required for counting votes manually. Experts from the MOFA, MOH and Qtel claimed that Internet voting would provide accessibility and privacy for voters as they can vote freely online at any time.

The interviewees from Qtel and the IBQ Bank said that Internet voting as an option would provide a fast voting process with no need to wait in queues, and this would increase voting participation due to accessibility, especially for those who cannot come to polling stations, such as patients in hospital, Qataris abroad and old and disabled people. The interviewee from the MOH stated that I-voting would facilitate the voting process for patients unable to vote in polling stations compared to the current voting system which allows patients to vote in an election by an arrangement set up upon patient request, where the judge will simply come to the patient personally to collect his/her vote manually, which is time-consuming and costly.

The Head of IT in MOFA added that I-voting could be considered as an appropriate option for Qatari voters abroad due to the accessibility, Government willingness to

introduce new technologies, E-government project infrastructure, and citizen computer literacy.

However, there are number of barriers to accessibility and accuracy which most interviewers mentioned such as the lack of 100% computer literacy, and the lack of 100% access to computers and Internet technology. Also, resistance to change is one of the barriers that should be considered were some of interviewed mentioned people resistance to change to I-voting even when they have the enough computer literacy and accessibility to the Internet and that due to their preference of traditional voting which they get used to and the fear of missing voting experience.

5.8.3 Security, privacy and usability

The majority of interviewees listed the main barriers faced or expected to be faced in the uptake of I-voting in Qatar are getting people's acceptance of such technology, especially considering the security, transparency, vote selling, missing voting experience and privacy issues, and the huge potential threat of hackers on the Internet nowadays. According to Waldrop (1999), "There is virtually no software that can't be hacked and most anything in a computer can be hacked". This means there is a possibility for hackers to penetrate I-voting and manipulate results. The MOI expert asserted that security can be implemented but it might affect usability and accessibility. The interviewee from the SJC stated that ensuring security is an issue, especially with possible threats from hackers on the Internet. Both the MOI and SJC experts believed that there is a possibility of infringing the privacy of a voter. In addition, the expert from IctQATAR stated that it is complex to achieve the same degree of privacy as in paper based voting.

The Head of IT in the MOFA mentioned the need for technical and non-technical solutions to secure I-voting but fear of a new type of attack remains a problem. However, the interviewees from the MOI, IBQ Bank, Q-tel and ictQATAR all claimed that the security aspect of I-voting can be assured technically with an acceptable percentage of error. The MOI and ictQATAR experts pointed out that, so far, the E-

government website had never become unavailable as a result of an attack, although they have received many attacks from different countries. However, IT experts from Q-cert and ICT, MOI and Qtel are collaborating to prevent and eliminate these attacks. The interviewees from Qtel and the IBQ bank stated that I-banking has a proven track record of success in security, people acceptance and trust. Therefore, Qatar could learn from I-banking in developing I-voting. However, I-voting is different to I-banking because voting is done anonymously, unlike in a bank where everything is recorded and can be traced.

Most interviewees spoke of the importance of getting people's acceptance and ensuring the usability of the system for all voters regardless of their computer knowledge. The interviewee from the MOH believed that older people would experience real problems in dealing with computers but, on the other hand, the new generation would welcome such a system. Therefore, they need to be involved in training and awareness sessions on how to use the system successfully and securely to eliminate the resistance to change, digital and social divides and usability issues. The Head of IT in the MOFA and the MOI claimed, Qatar is taking huge steps to improve education and to make learning computer technology a priority in the academic sector and in all jobs, this would assist people's acceptance of I-voting technology.

According to Al-hamar et al. (2011a, 2011b) Qatar is considered an attractive environment for e-crimes due to the lack of some Qatari's absorption of the rapid technological advances, the lack of laws to handle e-crime and availability of large number of unaware Internet users in terms of information security. This implies the essential need for consideration of the security of I-voting and enhancing people's awareness on how to use I-voting technology, and how to protect themselves from possible e-crime associated with the client-side of I-voting to providing a secure I-voting system on both client and server-side by applying the best practice security controls.

5.9 Summary of expert interviews

The interviews with experts are summarised in matrix form in Table 5.1.

Table 5.1: Summary of expert interview responses

	Increased turnout	Law	Technology	Political	Security	Privacy	Accessibility - Mobility	Vote selling	Digital divide
Ministry of Foreign Affairs	Yes	Internet law would encourage I-voting	Qatar not prepared for voting from abroad until connection of embassies is completed	Will affect monitoring of voting practice, missing voting experience, including media coverage of voting practice.	Technical and non-technical solution can secure I-voting but fear of new type of attack remains	Internet voting provides more privacy	Computer can use some devices to make it accessible	Will increase	Government should provide free Internet
Ministry of Health	Yes	No need to change the law	None	None	Security will still be barrier in I-voting. Is it going to be as secure as traditional voting?	No-one must know voter choice	Older people would experience real problems	Will increase	Government should provide free Internet
Ministry of Interior	Yes	E-election law should be introduced.	Qatar has IT infrastructure needed for I- voting	Political system would encourage development of I-voting which could ensure transparency	Security can be implemented, but usability and accessibility would be affected	No software that cannot be hacked and most anything in a computer can be hacked	Computer can use some devices to make it accessible	Will increase	Government should provide free Internet

	Increased turnout	Law	Technology	Political	Security	Privacy	Accessibility - Mobility	Vote selling	Digital divide
Q-Tel	Yes	Current e-law with election law could work with minor changes	As ISP, Qatar has state of art technology to develop I-voting	Fear of using I-voting for commercial or political purposes	I-banking has proved its security and people accept and trust it, so use of such technology in I-voting would be effective.	I-voting provides more privacy	Computer can use some devices to make it accessible	Will increase	Government should provide free Internet
ictQATAR	Yes	ictQATAR has developed e-law Covers e-commerce, e-transactions, e-signatures, e-documents and authentication	Internet voting part of existing E-government project in Qatar. Besides designing Internet voting, need to apply best model	Fear of failure of such a system which might have negative consequence for government trust	Qatar can develop secure Internet voting	Complex to achieve same degree of privacy as in paper based voting	Computer can use some devices to make it accessible	Will increase	Government should provide free Internet
Supreme Judiciary Council	Yes	Qatar should develop new law for Internet voting. Lack of legal requirement to use I-voting	Question for MOI, ictQATAR and Qtel	Qatar interested in being first country to apply state of the art technology in an election	Ensuring security an issue, especially with possible huge threats from Internet hackers	Possibility of infringement of voters' privacy becomes a problem	Computer can use some devices to make it accessible	Will increase	Government should provide free Internet

5.10 Summary of candidate and voter interviews

Generally, interviews with four candidates and six voters have confirmed what the experts say with some differences, for example they were divided between those who supported I-voting and those who thought it was not feasible due to the difficulty in getting people's acceptance and giving them knowledge on how to use such a system. This implies that I-voting is feasible, but only with consideration of people's acceptance and knowledge of how to use such a system. Furthermore all of the election candidates commended the low corruption in Qatar, and this provides motivation for the promotion of I-voting to boost electronic democracy with minimal risks. Also, all interviewed voters believed that the voting was corruption free, showing a great trust in the government and most show a great interest in I-voting with some concerns on the security aspects associated with such new technology.

Furthermore, the majority of interviewed candidates suggested I-voting could be applied as an alternative way of voting alongside the traditional voting system. They also suggested having an experiment to obtain an estimation of people's acceptance and whether it would increase participation levels and fulfil all voting principles. Similarly most of voters recommended using I-voting alongside with paper-based voting for redundancy and to give voters the choice to choose which one method of voting they prefer. This implies that I-voting could be used alongside paper based voting to provide flexibility and accessibility for voters.

All candidates believe that there is support to introduce I-voting in Qatar including the huge development introduced in Qatar in many sectors including education and telecommunication which has assisted in increasing internet accessibility and computer literacy. an interview with voters provide further evidence that the government is ready in terms of technology with some fears to people's acceptance and resistance to change along with security and usability.

In contrast, most candidates point out to the barriers of I-voting in terms of ensuring voting principles including security, privacy, transparency, anonymity, usability and accessibility. They added there is a fear of losing government trust if those principles were not achieved in I-voting.

5.11 Conclusion

This chapter determines the feasibility of I-voting in Qatar, based on a literature review and interviews. Seven representative experts were interviewed along with four candidates and six voters from different backgrounds. The interviewees were asked about the feasibility of I-voting and the knowledge required on how to use such a system, and they all concluded it would be feasible. The literature and interviews have identified the feasibility of I-voting in general, the possibility of modernised democracy and identified the willingness and barriers to introduce I-voting in Qatar. Research shows the willingness of Qatar to introduce I-voting due to various factors: educational development, technology development, the large number of Internet users, election law, the political aspect which does not bar the use of I-voting and Qatar's culture which supports the introduction of I-voting. In contrast, there are many issues concerning I-voting that need to be overcome, including ensuring security, privacy, usability, accessibility, accuracy and an e-law. This implies I-voting could be feasible, with government readiness and willingness pointing to the need for considering the possible barriers of such a voting system. It is therefore suggested that I-voting is provided as an alternative method of voting alongside the current paper based voting system.

Further investigation is described in the next chapter to determine the people's values and opinions about I-voting in Qatar for a general election.

Chapter 6 Qataris' Views on I-Voting

This chapter describes a survey combining interviews and questionnaires to discover the willingness of Qataris to participate in I-voting in Qatar and the barriers that may prevent them from accepting it. The data has been gathered to enable recommendations to be made on designing such an election system. Therefore, this chapter satisfies objective 5 of the research (see Section 1.5).

6.1 Aim of survey

A survey was carried out to assess the confidence and willingness of Qatari citizens to take part in the initiative of I-voting and to find the barriers that would inhibit I-voting in Qatar. It was aimed to highlight willingness and barriers from the viewpoint of Qataris. The purpose was to enable recommendations to be made to the Qatari government to introduce and encourage the uptake of I-voting in the State of Qatar. Additionally, the questionnaire asked participants for their opinions on features needed in an I-voting system.

6.2 Survey design

According to Yin (2003), *“The analysis of case study evidence is one of the least developed and most difficult aspects of doing case studies”*.

The research followed the design recommended by Myers and Avison (2002) to ensure smooth movement from objectives and questions, to theories, to specific data uncovered and, finally, to results and conclusions. The general approach was to use survey data to develop profiles for those people likely to use I-voting in Qatar. This carefully designed study followed a sequential explanatory strategy as explained by Creswell (2003). In the first instance, the population of the survey was defined as being all Qatari citizens, since the research focuses on the State of Qatar. However, the sampling was then further restricted to Qataris aged 18 and above, 18 being the legal voting age. The survey was

designed in Arabic as well as English versions, since Arabic is the national language in Qatar. It aimed to use simple and clear language and to be well structured in order to fulfil the ultimate aim of the survey.

Before its implementation, the survey questionnaire was pilot tested by five researchers in the field of E-government, IT and Internet use. The researchers were recommended by the Supreme Council of Information & Communication Technology (ictQatar) and were selected according to their knowledge and experience of similar systems. Several subjects of the pilot test commented that they felt uncomfortable answering some of the questions, such as the technical questions about designing the application and a few questions about the “digital divide”. Most of the researchers also commented that the questionnaire was too long. The comments were taken into consideration and the survey was modified accordingly to make it more effective.

The final form of the survey consisted of 11 simple questions arranged into 4 sections on background, willingness, barriers and features. Some questions were related to more than one section. Finally, the survey questionnaire was distributed by hand to a large number of Qatari public (about 4,000) with a return rate of 64.2% from governmental and private organisations across the country, using the drop-off and pick-up method, to ensure that only targeted participants (Qataris over 18) would contribute. The researcher's sponsor provided a letter of support to make the survey distribution easier and to encourage a response (see Appendix A). The population sample for the survey was taken from addresses provided by organisations with which the researcher had contact. The organisations contacted were the Ministry of Education, the Ministry of Foreign Affairs, the Qatar Foundation, Qatar University, the North Atlantic College, Q-Tel, ictQATAR, several banks, Qatar Petroleum and others (see Appendix A for more details). The organisations interested and willing to co-operate were asked to distribute the survey only to Qataris eligible to vote, and these organisations tried their best to ensure they followed the sampling criteria.

It took about one month to conduct the survey and collect responses. Later, the data was analysed electronically using an online survey tool (www.proquestion.com) since it facilitates the analysis process and provides the feature of response filtering.

6.3 Survey structure

The survey questionnaire asked the participants about their opinions on the design of the I-voting system, the barriers I-voting may encounter and the willingness of Qataris to participate in I-voting.

It included the following four individual sections:

1. Demographics (age, gender, education, Internet and computer knowledge)
2. E-services usage (online banking usage, experience)
3. Confidence in the management and accuracy of general elections
4. I-voting

The aim of the survey was to discover barriers to, willingness to participate in, and the opinions on the required features for I-voting, in correlation with the participants' demography. Willingness and barriers were derived from the participants' response to questions on the use of online banking, and on participants' confidence in the management and accuracy of general elections and on I-voting. Participants were also asked which of a list of system features would be required for an Internet voting (I-voting) system. Figures 6.1 and 6.2 show the structure of the survey questionnaire. The relationship of response choices to the willingness to participate in I-voting, barriers and system features is indicated accordingly.

Figure 6.1: Survey questions (Page 1)

Section 1 – Background

1.1 What is your age?

18 – 24 25 – 29 30 – 39 40 – 49 50 – 59 60+

1.2 What is your gender?

Male Female

1.3 Which Level of education?

School College University Postgraduate Others

1.4 Self rating of computing and Internet knowledge?

Absolute beginner Some knowledge Average knowledge Pretty knowledgeable Expert

Section 2 – Use of the Online Banking

2.1 On average, how often do you use the internet for Online banking or making online purchases?

Once a week or more 2-4 times a month Once a month Vary rare Not at all

Willingness **Barriers**

2.2 Why don't you use the internet for online banking or making online purchases more often? What are your reasons? *(Please fill all that apply)*

Don't think it is very safe/ secure Things restricting internet use No need for it Prefer personal interaction Unsure

[Asked of those who use online banking or make online purchases less than once a month.]

Barriers

Section 3 – Confidence in management and accuracy of general elections

3.1 Rate how confident are you that general elections in Qatar are managed fairly and that vote counting is accurate.

← Not Confident (0 – 3) Mid-Range (4 – 6) Very Confident → (7 – 10)

Barriers **Willingness**

3.2 Regarding abroad citizens, how do you think they should vote?

Going to Qatar embassy Through the website Phone Others

Barriers **Willingness** **Barriers**

Figure 6.2: Survey questions (Page 2)

Section 4 – Online Voting

4.1 How strongly do you agree or disagree with the following statements about online voting in Qatar general elections, assuming that it would use security systems similar to internet banking and reputable online retailers?

Rate the following:

	Strongly Agree (0 - 3)	Mid-Range (4 - 6)	Strongly Disagree → (7 - 10)
4.1.1 - I would choose to vote online instead of visiting a polling place	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2 - I would be comfortable with voting online	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3 - I would be confident that I could vote online without anyone seeing who I was voting for	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4 - I would be confident that I could vote online without anyone else unduly influencing my vote	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5 - I would be confident that vote online is more secure	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Willingness **Barriers**

4.2 If you were to vote online, would you regard the following security features as essential, nice to have or not important?

	Essential	Nice to have	Not important	Unsure
A screen which would ask you to confirm who you were voting for before it was made final.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Being able to revisit the voting website to confirm that your vote has been received but not who you have voted for.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Being able to request confirmation using a different means of communication, such as sms text	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other, please specify:				

System Features

4.3 If you do not believe there should be Online voting in Qatar, please state why:

The technology would be too difficult for some people to use.	<input type="checkbox"/>
The technology may not be reliable.	<input type="checkbox"/>
There would be no easy check that the results are correct and have not been manipulated.	<input type="checkbox"/>
A computer hacker may be able to affect the results	<input type="checkbox"/>
Vote selling	<input type="checkbox"/>
No need for it	<input type="checkbox"/>
Other, please specify:	<input type="checkbox"/>

Barriers

6.4 Survey results and analysis

The data gathered from the survey were analysed qualitatively and quantitatively. A summary of the results is as follows:

- The total number of Qatari participants eligible to vote was 2,567, a 64.2% response rate.
- The majority of participants (62%) were female.
- The majority (52%) were aged 18 – 24 years.
- Most participants (about 86%) were in further and higher education or had been educated to further or higher education level.
- 56% of participants had computer knowledge, ranging from having some knowledge to being pretty knowledgeable or expert. Less than 4% were novices in computing.
- The majority of participants (73%) use e-services.
- The majority of participants who are not using e-banking claim they prefer personal interaction (36%) or they do not think it is secure (25%).
- With regard to I-voting, 29% think its major barriers are that the technology would be difficult for some people to use and 25% believe that computer hackers might influence election results.
- About half of the participants (48%) were very confident about general elections in Qatar.
- The majority (76%) would prefer voting online rather than in polling stations.
- 43% of the participants thought that use of websites for voting would be an excellent proposal for citizens abroad.
- Most participants (70%) indicated they were comfortable with the idea of I-voting, and that it gave them confidence, ensured privacy and offered the ability to vote freely, though there was some doubt about security.
- Half of the participants (50%) thought it is essential to ask voters for confirmation of their vote before casting it and to enable them to verify their votes online and through different channels, e.g. SMS and telephone.

6.4.1 Demography

The majority of participants (62%) were female and the rest (38%) were male (see Figure 6.3)

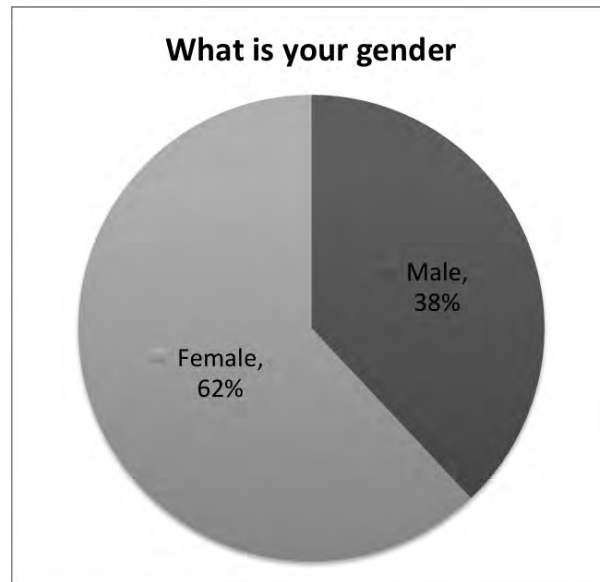


Figure 6.3: Gender of respondents

The results indicate that 52% of participants were aged 18 – 24, which reflects the fact that the majority have yet to complete their education (see Figure 6.4).

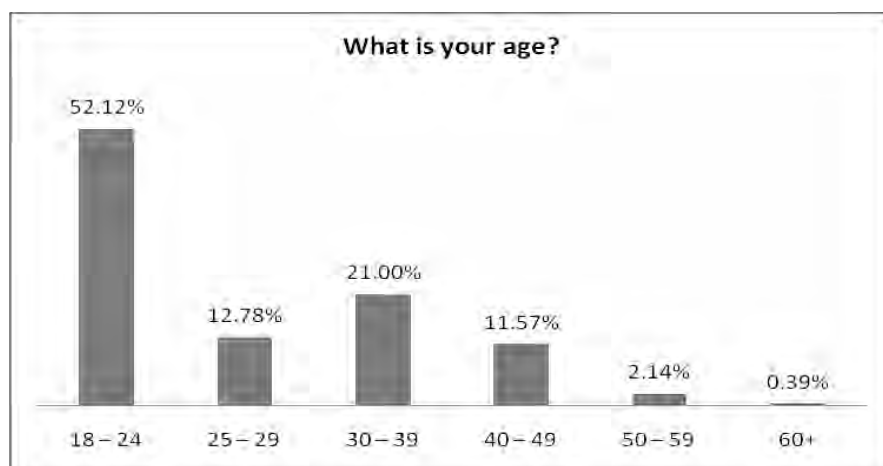


Figure 6.4: Age of respondents

The largest group of participants (45%) were in or had completed further education and 42% were in or had completed higher education. Less than 10% were at school or at postgraduate educational level (see Figure 6.5).

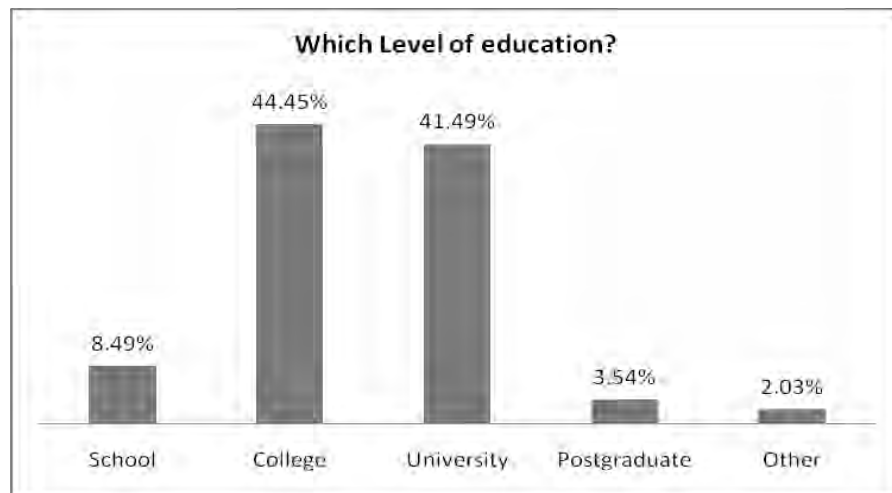


Figure 6.5: Final/current education level of respondents

56% of the participants have computer knowledge ranging from being pretty knowledgeable to expert, and about 40% had some or average knowledge level. Less than 4% considered themselves to be absolute beginners (see Figure 6.6). This is a good sign for the vision of I-voting since the majority of Qatari citizens have the knowledge required to use such a system.

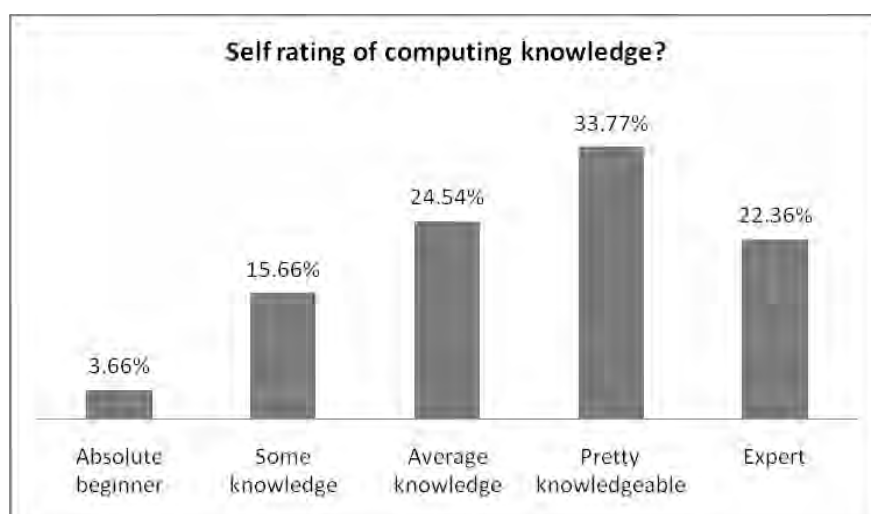


Figure 6.6: Computer knowledge of respondents (Self-rated)

6.4.2 Willingness to participate in I-voting

The use of e-commerce or e-services was not high: about 42% of the participants do not use e-commerce or e-services, about half of the rest use it very rarely (29%), only 12% use it once a week or more. This might be because most of the questionnaire participants were students of young age (between 18-20 years old) who do not have the income to perform such transactions (see Figure 6.7). However, more than half (58%) of them have used e-commerce before and therefore this indicates they are likely to be capable of using I-voting as it employs a similar process, except that they would be choosing their preferred candidate instead of choosing a product or a service.

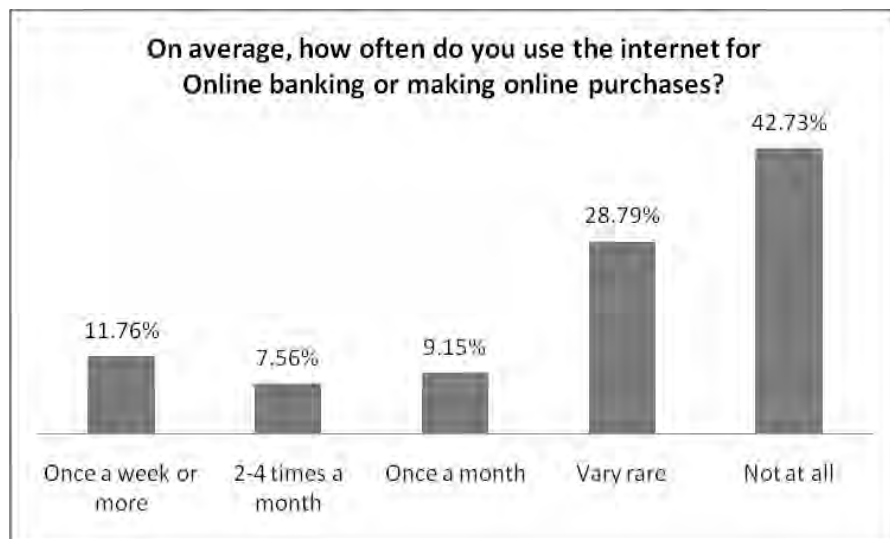


Figure 6.7: Frequency of use of e-services

About half (48%) of the participants were very confident about general elections in Qatar, considering them to be fair and accurate. This confidence would be an advantage for the vision of I-voting. About one third were not sure and about 13% had mid-range confidence and only 4% had no confidence in the national election process. Although there is high confidence in elections in Qatar, I-voting would need to be efficient and successful to avoid losing it (see Figure 6.8).

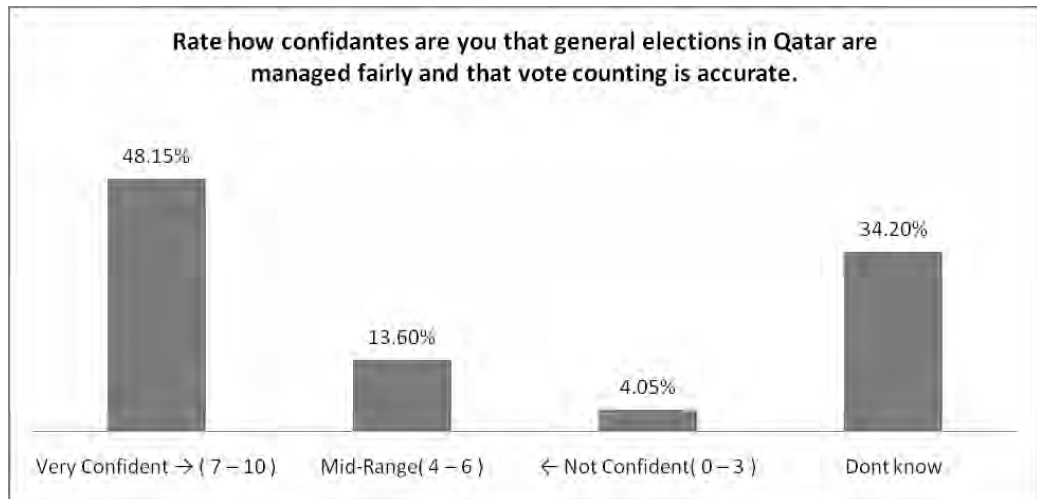


Figure 6.8: Confidence in elections in Qatar

More respondents would prefer to vote online than in polling stations (37% compared to 24%), but a significant number (39%) did not commit themselves strongly either way (see Figure 6.9).

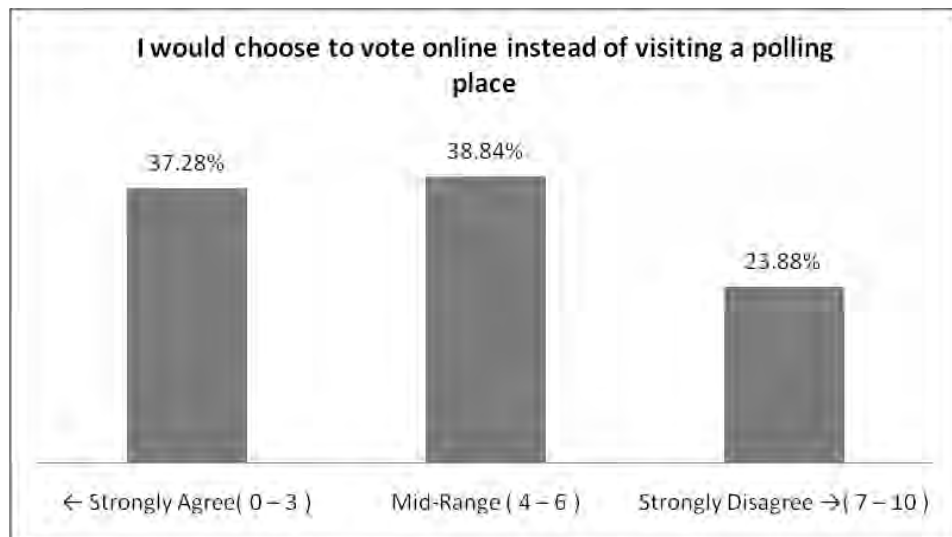


Figure 6.9: Preference for I-voting

Furthermore, 43% of the participants thought that the use of websites to vote was an excellent proposal for citizens abroad, but nearly half (49%) thought it would be better to go to the Qatar embassy to vote and a few (8%) thought it would be better for citizens abroad to vote by phone and other channels such as mail. This means there are a significant percentage of people who would trust I-voting, even from abroad. Although

this is less than half, it is a good indicator that they could trust I-voting given suitable safeguards and assurances (see Figure 6.10).

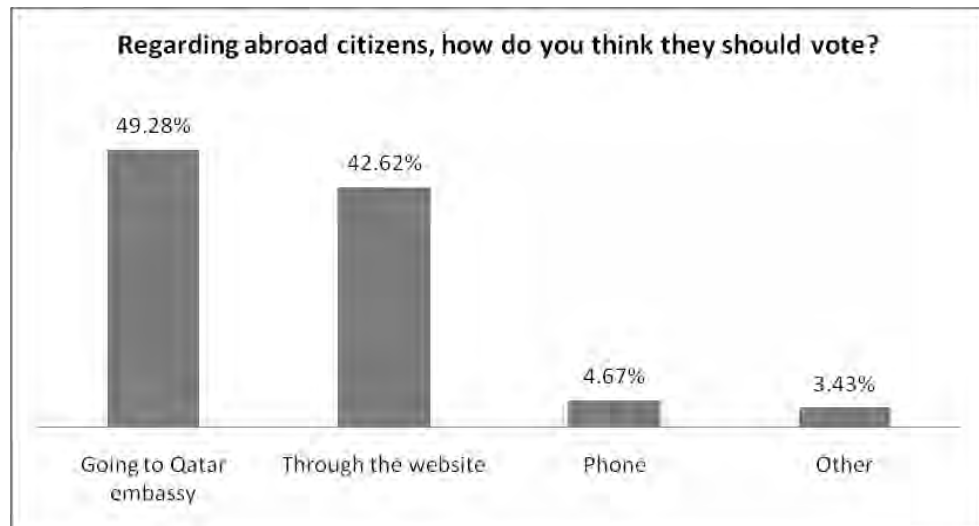


Figure 6.10: Voting method for citizens abroad

With regard to whether the participants felt comfortable with using an I-voting system, slightly more (30%) felt comfortable than those who did not (27%).

A significant number (43%) did not commit themselves strongly either way (see Figure 6.11).

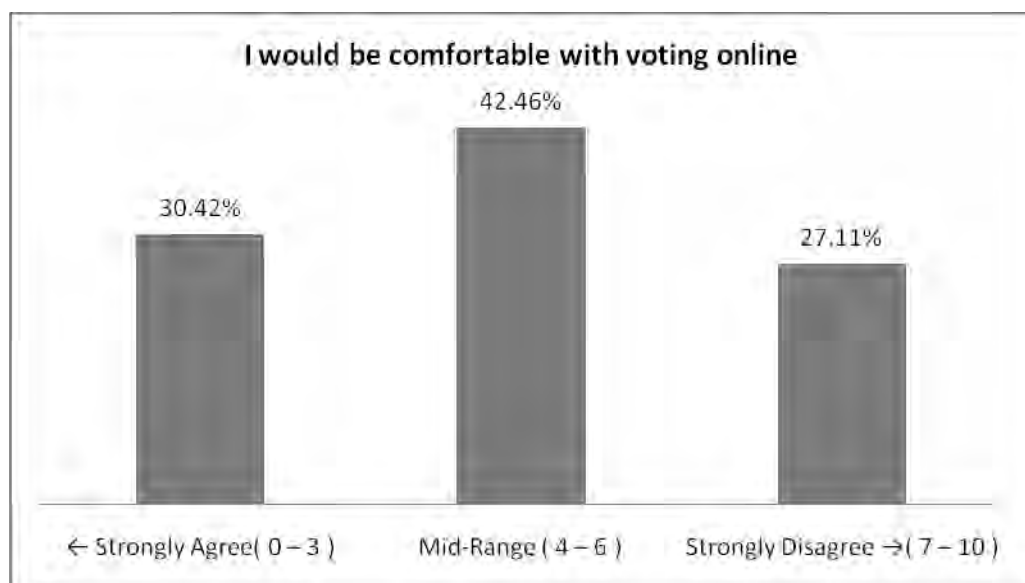


Figure 6.11: Comfortable feelings with I-voting

These results reflect the preference for I-voting compared with voting at the polling station shown in Figure 6.9, though it is interesting that slightly more said they would prefer I-voting than those who were comfortable to use it. This shows the desire for I-voting is stronger than people's readiness to use it. The results show a similar pattern for people's confidence in their voting privacy with I-voting. More people (35%) were confident than those who were not (27%), but a larger number did not commit themselves strongly either way (see Figure 6.12).

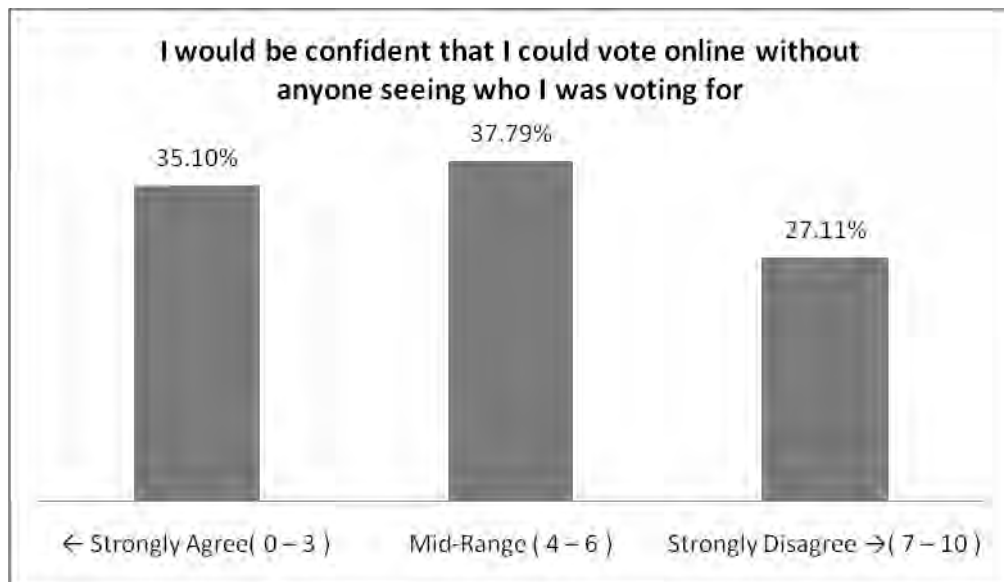


Figure 6.12: Confidence in privacy of I-voting

Interestingly, slightly more people (39%) responded that I-voting would enable voters to vote freely without influence from anyone than were confident in the privacy (35%), and fewer disagreed (22%) than were not confident in the privacy (27%), but again a large number (39%) did not commit themselves strongly either way. Perhaps the lack of confidence in voting privacy was connected to doubts about the security of the system as the number of people who had strong doubts about the latter was as large as those who had confidence in it (both about 29%), but again there was a large number (42%) who showed some uncertainty (see Figure 6.14).

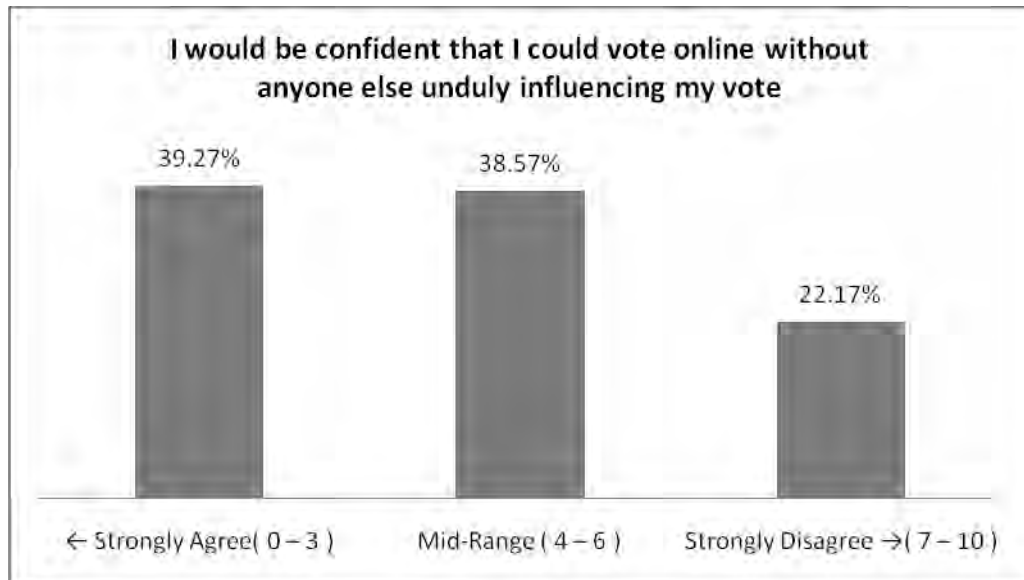


Figure 6.13: Ability to vote freely in I-voting

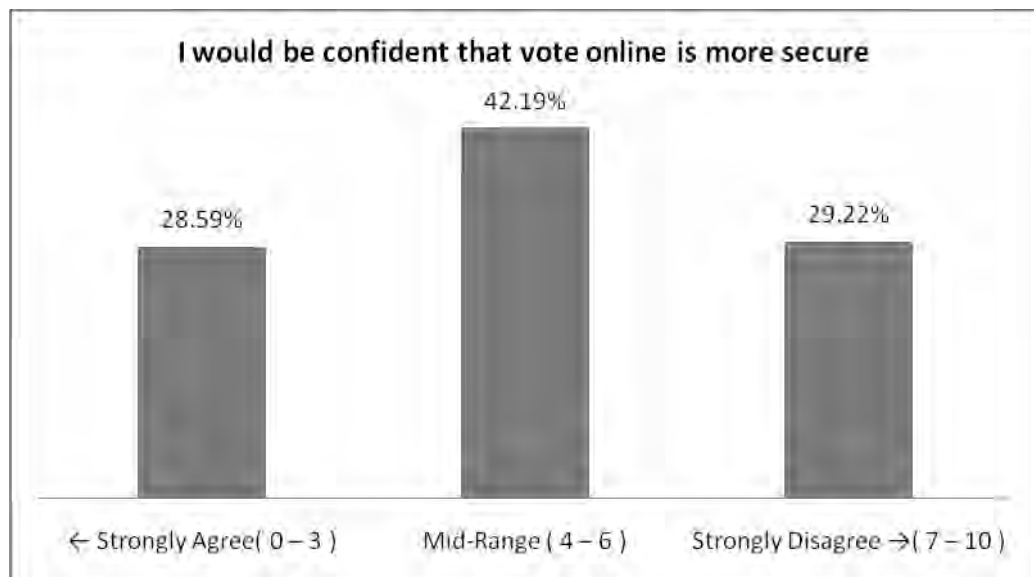


Figure 6.14: Confidence in security of I-voting

In general, responses indicate a willingness for I-voting to be introduced in reality, since many thought they would be comfortable with and have confidence in I-voting. They felt their privacy would be sufficiently safeguarded and they would have the ability to vote freely, but there were some significant concerns about the system security. However, a significant finding was that for all considerations there were between a third and a half of the people surveyed who felt unable to commit themselves strongly either in favour of or against I-voting.

6.4.3 Barriers to acceptance of I-voting

Of the participants who do not use e-commerce or e-services, the largest number (36%) gave their reason as a preference for personal interaction, then 25% blamed security issues and 20% said there was no need for such a system. A few (5%) referred to considerations restricting Internet use, such as its cost and a lack of knowledge of computers. 7% were unsure and 6% referred to other reasons such as they would miss the shopping experience, they were not interested or do not have a Visa credit card (see Figure 6.15).

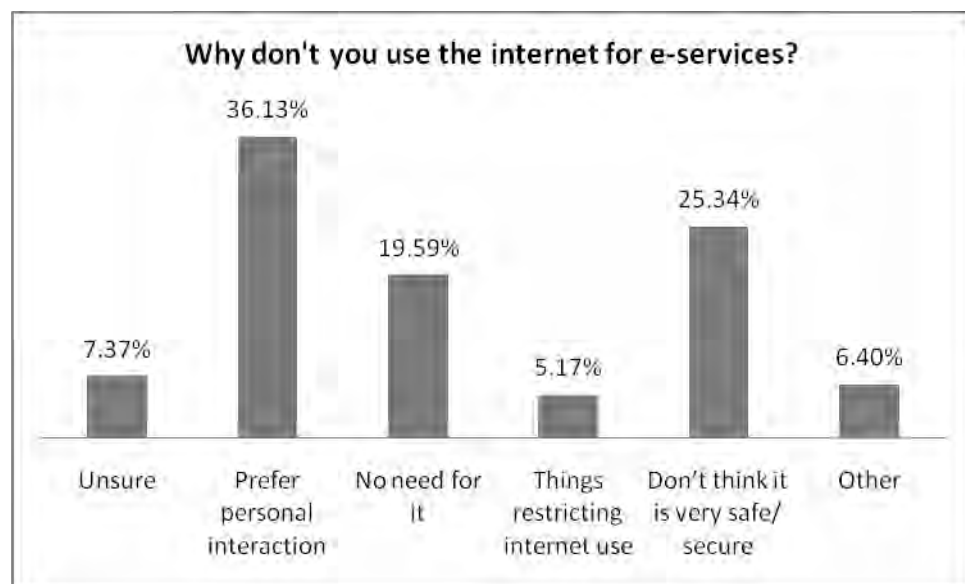


Figure 6.15: Reasons for not using Internet for e-services

The participants who do not believe there should be I-voting in Qatar referred to the following reasons: 29% said the technology would be difficult for some people to use, 25% were afraid computer hackers might affect the results and about 13% blamed the difficulty to inspect whether the results had been manipulated or the reliability of the technology. Only a few (10%) stated that there is no need for it and fewer still (8%) referred to the possibility of vote selling (see Figure 6.16).

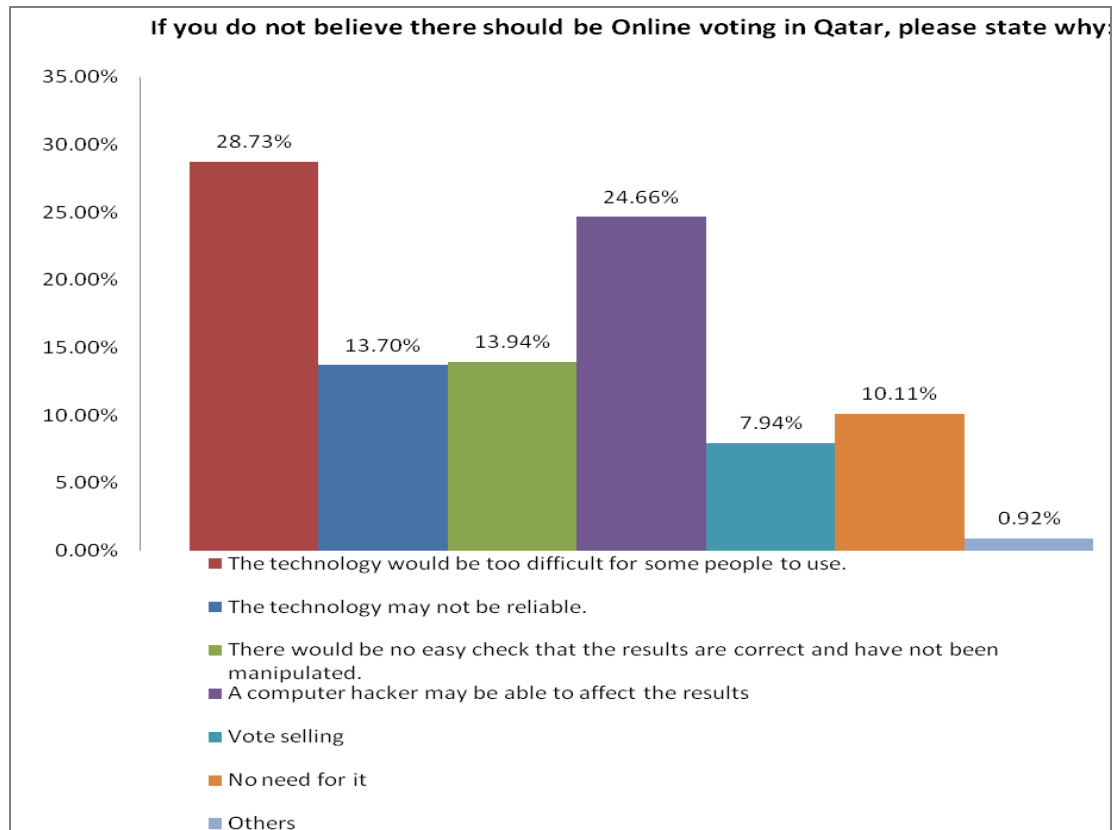


Figure 6.16: Possible barriers for I-voting

6.4.4 I-voting features

Participants were asked their opinion on the need for the system to ask for confirmation of the identity of a person online, for voters to be able to verify through different channels, such as SMS, who they were voting for before casting their vote, and for the ability of voters to verify their votes by messaging or phone.

In general, over half the participants responded that these I-voting features were essential, about 20% said they were nice to have and only about 7% thought the features were unimportant. Approximately 13% were unsure of the need for these features. This reflects the need for confirmation and verification through different channels to ensure the vote casting is correct. This gives an indication that, although more people found I-voting acceptable, they still require verification to ensure their votes are recorded correctly (see Figures 6.17-6.19). About half of participants thought it essential and a

further 20% thought it would be a nice-to-have the feature to be able to request confirmation using a different means of communication, such as SMS text.

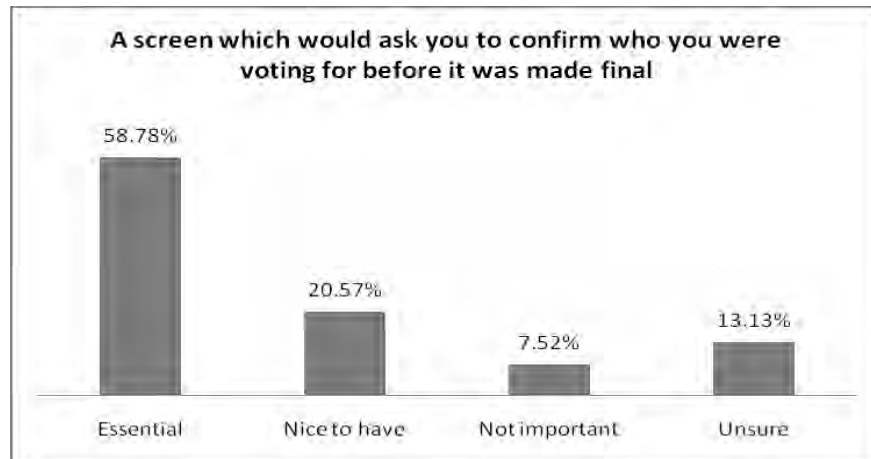


Figure 6.17: Voter confirmation of candidate selected before vote recorded

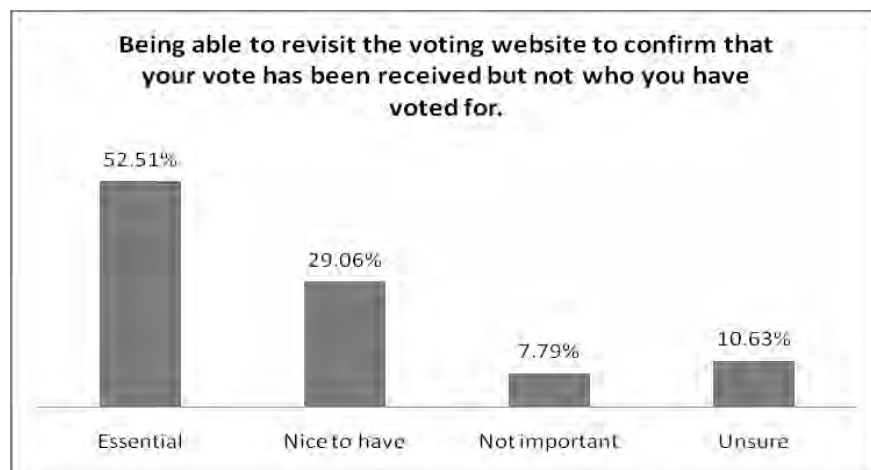


Figure 6.18: Ability to revisit the voting website to confirm choice

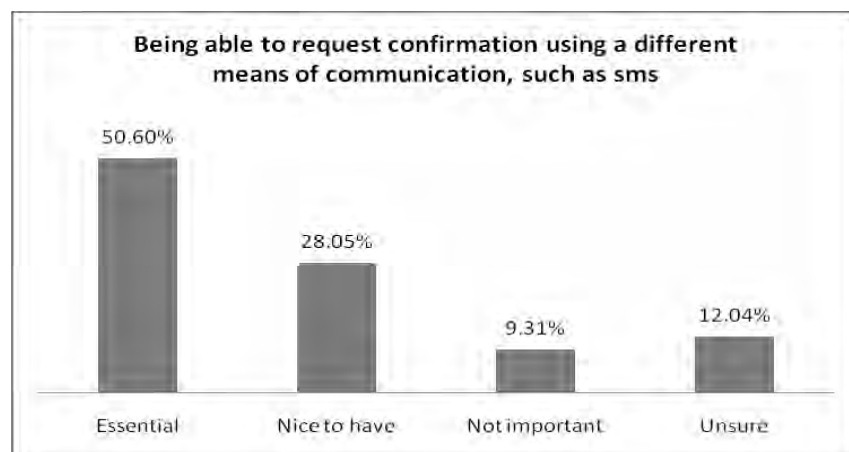


Figure 6.19: Ability to verify votes through different channels such as SMS

6.5 Analysis by respondents' education

It was discovered from the survey outcome that the respondents' education level was the main factor which reflected their acceptance of I-voting. The survey outcome with regard to each educational level is, therefore, shown in Table 6.1.

Table 6.1: Results by different education levels

Key to Education levels: P= Postgraduate, U= University, C= College, S= Secondary school

Education level*	S	C	U	P	Comments
<i>Biggest age group</i>	18-24	18-24	30-39	30-39	
<i>% with good level of computer knowledge</i>	91%	97.3%	96.9%	80.8%	Some over-confident in their computer knowledge. Postgraduates more aware of what they did not know.
<i>Confidence in Qatari general elections</i>	64.2%	50%	63%	70%	Government builds trust in the community by proving transparency, e.g. the E-government, global transparency ranking for Qatar. So varies slightly with participant's beliefs
<i>Preference for Online voting</i>	71.5%	71.6%	74.5%	74.7%	No significant difference
<i>Use e-services</i>	19.7	24	33%	52.8%	Postgraduates use more e-services due to their greater responsibilities
<i>Online voting for citizens abroad</i>	41%	45%	40%	46%	No significant difference
<i>Preference to vote at Qatar embassy</i>	45%	44%	55.4%	46%	Most participants would prefer to use I-voting from an Embassy of

Education level*	S	C	U	P	Comments
					Qatar because of the trust issue
<i>Comfortable with I-voting</i>	71.6%	71.6%	74.5%	74.7%	No significant difference
<i>I-voting gives sufficient privacy</i>	78%	61%	73.5%	73.6%	No significant difference
<i>I-voting free from outside influence</i>	82.1%	78.1%	76.8%	78%	No significant difference
<i>I-voting secure</i>	75.7%	69%	71.7%	71.3%	No significant difference
<i>I-voting unnecessary</i>	12.8%	11.6%	7.6%	12.6%	No significant difference
<i>Technology too difficult for some to understand</i>	32%	24.3%	32.8%	31.1%	No significant difference
<i>Computer hacking a problem</i>	21.5%	25.7%	25.1%	18.5%	Postgraduates are less concerned, believing that available solutions can overcome the problem
<i>Can't check vote</i>	11.5%	14.5%	13.5%	13.3%	No significant difference
<i>Vote selling a problem</i>	8%	8.5	7.1%	8.15%	No difference. Participants share the same low concerns due to faith and trust in government
<i>Need system to confirm who is voted for</i>	77.5%	81.5%	78.5%	71.4%	Postgraduates are less in favour of these features, probably reflecting their belief that such features could help vote selling
<i>Need ability to check vote has been counted</i>	83%	82.1%	81.5%	73.6%	
<i>Need ability to confirm with alternative media</i>	78.4%	78.7%	79.8%	74.7%	
<i>Technology may not be reliable</i>	11.9%	14.6%	13.2%	13.3%	No significant difference

In conclusion, the responses indicate that there is relation between participants' education and their willingness to participate in I-voting, but only if the education is at postgraduate level. People educated at that level were more experienced in e-services and this seems to give them more confidence in Internet transactions and fewer concerns about I-voting.

Furthermore, it can be concluded that there are many encouraging factors for the vision of I-voting. However, there are some barriers that will need to be countered to provide an effective I-voting experience in Qatar. With regard to I-voting features, participants believed that usability, confirmation and verification of vote are essential. Therefore attention would need to be paid to these features in any I-voting system to fulfil their requirements and for the system to be considered adequate and effective. Table 6.2 shows the willingness of Qataris towards I-voting versus the barriers that would inhibit it.

Table 6.2: Factors constituting willingness and barriers towards I-voting

Willingness	Barriers
<p>High confidence in general elections in Qatar.</p> <p>Majority comfortable with idea of I-voting.</p> <p>Preference to vote online instead of visiting a polling station, especially citizens abroad.</p> <p>Most believe it provides comfortable, private, secure, independent voting to some extent.</p>	<p>Preference for personal interaction</p> <p>Lack of belief that such a system is needed</p> <p>Concerns over:</p> <ul style="list-style-type: none"> • Security issues • Usability issues • Restrictions of Internet use • Vote manipulation • Vote selling.

6.6 Chi-squared test

In this research, the chi-squared test (χ^2) was applied to discover the relationships between the responses gathered in the survey according to the following hypotheses:

H0= The two responses are not related

with

H1= The two responses are related

χ^2 was calculated using the following formula: (Bock, Velleman and De Veaux, 2007, pp.608-615):

$$\chi^2 = \sum 2 n_i \ln \frac{n_i}{e_i}$$

where n_i is the observed number of individuals in category i and e_i is the expected number of individuals in category i .

In this research, the value of P (level of significance) is usually 1%, 5% or 10%. For a small P value, χ^2 is larger and this leads to the rejection of H0. Therefore, 5% was chosen as the target level. An online chi-squared calculator (Kirkman, 1996) was used.

There were some potential relationships between the different variables examined in the survey. These were tested and the results are given in Table 6.3.

Table 6.3: Relationship between survey responses

	C1	C2	C3	W1	W2	W3	W4	W5	W6	F1	F2	F3	B1	B2	B3	B4
B5	N	P	N	N	P	N	P	N	P	P	P	N	N	P	P	P
B4	N	P	N	N	P	P	P	N	P	N	N	N	X	N	P	
B3	P	P	N	P	P	N	N	P	P	P	N	N	P	X		
B2	P	P	N	P	N	P	N	P	N	P	P	N	X			
B1	P	P	N	P	N	P	N	P	P	P	P	P				
F3	N	P	P	N	P	N	P	N	N	X	X					
F2	N	N	P	P	P	N	P	P	P	X						
F1	N	X	P	P	P	N	N	P	P							
W6	P	N	P	X	P	X	X	X								
W5	P	N	P	X	N	P	X									
W4	P	P	P	X	P	X										
W3	P	N	P	X	P											
W2	P	X	P	P												
W1	P	N	P													
C3	P	P														
C2	N															

Key:

P = Positive correlation

N=Negative correlation

X=No correlation

Personal characteristics:

C1: Good computer and Internet knowledge

C2: Internet used for banking and e-commerce

C3: Confidence in general elections in Qatar

Willingness to use I-voting:

W1: Online voting is the preferred voting method

W2: I-voting should be used by citizens abroad

W3: Comfortable with voting online

W4: Confidence in privacy of online voting

W5: Confidence in being free from influence if voting online

W6: Confidence in security of online vote

I-voting features required:

F1: Confirmation of who is being voted for

F2: Verification that vote has been received

F3: Verification via alternative media

Barriers considered important

B1: Technology would be too difficult

B2: Technology may not be reliable

B3: No means to check a vote

B4: Computer hackers may influence the vote

B5: Vote selling is a problem

Table 6.3 shows the following interesting correlations:

There is a significant correlation between the following variables

1. Frequency of use of the Internet for online banking or making online purchases with the belief that citizens abroad should vote online. This agrees with the finding that postgraduate educated voters, who had greater experience of e-services, had fewest concerns about Internet voting security (see Section 6.5).
2. Respondents that do not use online banking or e-commerce with those that do not believe there should be I-voting in Qatar.
3. Respondents with low computing knowledge with those who do not believe there should be I-voting in Qatar.
4. Respondents who are confident in the accuracy of Qatari elections with those believing that I-voting is unnecessary.
5. Respondents who would prefer to vote online with those who do not have concerns about the security of I-voting and those that believe they would be free from outside influence in their voting.

6.7 Conclusion

In conclusion, the survey has assisted in discovering Qatari citizens' views on the barriers to I-voting, their willingness to participate in I-voting and the features of I-voting that Qatari citizens would want to have. In general, the willingness to participate in I-voting is indicated by the high computer knowledge (more than 56% with pretty to expert knowledge), high usage of e-services (about 40%), and the trust in general elections in Qatar (48%), as well as more than one third of people indicating a preference for I-voting over traditional methods, even for citizens abroad.

Furthermore, the survey shows 30% of participants were comfortable with the idea of I-voting and more than a quarter are confident their privacy and security will be ensured and 39% of them believe they will be free from undue outside influence on how they vote. In general, the willingness to participate was considerably higher for people who use e-services than those with no experience of them. It was discovered that education level has a major effect on people's responses to the survey, mainly when the education is at postgraduate level.

Although there is a lot of willingness, there are some barriers to I-voting needing to be considered before the introduction of I-voting. More than one third believed there were difficulties with the technology, including the use of computers and the Internet; about one quarter stated that I-voting is not secure enough for vote casting since it is vulnerable to computer hackers; about one seventh believed the system would not be reliable or accurate as it would be difficult to inspect the election results; one tenth think there is no need for I-voting and less than this proportion were concerned about the possibility of vote selling with this technology. Also, there might be a barrier in that some people simply prefer personal interaction, a problem many participants referred to regarding the problems of using e-services.

However, it was clear from the results that a significant number of people did not feel confident to give a strong answer either for or against the idea of I-voting. There is clearly a great deal of uncertainty. According to discussions subsequently held with 10 questionnaire respondents, the majority suggested the need to see what I-voting would be like in reality in

order to assess its acceptability. About half felt it would be essential to have a means of vote confirmation and verification to ensure voters have successfully cast their votes and to assist in the auditing process if there is a need for it.

The survey demonstrates some significant correlations between different survey variables including: participants who do not use online banking or e-commerce with those that do not believe there should be I-voting in Qatar, participants with low computing knowledge with those who do not believe there should be I-voting in Qatar, participants who are confident in the accuracy of Qatari elections with those believing that I-voting is unnecessary and participants who would prefer to vote online with those who do not have concerns about the security of I-voting and those that believe they would be free from outside influence in their voting.

As a result of the findings in this chapter, it was decided to conduct an experiment to experience I-voting in reality with a system with all the suggested features that may be introduced in Qatar elections in the future to evaluate people's acceptance of this technology.

The next chapter describes the development and results of the I-voting experiment to assess people's acceptance of such technology in Qatari elections. Also, to compare results with the Estonian election and to review both cases to learn for future development.

Chapter 7 Experimental Study: Comparison between Qatar and Estonia in Acceptance of I-voting

This chapter discusses the instigation of a voting experiment utilizing a prototype I-voting system to assess the feasibility and acceptance of I-voting in Qatar in terms of technical solution, voters and election committees. The prototype was developed according to Qatar's election requirements and voting principles. The voters' behaviour and experience were assessed by means of questionnaires and interviews. Furthermore, a member of the Qatar Election Committee kindly assisted in the experiment by checking the vote counting to assess the accuracy of vote results. A comparison is provided between the outcome of the experiment and the outcome of the Estonia general election held in 2007. From this comparison, a lesson can be learnt on how to overcome possible obstacles when introducing I-voting in Qatar's election. This chapter satisfies objective 6 (see section 1.5).

7.1 Experiment methodology

In this chapter, an experimental case study of I-voting in Qatar was carried out, to investigate: the security of the approach, the election environment, the acceptance and trust of the people, system usability and accessibility, the transparency of the process and the quality of I-voting system. Comparisons were then made with the Estonian experience reported in the literature.

According to Abercrombie et al. (1984) and Campbell and Stanley (1966) case studies are an ineffective research methodology since they do not provide reliable information about the broader subject. Nevertheless, case study methodology has recently become more common in research, showing its success in exploring many subjects effectively (Ragib and Becker, 1992; Stake, 1995; Yin, 2003a,b).

The research community has identified (e.g. Jensen and Rodgers, 2001; Perry, 2001; Welman and Kruger, 1999; Myers, 1997; Tellis, 1997; Cavaye, 1996; Yin, 1994) case

studies as empirical work deployed to investigate a phenomenon. Yin (1994) thus states the purpose of a case study is to investigate a phenomenon in real context. Furthermore, Stake (1995) defines a case study as “*the study of the particularity and complexity of a single case, coming to understand its activity within important circumstances*”. Others (e.g. Alavi and Carlson 1992; Orlikowski and Baroudi, 1991) have added that it is a common qualitative method.

According to Yin (1994), there are different types of case study, determined by three choices:

1. Is the research exploratory, explanatory or descriptive?
2. Does the research cover a single case or several cases (multiple case studies)?
3. Does the study follow an embedded or holistic design?

The case study methodology is an ideal technique for investigating I-voting acceptance in Qatar and answering the research questions identified for this experiment, which is targeted at determining.

- 1) Whether the I-voting prototype was designed according to Qatar’s election requirements,
- 2) Whether Qataris would accept I-voting after using the prototype,
- 3) How effective the prototype is in fulfilment of voting principles and overcoming the possible I-voting challenges,
- 4) What the differences and similarities are in I-voting between the Estonian and Qatari case studies.

Hence, this experiment is a combination of exploratory and descriptive case studies. Furthermore, it is a multiple case study involving both Estonia and Qatar. An embedded case study involves more than one unit of analysis in the same context, whereas a holistic case study involves only one unit of analysis. Since this experiment only addresses one unit of analysis which is to determine the level of acceptance of I-voting by Qataris, this experiment will be a holistic case study.

There are different categories of case studies defined by Jensen and Rodgers (2001: 237-239):

Snapshot: A comprehensive study of one research area at one point in time.

Longitudinal: A quantitative and/or qualitative investigation of one research study at multiple time points.

Pre-post: The study of one research entity at two time points delineated by some critical event.

Patchwork: Defines a comprehensive vision of the research since several case studies are used for one research project (e.g. snapshot, longitudinal and/or pre-post).

Comparative: Uses various case studies for different research to provide a comparison.

This research used a combination of both pre-post and comparative case studies which aimed at studying Qataris' acceptance of I-voting in Qatar after the critical event of being in an experiment involving a prototype of I-voting. It also provided a comparison of Estonia's experience in I-voting and the outcome from Qatar's experimental case study. Yin (1989, 1994) claims that case studies could involve several data collection methods such as observations, interviews and surveys. In this experimental case study, questionnaires and interviews along with observation were used.

7.2 Experimental process

There are many I-voting approaches and solutions suggested in the literature (Krimmer et al., 2008). Each has its own advantages and disadvantages. This research attempts to assess the feasibility and acceptance of I-voting in Qatar by means of an experimental case study, a unique system was proposed for use.

The process of the experiment involved four phases to achieve the overall aim of the study:

- 1) Plan and design the experimental systems,
- 2) Test the system and experimental performance,
- 3) Analyse the results and discuss the findings,
- 4) Finally, compare and contrast the results and findings with the Estonia I-voting case study (see Figure 7.1).

Each phase is explained as following sub-sections.

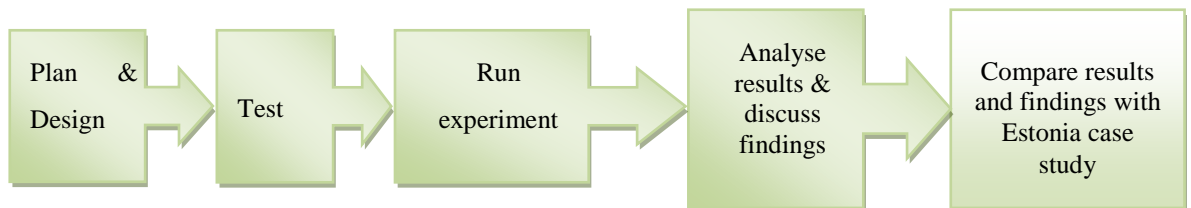


Figure 7.1: Experimental process

7.2.1 Plan and design

The I-voting application design used in this experiment was based upon best-practice, and made in accordance with the Qatar election .. Considerations have been given to fulfilment of voting principles and their applicability to the situation in Qatar.

A face-to-face semi-structured interview was held with Abdul Rahman Al-Sulati, the head of the Permanent Election Committee in MOI, to discuss the process of replacing manual voting with I-voting. This interview included a discussion which identified the

requirements for introducing a successful I-voting system in Qatar. Since the system is Internet-based, there is almost no limit to the number of personal computers which can be used to send information to the system.

The main outcome from the interview was to identify Qatar Election requirements for the voters and the system:

1. The original citizenship of voters must be Qatari or Qatari citizenship must have been granted at least 15 years earlier.
2. Voters must be aged 18 years or more.
3. Voters must not be convicted of dishonourable crime unless rehabilitated.
4. Voters must be resident in the electoral constituency in which electoral rights will be exercised.
5. Voters must not be employed by the armed forces or police.
6. Multicast voting must be forbidden.
7. The system must be easy to use and must have a Qatari 'look and feel'.
8. The system must satisfy basic voting principles such as security and anonymity.

A simple design was used, which required only a limited number of resources. Where votes are encrypted. This encryption system is based on private and public keys. A public key is given to the citizen in order to secure their data. The private key is used by the server to identify and confirm the eligibility of the voter while the design was simplified compared to other I-voting models, it allowed for a pilot study which determined the acceptance by the Qatari people of such a new technology. The algorithm was designed to ensure that the anonymity of the voters is maintained with the strictest confidence.

There were two experimental viewpoints:

- (1) the voter environment, which allows authorised voters to cast their votes.
- (2) the permanent election committee environment, which allows the committee to view the election results.

7.2.2 Test

After the design had been implemented and tested successfully by two computer experts from Almajaz Telecommunication Company, the testing and evaluation of the developed I-voting prototype was carried out by the researcher to assess its effectiveness in terms of fulfilment of voting principles (See section 1.1). Semi-structured interviews were held with the two computer experts in order to evaluate potential threats to the source code. They were asked questions oriented towards the technical aspects of the system and its ability to meet the voting requirements of Qatar. The experts were testing the functionality of the I-voting system based on the document provided by the researcher (See appendix C).

The experts believed that the system was sufficiently usable to act as a pilot study, providing a demonstration of how I-voting could take place in Qatar. They indicated that they thought it was well structured and easy to use, even by novice computer users. However, they said that it would only be useful on a small scale for demonstrating I-voting. This is due to the infrastructure employed to run the application which was only capable of handling an experiment and would not be practical for large-scale voting. They indicated that it would be unstable for larger scale application. Additional resources, servers and more advanced infrastructures would be required to introduce I-voting throughout Qatar for all its citizens. Also, the programming language (Visual Basic) used in the application was not capable of managing large scale operations and so they suggested using a more robust programming language, such as Java or PHP for a full scale implementation. Furthermore, the experts stated that the application required improvements to provide more authentication factors, such as the use of a smart card and biometrics. Also, the system needs to provide a method for distributing the required PIN for logging-in to the system, such as through SMS to ensure privacy. In addition, there is a need for advanced encryption method such as 3AES and a combination of mix-networking and blind signature to maintain anonymity. Additional suggestions were to provide a backup for recounting through paper-based voting and enabling a third party to monitor the integrity of voting processes.

The experts also suggested having an awareness programme and training sessions for people, especially those with little computer knowledge, to enable them to use the system easily. It was suggested that the media, academics and employers should play a role in the awareness programme to help introduce the society to such a new technology. The experts voiced the opinion that the I-voting system developed was a good step for Qatar since it was uniquely designed to fit Qatar's election requirements. However, they suggested a lot of improvements in the application are required before moving from the experimental stage to large-scale application (see Appendix B).

7.2.3 Running the experiment

After ensuring that the I-voting system was functioning properly, the experiment was carried out with a sample of 86 eligible Qatari voters from different demographic backgrounds (age, education and computer knowledge) selected by convenience from friends and relations of the researcher. Due to the large participant sample size, the experiment was held in 5 sessions each involve about 17 participants. This would ensure that all participants had adequate resources to participate in the experiment and the researcher had the capability to observe and assess their acceptance. The participants were motivated to join in the experiment by invitation letters which explained its significance and the importance of their participation. They were then given a consent sheet to sign, indicating their willingness to participate in the experiment and ensuring their confidentiality. Participants were given an oral short presentation which took ten minutes explaining about the I-voting prototype capability and how it worked (See Appendix B). The participants were asked to vote through the I-voting system within a maximum of 5 minutes including the time for authentication and vote casting (see Appendix B).

Later, the participants were asked to provide feedback on a questionnaire to evaluate and assess how acceptable they found the I-voting in practice and to determine the nature of any barriers to successful implementation that may exist. The questionnaire consisted of two sections, a background section and a post-ballot section. In the background section, the voters were asked to provide some background information about their gender, age, occupation, computer literacy, previous voting behaviour, and

their opinion of I-voting and the effects of ICTs on society. In the post-ballot section, specific questions were asked about the usability of the system, the quality of the system in terms of secrecy (privacy) and security (against fraud), about their viewpoints related to I-voting and some questions related to the voters' identity (see Appendix B).

An independent observer from the Qatari election committee (QEC) was involved at the end of each session to inspect the vote counting, where votes were counted manually and compared with the vote counting shown in the I-voting system in order to determine the accuracy of the I-voting counting process.

7.2.4 Analysis of results & discussion of findings

After the experiment, the questionnaire results were gathered and analysed quantitatively and qualitatively. Both the positive and negative reactions of voters were examined, as well as their ability to use the technology successfully. The results of this study indicated that the overall reaction of the voters towards the I-voting system was favourable. There was a high correlation between pre-voting anxiety and good perceptions of the new system. The vote casting stage had a slightly less positive reaction due to problems regarding the functionality of the system. There were difficulties with the pictures of the candidates, graphics describing how to use the new system, and explanations of encryption and decryption. The studied results indicated that voters reacted to the electronic system similarly to the traditional voting methods. However, individuals with high degrees of anxiety regarding the system often recorded a less positive experience with the new technology. The election committee showed their acceptance of the proposed system and of the accuracy of vote counting as result of comparing the manual count matched the electronic one.

7.3 Reasons for the comparison with Estonia

Estonia was chosen for a comparison with Qatar case study because it shares some similar characteristics to Qatar:

- (1) the small country size
- (2) rich in computer literacy and Internet access
- (3) the people's and government willingness
- (4) a well-established of IT infrastructure
- (5) an E-government portal which used Smartcard, e-certificate and e-signature are deployed and in operation since 2003 (Ministry of Foreign Affairs, 2007b).

However, there are some differences and similarities in election environment of both countries which has to be considered in the design of I-voting.

Elections in Qatar are limited to the Central Municipal Council (CMC) at this moment but, the Emir established the Permanent Elections Committee (PEC) of the Supreme Council for Family Affairs in 2003 to raise public awareness of voting rights and responsibilities and to empower citizens, particularly women, to prepare Qatari people for future parliament election. Qatar is divided into 10 Municipal areas. The election committees are responsible for validating candidate applications. By law, voters are invited by letter to participate in the election. Each voter should register and the staff committee should use ID cards to verify the identities of the applicants and whether they fulfil the conditions to contest the CMC elections. The voters are only allowed to register in their district area. The voters will be flagged as having voted once the voter has cast his/her vote. Any blank vote card would not be counted.

In comparison, in the Estonian electoral system, the country is divided into 12 multi-mandate electoral districts. The law permits advance voting by means of paper-based votes at a polling station or Internet voting from anywhere. Voters who choose to use paper-based voting have to register with the National Election Committee (NEC) in the voters' electoral district. Internet voting offers a registration-free process that means voters do not need to register, but simply use their e-ID card to vote online. In paper-base voting, voters write the registration number of the candidate of their choice to cast the vote.

7.4 Technical details

This section described how the experimental system was inspired by the Estonian system (see Table 7.1). The Estonia case study was based on available reports obtained from the European Union Democracy Observatory (EUDO,2007) and the Estonian National Electoral Committee (2007a,b). Solvak and Pettai (2008) have drawn up an overview of Estonia political concerns.

Table 7.1: The technical details of Estonia experiment and Qatar case study

Qatar Experiment	Estonia Election
Theoretical approach	
<p><u>1. Authentication Stage</u></p> <p>1.1) Voters insert an e-token (instead of a Smart card), which has public and private keys, then type their own password to be identified by the authentication server.</p> <p>1.2) The authentication server checks if the voters are eligible for voting.</p> <p>1.3) Eligible voters receive an e-certificate from a certificated authority (CA) server. This would be stored in the voter machine to be used in vote casting to digitally sign the vote.</p> <p><u>2. Vote casting Process</u></p> <p>2.1) The voter chooses a candidate. The vote is then concealed using a blind signature algorithm, e-signed using a digital certificate, and encrypted using a public key and sent to the election committee server (trusted third party) to confirm the vote and to add their e-signature. A copy would be made by this</p>	<p><u>1. Authentication Stage</u></p> <p>1.1. The voter inserts a Smart card to a card reader and then types their PIN1 (This system use two PINs). The server then checks if the voter is registered in the eligible voter database.</p> <p>1.2 The authentication server checks if the voters are eligible for voting.</p> <p><u>2. Vote casting Process</u></p> <p>2.1. A screen with the candidate names would appear allowing the voter to choose one candidate and confirm their choice.</p> <p>2.2. The vote is then encrypted using a public key obtained from a Counting Server. Also the voter types a second PIN (PIN2). PIN2 is used to digitally sign the encrypted the vote.</p> <p>2.3. Data is then sent to Internet Server to check the validity of the digital signature to ensure data integrity.</p>

<p>server.</p> <p>2.2) The election committee server sends back the voter data to the voter to check the integrity of the data, the voter e-certificate is flagged to show the user has voted and can't vote again.</p> <p>2.3 The voter sends back the data to the application server (this server is a front server consisting of several servers connected internally) to eliminate any attack on the actual servers:- The first server checks only the validity of the vote and keeps a copy of data for auditing. This server has only the (e-token) private key to decrypt the data. The second server has the Election Committee private key to decrypt the content and count the votes.</p> <p>2.4) The Application Server acknowledges to the voter that the vote has been received without confirming the choice.</p> <p><u>3. Counting Process</u></p> <p>3.1) The Counting Server and Election Committee Server compare both lists to check the integration of data (the data was not altered by an insider) then the Election Committee server decrypts the data using their private key which no one else has knowledge of.</p> <p>3.2) The Count Server computes the results</p>	<p>2.4. The Internet Server then sends the data to Vote Storage Server, to check the validity of the voter's certificate from the CA Server. If valid, the Internet Server verifies the digital signature using the voter's public key from the voter's certificate.</p> <p>2.5. The Vote Storage Server sends an acknowledgment to the voters through the Internet server to inform the voters that their vote casting was successful.</p> <p>2.6. The vote is kept in the Vote Storage Server to perform vote counting on election day.</p> <p><u>3.Counting process</u></p> <p>All entries transferred to the Counting Server are logged</p> <p>3.1. A list of votes is sent to the Counting Server by CD-ROM. The Counting Server decrypts the votes using the Hardware Security Module (HSM) and performs counting.</p> <p>3.2. Results were then published and viewed in a spreadsheet.</p> <p><u>Notes:</u> (1) Any communication between voters and server is secured using an SSL connection.</p> <p>(3) The HSM required six physical keys. By law, at least half of the NEC members must be present in order to decrypt and count the votes.</p>
---	---

Election environment	
<p>With I-voting, a similar process would take place: (1) invitation letters would be sent to voters (2) the voters already have their own Smart card since Qatar law requires every adult to obtain a card to perform any government services. (3) The voters would access the Internet voting website and follow the instructions e.g. a video demonstrating how to vote.</p> <p>In this experiment, voters were allowed to vote only one time.</p>	<p>Internet voting offers a registration-free process that means voters do not need to register, but simply use their e-ID card to vote online. In paper-based voting, voters write the registration number of the candidate of their choice to cast the vote. With Internet voting, voters simply select the candidates from options. The NEC allowed the voter to overwrite their vote multi-times using Internet voting only, only the last vote would be counted. Voters were also allowed to vote using Internet voting and then change it at the polling station but it would then be final. Internet voting is used only in advance voting, so voters would not be able to use I-voting on election day.</p>
Acceptance and trust	
<p>In this experiment, the e-voting system was not used in a real election, but an experimental election was set up to record people's experiences and comments.</p>	<p>In the Estonian case, no direct study examined people acceptance. Therefore, the author had to rely on turnout statistical data obtained from the National Election Commission.</p>
Usability and accessibility	
<p>To facilitate the registration phase, the experiment uses e-token which is "<i>USB plug and play</i>" which does not need any installation. A simple interface design was applied similar to the ballot paper currently in use in traditional voting. The system was designed to provide more information as each entity appeared on the screen for people who needed more information e.g. the login screen ask for username and PIN, users can hover</p>	<p>Internet voting in Estonia uses an e-ID card, for identification via the Internet and to sign documents digitally. Voters must obtain a Smart-card reader, in order to authenticate voter in the Internet voting application. The voters must download and install voting software from the Election website. Three different operating systems (OS) were used for voting applications. Statistically, Microsoft Windows, Mac OS and Linux were used</p>

over the entry field for more help information	98.9%, 0.75% and 0.42%, respectively. The voting application interface was a standalone program that used a simple and easy to apply with Estonian language interface.
Security	
The main security of the system relies on the use of a smart card, blind signature and encryption.	The most important part in the security in Internet voting system is related to the separation between the storage of the vote and its counting. Storage of a vote is carried out on a server connected to the Internet whilst the Counting Server is disconnected from Internet.
Transparency	
In this experiment, transparency was considered by using open source algorithms which guarantees anonymity, the so-called “blind signature” (Chaum, 1983).	Estonian I-voting tries to make the process as transparent as possible by getting people and experts involved. Also procedures were defined and the law modified to cover I-voting problems.
Quality	
Since the system was laboratory based, the existence of real attacks were not encountered. The experiment was not designed to stress the security of the system, more its usability. Therefore, the quality of the system were mainly focused on the usability, accessibility and how people found the quality of their experience. Furthermore, the people who used the system at the same time were only 17. The experiment relied on the quality of the Interface design and the time that the system takes to respond for the user request. Additional experiments need to be done to fully consider the quality part of this system.	Estonian Internet voting has not been independently tested. No full end-to-end accuracy test has been held (OSCE, 2007). The auditing is carried out by an external company that observes and checks the performance of the NEC against written documentations.

7.5 Results

The results of the experiment were gathered from questionnaire responses with participants and evaluation by experts, and the two election committees. A summary of questionnaire results and findings is shown in Table 7.2.

Table 7.2: Questionnaire results

Questions at registration			
Question	Yes	No	Researcher comments
Did you find problems at the authentication stage?	52%	48%	Due to use of e-token instead of smart card. The Smart card application would load needed files automatically but e-token files must be uploaded manually.
Did you find authentication process secure because it asks for two factors?	83%	17%	Using two or three factors of authentication would provide superior security.
Did the system identify you without problems?	90%	10%	10% of participants experienced a problem in identifying themselves to the system due to forgotten PIN numbers. To overcome this, it would be necessary to provide a method of delivering the PIN for each voter when needed (Key distribution management should consider sending the PIN via SMS, for example).
Was the e-token easy to install?	100%	0%	It was USB plug and play, which participants can handle easily.
Were you concerned about what would happen to your e-token, if it is lost?	66%	34%	A presentation to the participants explained that the e-token alone would not work. It would require a second authentication factor, the personal PIN number.
Was the process fast?	40%	60%	This is due to 52% asking for help

Vote casting phase			
Was the quality of ballot design maintained?	90%	10%	The interface design was kept simple, keeping the look and feel of a Qatar election.
Was the system fast?	100%	0%	The experiment was held within a lab set-up so this result is assumed to be because the system had all resources in place.
Did you have any problems at the voting stage? If yes, please write it down.	12%	88%	Some problems with identifying IP addresses of voter machines. In some machines, the IP address was not registered in the server set-up for the experiment.
Did you find confirmation of the vote received useful?	77%	4%	Not everyone completed this question. Some requested the receipt of voting to include the voter's choice along with their ID number so they could request an appeal if needed.
Did you feel the same experience as with paper based voting?	45%	55%	Some felt I-voting was better than paper-based voting since they did not need to queue for hours. Others found traditional voting more exciting and worth the effort.
Other questions			
Was the presentation given on how system works useful to build trust and confidence?	84%	16%	The presentation argued awareness is a key element in bridging the gap between trust and sociological beliefs. The results confirmed 84% found awareness useful and 32% of voters changed their minds after the presentation.
Did the presentation change your mind about trusting the system?	23%	77%	

The above findings in Table 7.2 from the experiment were compared with I-voting in Estonia, showing the similarities and differences between the results of each case study (see Table 7.3).

Table 7.3: Comparison between Qatar and Estonia Results

Acceptance and trust	
Qatar experiment	Estonia election
<p>In the survey described in section 6.2, 76% of the 2,567 eligible voters who participated said they would prefer voting online rather than through the use of polling stations. Participants in this experiment confirmed their acceptance of the concept of I-voting after using the system to cast their vote. At the registration stage, 83% of 86 participants felt secure due to the combination of authentication factors used (note: the author had explained to participants that an additional factor of authentication would be added e.g. biometrics to achieve a high level of authentication) .the remainder had some difficulties during the authentication stage. Furthermore, trust on government was found by earlier research (see section 6.6) however, only 4% distrust the Qatar election. In this experiment, participants had mixed feelings, trusting the government but not the technology, especially in preserving voting anonymity.</p>	<p>In 2009. 24.3% (140,846) of vote was casted over the Internet. 580,264 used traditional voting.</p> <p>The usage of I-voting has increased ever since I-voting was introduced in 2007. In the Parliament election in 2011, it was reported that voting over the Internet has reached 35% (EUDO, 2011)</p> <p>This could be a significant sign that the Estonian people accept voting over the Internet. On the other hand Internet voting did not significantly increase turnout. The author has argued that increasing turnout could be obtained by providing a different voting channel e.g. mobile voting. However, there was no evidence that this would maintain high turnout in this election.</p>
Usability and accessibility	
<p>The participants were asked at both stages (registration and vote casting) about usability. More than 52% of participants asked for help at the registration stage although in this experiment we used an e-token, a “<i>USB plug and play</i>”, which does not need any installation.</p>	<p>The result from the recent election in 2011 shows that 35% of voters casted their vote using the Internet. This provides significant evidence that I-voting within Estonia is useable and accessible.</p>

<u>Security</u>	
<p>The security is based on smart card and blind signatures. According to the experts evaluation, the security of the system showed strengths and weaknesses as follows:</p> <ol style="list-style-type: none"> 1. The voter would interact with one online server while other servers are offline. This would reduce the consequences and risk of attack on the one server which only forwards voter requests. 2. E-tokens are used to act as Smart cards to authenticate the voters. 3. An e-certificate is downloaded from the CA server. This would reduce the voting process, instead of physically registering to obtain the certificate, the voter can download it online during authentication. 4. A blind signature is used to make the process anonymous. 5. A member of election committee has to enter their secret key to make sure votes are not altered. 6. Voters digital certificates are modified to show that voters have already voted. (One vote per a voter is maintained.) 7. Only Qatari IP addresses are allowed to access the system. In this experiment, the system only allowed a limited set of IPs to use the system. 	<p>The security is based on the separation between the storage of the vote and its counting. The following protocols are employed to maintain security:</p> <ol style="list-style-type: none"> 1. Integrity checking of the installed voting software, to ensure that the correct software is installed. 2. Setting up a firewall to secure the link between the Internet and the storage of vote by policing the traffic. 3. Monitoring the traffic to the Internet server in order to check potential attacks and malfunctioning. 4. Sealing and locking the Internet Server and the vote storage server in a place permanently protected by a police officer and CCTV. 5. Backup of the private key of one of the members of the NEC in case of failure of the HSM. This ensures the availability of the results of the Election. 6. To eliminate the possible attacks on a voter's machine. Three steps are considered: (1) Advise the voter to type directly the IP of the server in the URL of the browser, (2) Issue a certificate to the voter from the server (3) Check the integrity of the voting software by providing information from the server to the voter. 7. Allow voters to overwrite votes in order to reduce problems of privacy and vote selling.
<p><u>Weaknesses</u></p> <ol style="list-style-type: none"> 1. The client side still remains major concern in the system design. Alternative solutions, such as using a vote code sheet or using a 	

<p>secure operating system or browser are possible.</p> <p>2. Voters are not allowed to over-write their vote due to the law, which might create problems of pressure on the voter to vote for particular person. This could be especially true in Qatar culture where families are closely connected, and people respect and follow their head of family, such as the father or an uncle.</p> <p>3. The e-token was not totally secure in the experiment because it is simply a USB stick which has a PKI file.</p> <p>4. The counting stage, fails to provide evidence that all votes cast have been counted. Although the system was designed to keep a copy of the votes at the election committee server, no comparison was performed in this experiment. Comparing the votes in the counting server against votes in the election committee server would ensure no insider attack could change the votes,</p>					
<p><u>Transparency</u></p>					
<p>Transparency could be obtained due to the design which relies on validated technology. Attack from an insider is possible as the system relies on the government's integrity and their willingness to provide fair and free election. The source code was also inspected by two experts. In addition, participants were asked to suggest ways to gain transparency. suggestions were received as listed below:</p> <table border="1" data-bbox="304 1883 858 2033"> <thead> <tr> <th data-bbox="304 1883 576 1944"><u>Participant suggestions</u></th><th data-bbox="576 1883 858 1944"><u>Response</u></th></tr> </thead> <tbody> <tr> <td data-bbox="304 1944 576 2033">Receipt of my vote</td><td data-bbox="576 1944 858 2033">This would increase vote selling, but the system does send a</td></tr> </tbody> </table>	<u>Participant suggestions</u>	<u>Response</u>	Receipt of my vote	This would increase vote selling, but the system does send a	<p>The two main areas where the transparency is unclear: (1) The voters have no confirmation that their votes have been counted correctly, (2) the algorithm is designed to separate voter identity and choice to obtain anonymity. Moreover, there was no evidence of performing the separation of the vote identity. Nevertheless, the use of algorithms such as blind signature or mix-netting would guarantee anonymity (Chaum, 1981; Fujioka, et al., 1993). However, Estonia invited all political parties and qualified observers at</p>
<u>Participant suggestions</u>	<u>Response</u>				
Receipt of my vote	This would increase vote selling, but the system does send a				

	confirmation of the vote cast.	every stage of the Internet voting process, e.g. Inspecting the source code and setup procedures would gain trust and confidence in the system.
Involve a third party to monitor the process	The system requires a secret key from the Election Committee (third party), therefore, a third party is involved.	
Make source code available for inspection	In this experiment, the source code was public, and inspected by two experts	
Allow the head of a family tribe to monitor the voting process	In a real election, a representative of each party would usually be allowed to observe. Therefore, this would be possible if the law permits it.	
Allow foreign experts to observe the election process	This would be possible if the law permits it	
Although those comments are reasonable and can be achieved in future developments but amendments to election law would be needed.		
<u>Quality</u>		
<p>The quality outcome of this experiment was satisfactory, but it was in a lab session in which there was no outside or inside attackers.</p> <p>Experts who checked the software and the QEC officials who checked the count have found the system of good quality but not suitable for large scale in real elections and suggest the need for the government to support and improve the system and take it further from experiments to real elections.</p> <p>The majority (90%) had a positive feedback on the quality. 77% of the participants found that the design was straight forward and similar to the system that they use in the e-government portal. Voters simply needed to login and choose their candidate.</p>		<p>The final report for quality auditing was not published publicly. The auditing company has not been asked to conduct a further post-election test. Also, there is no clear information on government inspection of the software after receiving the system from the company. However, another third party company have perform the auditing other than the company who develop the system.</p>

7.6 Discussion of the results

This section draws a deeper analysis from the above table 7.3 discussing and comparing both the Qatari and Estonian case studies. Although, the Qatar experience is drawn from the boundaries of the laboratory experiment, there are still valuable points the government could draw from the comparison between Qatar and Estonia because both countries share so many similar characteristics.

Investigations of both case studies involved the following aspects:

7.3.1 Security of the theoretical approach

The approach taken in the Qatar experiment was inspired by Estonia's use of I-voting, which relies on state-of-the-art technology to achieve a high degree of security. Both approaches used the same technologies for authentication and confidentiality. Strong cryptographic solutions based on digital signatures and a public key infrastructure were used. However, in the Qatar experiment, the voters were supplied with an e-token (USB Stick) instead of a Smart card as used in Estonian. This does the same job as the Smart card but without the need for card readers. Both approaches were open to possible threats, such as from web side spoofing and malware which could lead to re-direction to a site other than the one apparently displayed on the screen (Jefferson, et al., 2004). The Qatari and Estonian systems used some different techniques and algorithms. For example, the Qatar experiment relied on the well known, Blind signature protocol to maintain anonymity (Chaum, 1983) whereas the Estonian system separates the identity of the voter from the vote before decrypting the votes for counting. The Estonian approach could be questioned as the voter gets no proof of the voter identity separation from the vote. This relies on trust that the government and National Election Committee (NEC) would do this process fairly. Both approaches have no comprehensive auditing system although, in the Qatar experiment, there was a suggestion that having an additional copy of the vote at the Election Committee server would enable comparison with the result from the counting server. However, this was not implemented due to resources limitations of the research. Also, both approaches fail to inform the voters that their votes were counted successfully, however, it can be argued that it is unattainable to maintain anonymity and give acknowledgements to the voters that their votes were

counted successfully. Basically, it will not be possible to investigate who cast each vote. In the Estonian approach, this option was possible but counting the vote is done after the election has ended. Votes are kept safely in a storage server, then transferred to counting server, thus proof of vote counting is impossible when the vote is cast because it is not counted at that time.

7.3.2 Election environment

Both countries need to change their current election laws to accommodate Internet world challenges e.g. the Estonian Election Act does not contain specifications of the Internet voting system, does not define the responsibility of any institution, and does not provide for sanctions in case of failure of the system (EUDO, 2007). Estonia and Qatar have e-Laws covering Public Key Infrastructure (PKI), digital signatures and digital certificates (ENEC, 2007a,b). Although Estonia has already made some changes to their laws, the laws need to be adaptable for change to accommodate the evolving nature of the Internet. For example, Qatar and Estonia consider that digital signatures are equivalent to traditional handwritten signatures obtained from users (Solvak and Pettai, 2008). Qatar has established the Computer Emergency Readiness Team (Q-cert), which is responsible for intercepting and dealing with Internet attacks. Also, it can communicate with similar organisations in other countries to react quickly to any incidents. In the literature, no record could be found of any Estonian plan to monitor the network to deal with Denial of Service (DoS) attacks (EUDO, 2007).

In the Qatar election, the voters were invited by letter asking them to participate in I-voting. 63% of participants felt that their contribution would be valuable for the research and this encouraged them to take part in a vote over the Internet. Whereas, in Estonia, voters were not invited by letter, but Internet voting is, nevertheless, becoming more and more popular, with 35% voting through the internet in 2011(ENEC, 2007a,b).

Furthermore, the size of both counties means they may be more adaptable to changes than larger countries. This is a particular advantage for Qatar where eligible voters number around 50,000 whereas in Estonia there are just over 900,000 (ENEC, 2007a, b).

7.3.3 Acceptance and trust

This section relies on statistical data. Both Qataris and Estonians show faith and trust in the system and government. In Qatar a national survey, held with 2,567 eligible voters, showed an encouraging outcome where 76% of participants said they would prefer I-voting (see Section 6.2). The experiment recoded 83% of participants believed the system was secure and useful. In Estonia, statistical data from National Election Commission (2007) shows a high percentage of voters use the I-voting system and this figure is growing day by day. Therefore, both countries share a great interest in using I-voting as additional tools for voting.

7.3.4 Usability and accessibility

With regard to usability probably a Smart card reader would have been easier for people to use since people are familiar with it in the e-government portal. However, this indicates that the usability of a system asking for hardware and software installation would be a problem for many voters. However, it could be argued that training to show the voters how the system works would overcome this problem, and the government should introduce I-voting gradually till technology can come-up with a better solution.

One question this research attempts to answer is, would I-voting increase people turnout for election? The question is challenging however, according to the author point of view it could attract new user's who desire to use the I-voting and gradually increase voter turnout especially if it was usable and accessible to all voters. Nevertheless, we must bear in mind that the increasing of the voter turnout affects by other factors.

- 1) Believing that one vote will not make different
- 2) People self-satisfy or distrust government

The accessibility of both approaches is similar, voters can use any operating system or Internet browser to cast their vote. Also, the software has the compatibility with tools and technologies that can help disabled voters. However, usability is a broad term. Installing hardware and software to perform the task makes it less usable, which is the case in Estonia. In the Qatar experiment, there was no additional hardware or software

required to cast the vote apart from plugging in the e-token (USB Stick). Participants found the Qatari system was easy to use.

7.3.5 Transparency

The Estonian system was not certified by an independent third party. In addition, no full end-to-end logic and accuracy tests were carried out. An auditing company has the responsibility to carry out a review of the election process. However, the final report is not public. Post-election audits were not requested from the company (OSCE, 2007). In Qatar, the experiment had an observer from QEC to check the accuracy of the counting process. Also two IT experts were asked to inspect the software. Participants suggested a few ways to enhance the transparency of the system (see table 7.3). Certain actions would help making the system transparent by involving the public and other parties. The observers can be divided into two:

- (1) Independent observers: These can be citizens, parties and third party observers as is normally the case in the traditional voting process to enable the population to be assured that the system is doing what it should do.
- (2) A Software Development Company: A company with a strong reputation for IT security needs to check the system against well-written documents such as the Council of Europe set of standards (2004) for e-voting. The outcome of their report should then be available to the public.

However, I-voting is an unsupervised election system, which means voters are using their own computers to cast their vote. This could be the weakest link in I-voting as there is no evidence of the voter's machine being secured. This could be a fundamental obstacle to making I-voting secure. Basically, computers need to be considered as untrusted and infected with harmful viruses and malware which could change a voter's choices at their own computer.

7.3.7 Quality

In the Estonian election, no security incidents have been reported. However, this is not evidence that none occurred. The I-voting deployment has been generally accepted by citizens, politicians, and election officials (ENEC, 2007a, b). This could be due to the fact that it was supported by the government of Estonia. In the Qatar experiment, there was no independent authority to examine the quality of the experiment although the researcher ask for independent observer two IT experts who checked the software and the QEC officials who checked the vote count. Moreover, participants of this experiment were asked about the quality of their experience in term of using I-voting compared to traditional voting. Qatar could clearly benefit from the Estonian experience in their efforts to achieve a high quality election process.

7.4 Conclusion

Implementation of Internet voting still remains a hard task in large-scale elections (Mohen and Glidden, 2001; Philips and Spankovsky, 2001). The Estonian experience could provide a solid basis for future development of I-voting in Qatar, since it has the advantage of highly innovative IT infrastructure, and Estonia is also a small nation.

The future challenges are:

- (1) to provide a mechanism to secure client machines (chapter 8 further investigates this aspect with further research to measure Qataris awareness of the need for securing their computer)
- (2) to bridge between what has been proposed in the literature and what is implemented in practice
- (3) to develop a set of standards for I-voting based on best of practices For example, the Council of Europe has developed guidelines and standards for certifying e-voting (Council of Europe, 2004).

The comparison between Qatar and Estonian was not a comparison of like for like, since Qatar was an experimental case study held in labs. However, this could be an introduction for future pilot projects and full testing for any further deployment of I-

voting. Qatar would need to amend the current election law to consider new features, such as over-writing a vote to reduce vote selling or family pressure.

The work described in this chapter could be used by the Government of Qatar to provide evidence for the feasibility of an I-voting system. Moreover, technology and IT management experts could learn from the results of the experiment carried out to enable them to better assist with the transition to I-voting, ensuring that the adoption of the new system does not interfere with the current processes which exist in Qatar.

Chapter 8 Assessment of Client side I-voting Security

This chapter presents a profile of voters' awareness of information security derived from a survey designed to measure the level of awareness on the client side of I-voting. The previous chapter has pointed out the risks that might appear due to lack of awareness of information security, which could put an otherwise very secure I-voting system in danger of manipulation by unauthorised persons.

8.1 Introduction

The client side remains one of the important issues in introducing I-voting and the SERVE report (Jefferson et al., 2004) stresses that the weakest link in this process is the voter's end device, as no matter how secure the voting protocol is, hackers can change the voter's vote before it is transmitted over the Internet. Volkamer et al (2006) describe a few methods to overcome the problem of insecure voter devices:

- (1) Providing training and raising the awareness of computer security.
- (2) Using a secure operating system.
- (3) Using trusted computing elements.
- (4) Using voting code sheets.

Jefferson et al. (2004) also argue that Internet voting has other security challenges because of the use of the Internet network, which is vulnerable to cyber attacks (insider attacks, DoS attacks, spoofing, etc.). I-voting has many challenges but, taking the example of the Estonian experience in using I-voting in a general election, these can be overcome. Although, in 2007, the system in Estonia failed due to a DoS attack after three days, this could be an acceptable experience as three days is a long time to carry out an election which could be carried out in one day. Furthermore, a secure voter machine would eliminate the DoS attack since attackers would need to use the voter's infected machine to strike. A reliable, trusted operating system could solve the problem.

Securing an I-voting system is shared responsibility of the developer and the user. Schneicher (2004) indicates that “Security is a process, not a product.” Therefore information security awareness is needed on the user side. The literature has argued that training and education could contribute and partly solve this problem (Aloul, 2010; Boujettif and Wang, 2010; Talib et al., 2010; Tolnai and von Solms, 2009; Meister and Biermann, 2008; Smith, 2006).

The conclusion from the literature is that the main problem facing I-voting concerns the threats associated with the client side, either due to the unsecure client machine (e.g. contain viruses, Trojan programs) or a lack of users’ awareness on information security (Gerck et al., 2001; Oppliger, 2002; Swiss Federal Council Report, 2006; Thielbeer, 2007). Therefore, a focus for this research is enhancing the level of client awareness on information security to achieve a secure and reliable I-voting system, especially on the client side.

To determine users’ awareness of information security, a survey entitled Computer User Security Awareness Survey, was distributed manually to 400 Qatar Foundation students and employees, who were Qatari citizens aged over 18, regardless of their background or education level, to obtain a broad spectrum of views. The return rate was 37.5% (150 completed questionnaires).

The results demonstrate that most participants behave inappropriately, leaving them at risk, even though they are aware of the risks. Finally, the study concludes that technical solutions along with training would enhance users’ information security knowledge, helping to eliminate client side risks.

This study will be used to assist the development of I-voting in the State of Qatar by giving an understanding of the users’ knowledge of the Internet and computer security to enable an appropriate solution. It shows more effort should be made in terms of practical training to solve the problem of phishing and that educational and training material about phishing can be presented in learning sessions, distance learning (e-learning), embedded training, regular learning messages or even through the media. (Kawakami et al., 2010).

8.2 Problem of awareness

The problem of security awareness of computer users has recently become apparent and some researchers (eg. Kvavik, 2004) emphasise that user awareness is a core element in securing the client side. For example, research by the EDUCAUSE Centre for Applied Research at the University of Minnesota was carried out to find the main common barriers in that university to effective IT security (Kvavik, 2004) (see Figure 8.1). The research shows that user awareness and other cultural factors are the second most major problem in US institutions, concerning 46% of IT users, which shows how much awareness is needed to prevent any security failures in an organisation. Moreover, a survey by the National Infrastructure Security Co-ordination Centre (NISCC, 2003) confirms that the top cause of corporate data risk (78%) is human incompetence and threats from disgruntled employees.

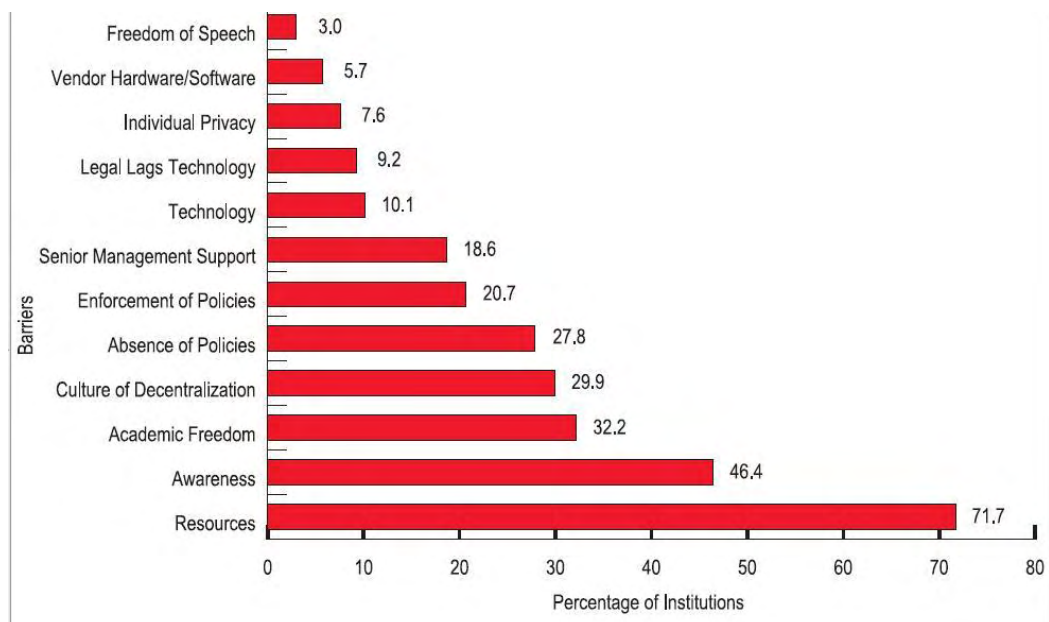


Figure 8.1: IT security barriers, University of Minnesota (Kvavik, 2004)

A survey in the UK (Furnell et al., 1999) to assess the awareness of the general public regarding computer crime and abuse showed that most people have the wrong idea about where the danger is coming from and who is responsible for it. In computer security, the media has a major influence on computer users' opinions, as the media tend to blame any computer breach on hackers. Moreover, they claim that hackers are knowledgeable in making cyber-attacks which can not be stopped. In reality, hackers

tend to attack the system from the weakest link, trying to find a “back-door” into the system in order to find a way to attack. Most computer users do not know how to configure their own computers to make them secure. In addition, the survey results indicate that 30% of participants believe that hackers are lonely, young, males without social skills, which shows a lack of awareness about hackers and their social skills which they use to trick their victims with so-called 'social engineering'. On the other hand, the media do help people understand that there is a danger of being attacked, showing them the type of crimes that might happen when using computers. The research shows that 80% of respondents felt that computer crime and abuse was a problem and most people consider computer crime is a serious concern (Furnell et al., 1999) (see Table 8.1).

Sabotage cyber-attacks have been recorded as a serious threat to business. Recently, some credit card companies were sabotaged by a group of hackers in revenge for suspending WikiLeaks' accounts (BBC, 2010). This type of attack has come from both “black hat” attackers, who have criminal intentions, and “white hat” attackers with non-criminal intentions. However, I-voting is expected to experience such attacks. Limiting access to I-voting within the country, so only people from Qatar have access to the system, could reduce possible security risks (see section 3.4). Although this will enhance the security of I-voting, it will make I-voting hard to access for overseas voters who would then have to vote in a Qatar embassy.

Table 8.1: Views on computer crime and abuse (Furnell et al., 1999)

	Very serious	←	Indifferent	→	No crime
Viruses	71%	17%	9%	1%	2%
Viewing someone else's data	29%	37%	25%	4%	5%
Altering someone else's data	80%	15%	3%	0%	2%
Theft of computer equipment	82%	15%	3%	0%	0%
Unauthorised copying of software	18%	22%	36%	13%	11%
Unauthorised copying of data	24%	35%	26%	6%	9%
Computer fraud	70%	20%	9%	0%	1%
Sabotage	90%	6%	3%	0%	1%

Security awareness is one of the most prominent security problems at the present time and research has shown (e.g. Aloul, 2010; Talib et al., 2010; Tolnai and von Solms, 2009; Smith, 2006) that the best way to tackle it is by training to build a good security culture by making all users aware of the real threat they are facing. Both technical and non-technical solutions would be needed to provide a secure system. Training can take many different forms and styles. Providing an online training tool could be very useful and accessible to large numbers of users especially those who are familiar with computers (Edelson and O'Neill, 1994; Pea, 1994; Dede, 1996; Khan, 1997; Edelson, Gordin and Pea, 1999; Kearsley, 2005; Willems, 2005). Research has found that e-learning would reduce overall cost and learning time by about 50% and increase knowledge retention by 25-60% compared to traditional learning methods (Fletcher, 1991, pp.33-42; Hall, 1997, p. 108; Zenger and Uehlein, 2001).

A training capability can be a powerful tool that can save organisations time and money and can even make people feel safer and more confident to use computers and other online technologies (Aloul, 2010; Boujettif and Wang, 2010). Interactive learning tools (e.g. e-learning, posters, leaflets, videos, games) could educate users on the importance of information security, making them aware of the potential security threats and the need to protect their information from unauthorised users, and give guidelines of how to protect themselves (Al-Hamar, 2010). Users should be taught what to do to protect themselves from possible security threats, for example never giving out their passwords, updating their anti-virus software, accessing only trusted websites, not opening unknown junk mails, and not download from untrusted websites.

8.4 Reasons for survey

The aim of the survey was to collect information about the normal behaviour and actions of people while using a computer and the Internet and to assess Qataris' level of awareness on information security. The level of security awareness was surveyed to determine the risks which might arise from users voting from their own machine through an I-voting system.

The survey target was a sample of Qatari voters who are eligible to vote. Their responses would play an important role in making recommendations or designing tools for Qatari people on how to enhance their awareness.

8.5 Survey design

In order to determine the level of users' security awareness, a survey was required to assess the use of computers and their vulnerability to security threats.

This survey was intended to help find some of the common security mistakes of users and how they normally react to some common threats they can face in their daily use of the Internet, computers and some other electronic devices such as mobile phones. Important questions this survey tried to answer are the following:

- Is the level of awareness of users reflected in their actions while using the Internet and computers?
- Is a computer security awareness campaign needed?
- Can such campaigns help to increase the level of security awareness among all computer users?

The survey is divided into three sections, each with a number of questions, and participants were asked to complete each section in turn before moving to the next. The first section gathered general background information about the participants, who were asked about their gender, age and education. The second section covered computer and Internet security aspects. To measure participants' computer and Internet security awareness, questions were selected according to the book "Computer security – Client side" (Hosseini, 2005, p.342) and the results constituted an empirical study of Qatari computer users. The third section had questions about participants' willingness to take part in a further survey to evaluate the researcher's proposed solutions to the problems identified. Contact details were collected for this purpose. A copy of the questionnaire, in its English translation, is given in Appendix C.

8.6 Analysis of Survey

8.6.1 Section 1. Background

The first section of the survey consisted of three questions asking participants for their background information.

8.6.1.1 Question 1. Gender.

The survey was dominated by 91% male respondents.

8.6.1.2 Question 2. Age.

Responses to the second question showed that most of the respondents were aged from 18 to 29, this being 80% of the total, followed by 20% aged between 30 and 59. There were no respondents over the age of 60.

8.6.1.3 Question 3. Education.

The third and final question in this section concerned the level of education of respondents, to help to find out if education has any impact on the respondents' level of security awareness. The responses to Q3 covered the comprehensive range of certificate, diploma, bachelors', masters' and PhD programmes undertaken by the respondents. The results indicate that the main concentration of respondents was drawn from those educated to higher-level education, this being a total of 60%. The remaining 40% are undergraduate and further education students, 22% being undergraduates and 18% further education students.

8.6.2 Section 2. Computer and Internet security

The second section of the survey concentrates on the computer and security issues faced by those computer users. Some questions included images related to the issues and which the participants were asked about. They were given multiple-choice questions, some single answer questions and others requiring a selection of more than one answer.

8.6.2.1 Question 1. Frequency of use of the Internet

The first question asked participants how often they use the Internet. This can help to understand how experienced the respondents are with the Internet and the scale of the security problems they are facing, depending on their use of it. The response to Q1 indicates that the majority of respondents (87%) use the Internet more than once a day, followed by nearly 7% who use it once a day, giving a total of 93% who use it every day, and nearly 7% using the Internet once a week. This indicates that the Internet plays an important role for the future of communication and services, therefore user privacy and security should be considered.

8.6.2.2 Question 2. User reaction to a fake Internet security pop-up.

The second question looked at the response of the Internet users when an Internet pop-up box comes up with a fake security warning while they are browsing the Internet (see Figure 8.2). The participants had a number of answers to choose from, one being to respond to the pop-up message box, another to ignore it. The appropriate choice is the latter, to avoid the possibility of clicking on a link that can lead to virus infection or security attack on one's computer. 78% of respondents said they would ignore the message if it came up, while the remaining 22% said they would respond to it.



Figure 8.2: Example of a fake Internet pop-up message

It may appear positive that most respondents had chosen to ignore the pop-up message but 22% is still a relatively big number, especially when bearing in mind that 80% of the respondents who chose to respond to the pop-up message are using the Internet more than once every day. A very serious security threat faces those who respond to that kind

of pop-up, since malware software could be installed in the PC, unknown to the user, and it could open a back door to take control of the user's computer remotely. An infected computer then could become part of the "botnet". By widespread use of broadband, Internet criminal hackers use a botnet, a group of Internet computers controlled by malware code, to attack businesses using a denial of service (DoS) attack to gain financial benefit. This security threat could infect both the individual's computer and the wider Internet community. A good slogan to adopt is, therefore, "Be safe and keep others safe". According to experts interviewed (see section 5.7.4), I-voting faces a serious threat from a botnet attack and user awareness and training could avoid users becoming part of a botnet, helping to keep the Internet safe (see section 3.4.1).

There appears to be a relationship between a user's age and the amount of user security awareness. The responses indicate that most of those who responded to the pop-up message (70%) are in the 18 - 29 age group, with 30% of respondents aged 30 to 59. This demonstrates the importance of educating young Internet users about the safe use of computers and the Internet, particularly as 89% of respondents aged 18 to 29 use the Internet more than once a day and currently make up the majority of all users.

8.6.2.3 Question 3. The best way for computer protection.

The third question asked participants about the best way to protect their computer. There were a number of options to choose from, with the possibility to choose more than one.

The majority of respondents (91%), believed that virus protection software is one of the best methods of protection, followed by 62% for a firewall and 38% for patching their operating system. Some (15%) believed that the best way to protect their computer is by not accessing the Internet at all, which for most people would not be a practical solution. Most of the 11% remaining respondents had selected the “other” option, believed that Spyware software provides sufficient protection for their computers (see Figure 8.3).

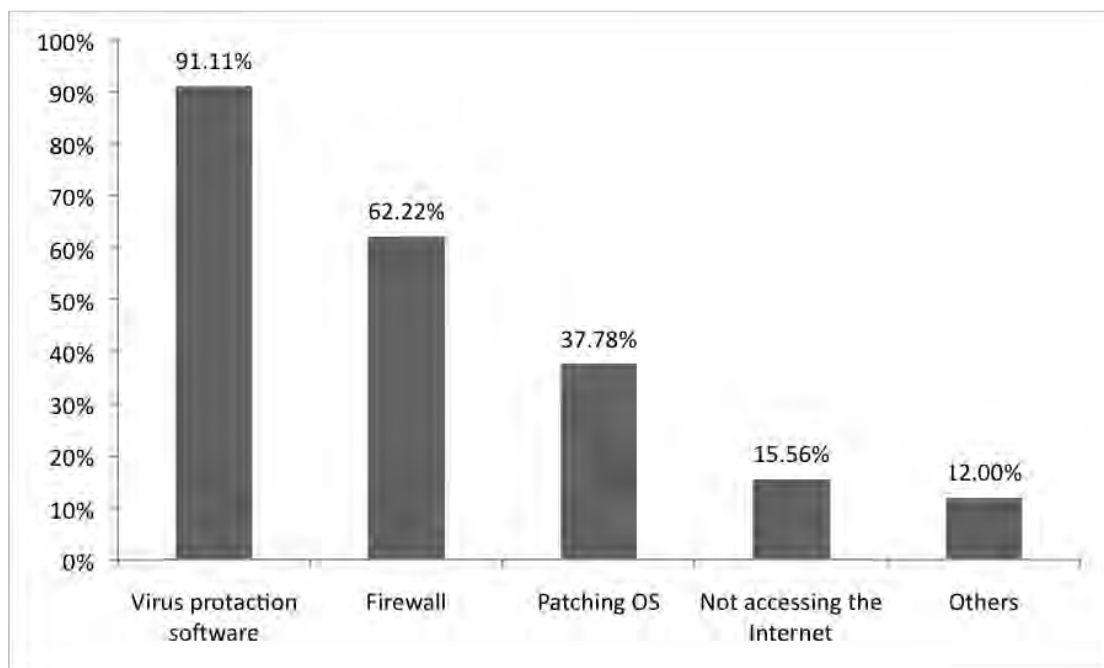


Figure 8.3: Perceived best way to protect computer

The results indicate that one third of all respondents would want all options as the best way of protection. With 73% of these respondents having high level or postgraduate education, this indicates that people with higher education have better awareness when it comes to Internet security. In fact, of the 33% of respondents who answered that

question appropriately, 80% also chose to ignore the pop-up message in the previous question (Question 2).

The results show that a high percentage of participants have the wrong idea or not the complete answer for computer and Internet security. This was evident when 91% of respondents had chosen virus protection software, whereas patching their operating system came in third, chosen by just 38% of the respondents, when it is in fact a more effective option. Internet voting would need a secure and recently patched operating system in order to have a secure computer to vote from, which could potentially be provided in a bootable CD.

The next three questions (Questions 4 to 6) are about passwords and their use.

8.6.2.4 Question 4. Use of the same password.

The response to Q4 indicates that 56% of respondents use the same password with different applications, whereas the other 44% claim they do not.

8.6.2.5 Question 5. Remembering passwords.

The response to Q5 indicates that 73% of respondents have no problem in memorising passwords. This represents positive feedback regarding their computer security awareness. 7% write down their passwords and keep them in a safe place, closely followed by a further 7% who do the same but keep it somewhere close to the computer or stick it on the computer monitor. 4% of respondents save their passwords on their computers, by writing them in a text document, which is then saved. Another 4% use password management software to keep their password in a safe place. 2% of respondents store passwords in their mobile phones. The remaining 2% of respondents have another way to remember their passwords but did not state what it is (see Figure 8.4). This implies that using different levels of authentication such as a fingerprint, voice or iris recognition or a smart card in I-voting would provide stronger security than a password. A voter can choose a weak password but not weak biometric data. A better approach to overcome the problem of remembering passwords would be to use a one-

time password which would be generated while logging into the system or it would be sent to the user using a different method, for example SMS or email. The user would then not then be required to remember any password.

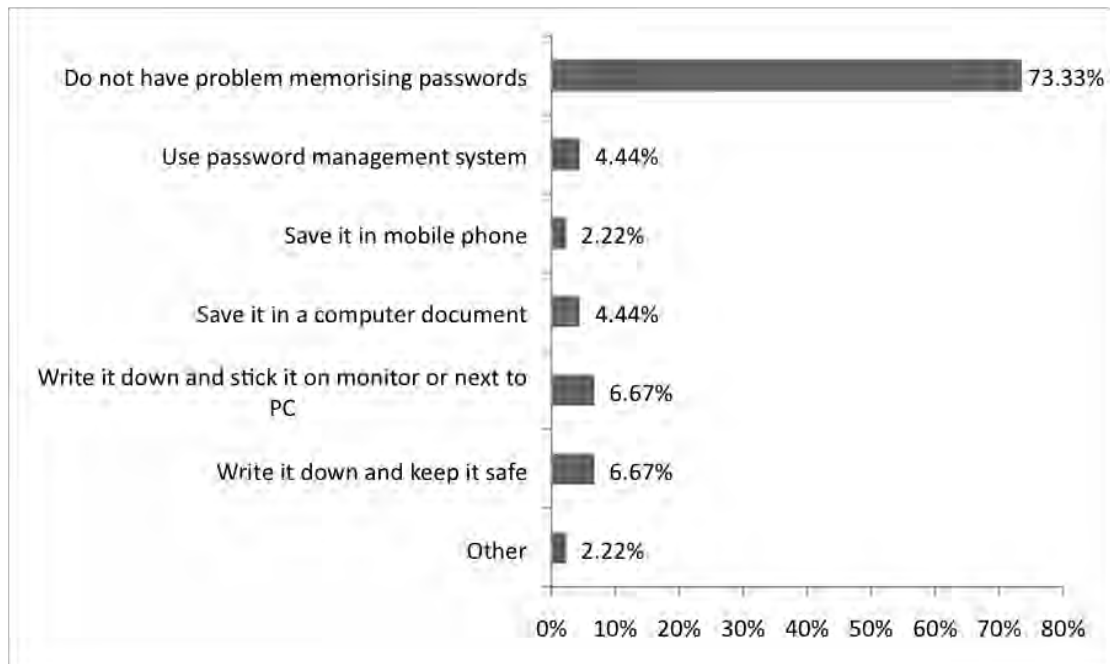


Figure 8.4: Remembering passwords

Among the majority of respondents (73%) who said that they have no problem in memorising their passwords, 82% of them are aged 18 to 29 and perhaps have better ability to memorise things than older people. However, 52% of those who have no problem in memorising are actually using the same password for more than one application, which provides further evidence that computer users lack simple security awareness.

8.6.2.6 Question 6. Method of choosing a password.

Participants were asked how they could describe the construction of their password. 36% of respondents said that they constructed them by combining words, numbers and characters. 31% said that they used memorable words. Another 20% said that they combine words and numbers. 4% use words that are hard to predict as a password, even if it is a short one. Most of the 9% remaining said they combined strange words and numbers (see Figure 8.5).

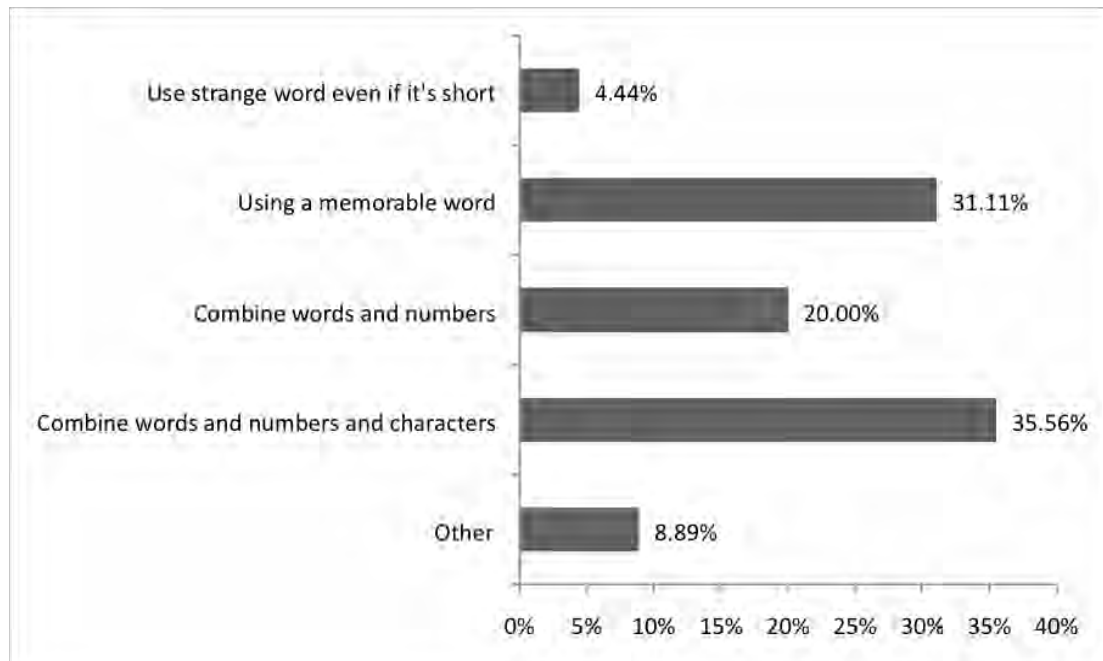


Figure 8.5: Methods used for choosing password

Using just a word as a password makes the password less strong, because of the possibility that the word used can be figured out, creating a weaknesses against dictionary attacks. What is more, most of the 4.4% respondents who use words as a password, use memorable words. Having a memorable word as a password can be described as weak as the chance for it to be figured out is high. Of those who use characters, names and numbers combined to construct their password, 81% said that they have no problem in memorising them. It is not clear whether it is just the memorising factor that makes people decide which type of password they are constructing, pure lack of awareness or a combination of both. Most respondents whose passwords can be described as strong, which is a combination of characters, words and numbers, are highly educated, with 75% with high level or postgraduate education.

In the Internet voting system design described later in this thesis, the architecture is based on a number of security layers, which would not need users to remember information such as a code or password or even personal information.

8.6.2.7 Question 7. Trustworthiness of a suspicious link.

Participants were provided with a picture (see Figure 8.6) showing a screenshot of an instant messaging window, with a link on it. They were asked about what they thought of the link.

The response to Q7 indicates that 69% of respondents were suspicious about the link, but 13% thought it was a normal message from a friend and there was nothing wrong with it. Another 9% of respondents were suspicious about it but they were still going to click on the link. The remaining 9% of respondents said they did not know (see Figure 8.7).

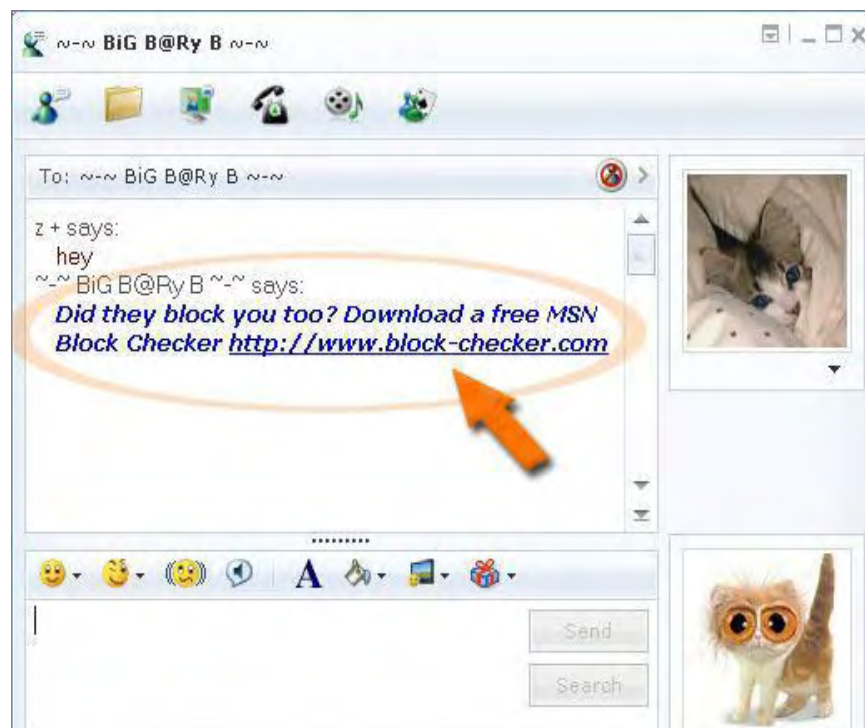


Figure 8.6: Suspicious link in instant messaging window

The link that appears in the instant messaging window is generated by malware, which has infected the computer of the person chatting. The malware sends the message with the link to other people, as if it was a message from a friend, in an attempt to deceive people to make them click on it and then get infected by the same malware, which in this case was being used for advertising purposes. Nearly a quarter of respondents indicated they would click on it, which shows that the purpose of the malware had been achieved and computer users were easily deceived.

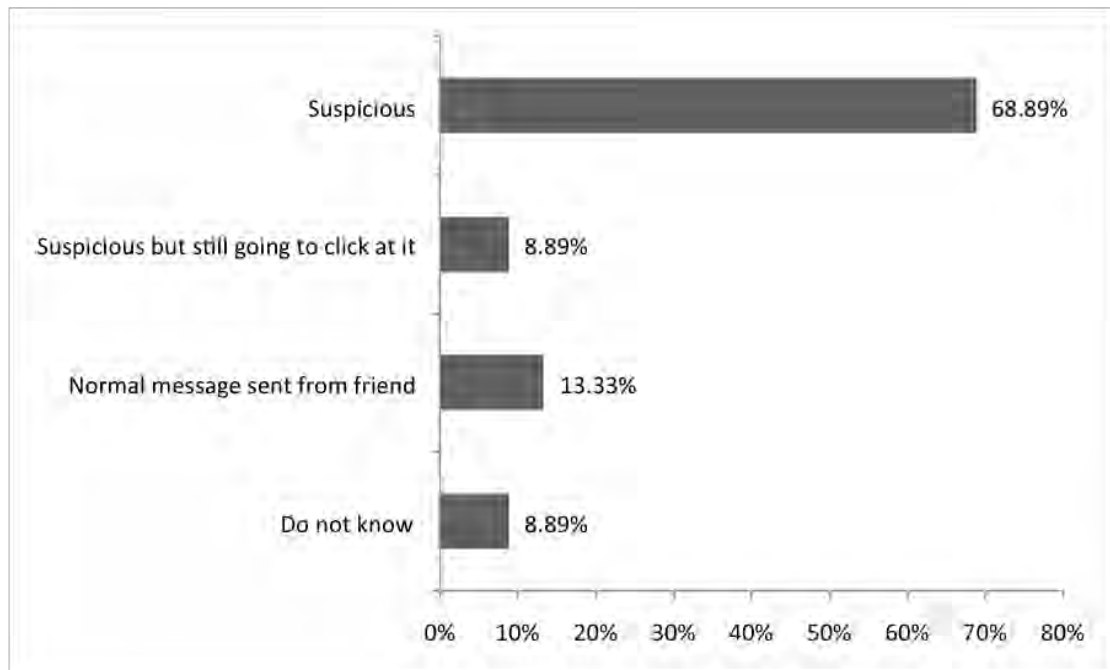


Figure 8.7: Respondents' thoughts on Instant Messaging window link

Malware writers regularly come up with new ideas to trick Internet users. Obviously, it does work and the evidence of that is that 43% of the 31% of respondents who did not say that the link in the instant messaging window was suspicious (and who might click on the link) said they would respond to the Internet pop-up box presented to them earlier (see section 8.6.2.2). Furthermore, 86% of the respondents who may click on the link on the instant messaging window use the Internet more than once every day, with the same percentage of respondents (86%), aged 18-29.

8.6.2.8 Question 8. Use of P2P software.

This question asked participants about their use of peer-to-peer (P2P) software for file sharing. The respondents indicated that 38% use P2P software and 44% do not do so, with the other 18% of respondents saying they do not know (see Figure 8.8). The results indicate that 24% of the respondents who use P2P software also responded to the Internet pop-up message in Question 2 and the same number (24%) said they might click on the link appearing on the instant messaging window. P2P networking opens the user to various forms of attack, break-in and espionage. It gets around most security architectures in the same way that a Trojan horse does. Once a P2P application is installed on a 'trusted device' a connection is made from the computer to the external

Internet attackers who can thereby have remote access for the purpose of stealing confidential and corporate data, launching a DoS attack or simply gaining control of network resources.

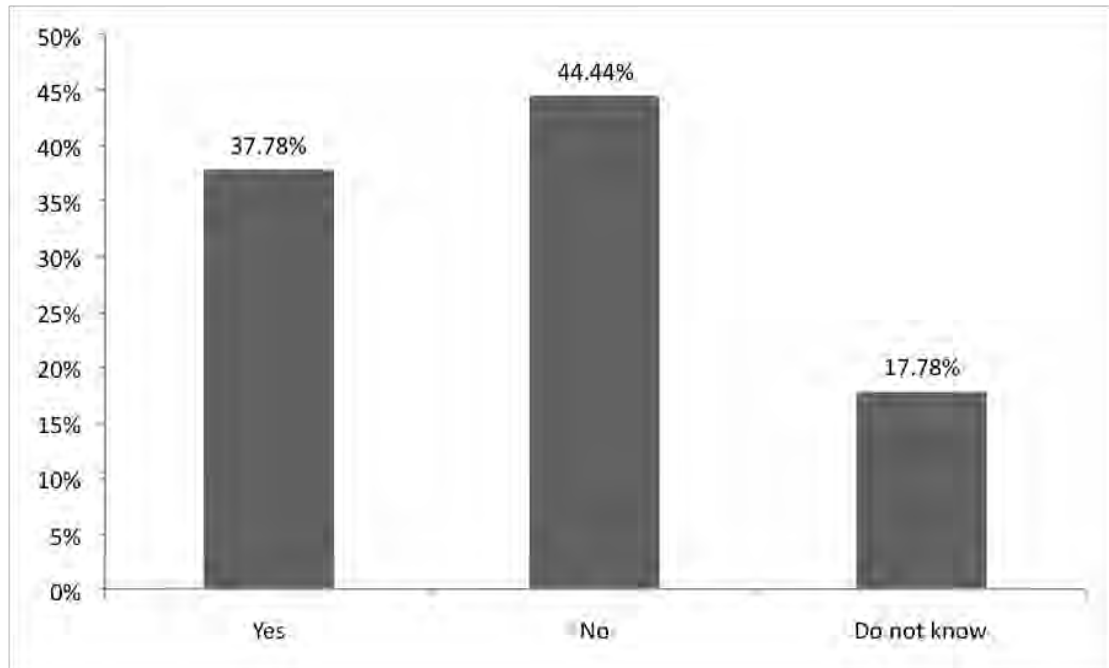


Figure 8. 8: Respondents using P2P software

8.6.2.9 Question 9. Checking file extensions before downloading.

Participants were asked if they check file extensions before they download any files or music from the Internet. The majority of respondents (76%) claim that they do check the file extension before they download any file, while 18% admit they do not; 7% do not know (see Figure 8.9). However, this represents a positive discovery that 94% of respondents who use P2P software do check file extensions before downloading. Furthermore, 92% of respondents who use the Internet more than once a day indicate that they do check the file extension before they download any file and that demonstrates a very good awareness when it comes to downloading files, especially by regular Internet users. It is important in I-voting that users should not get phished by hackers who trick them into downloading a different file from the voting application.

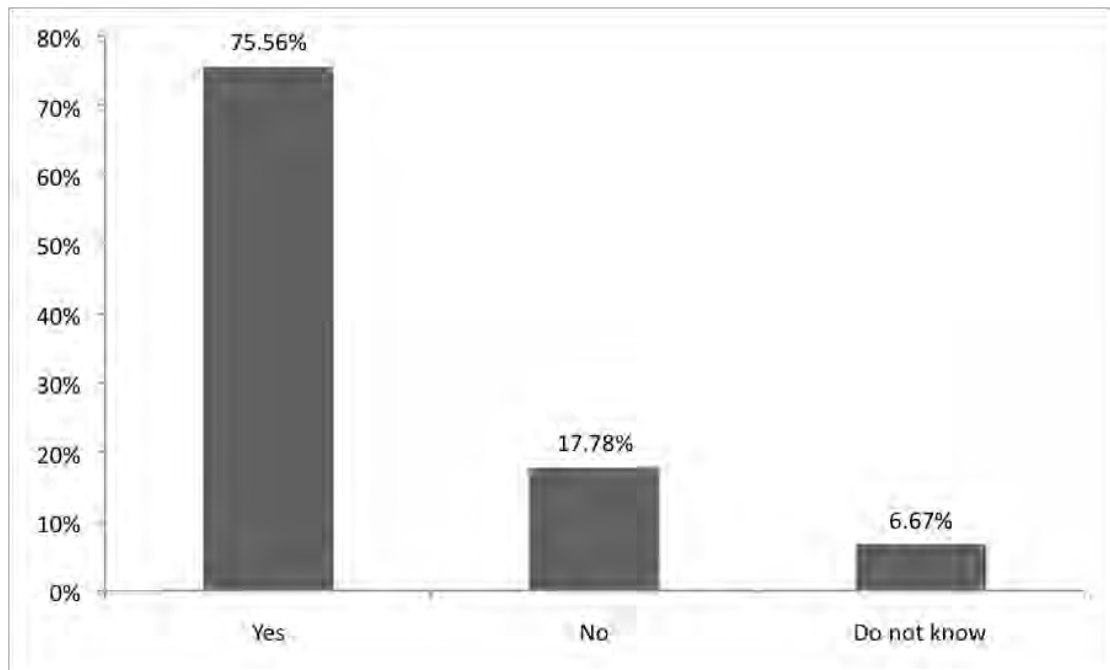


Figure 8.9: Checking file extensions before downloading

8.6.2.10 Question 10. Reaction to a warning of a virus attack that is imminent or on certain date.

This question asked participants what they would do if they hear about a virus attack that is imminent or on a certain date. In this question, participants were given the option to choose more than one answer.

The most popular action, accounting for 64% of respondents, is immediate updating of their virus protection software. Patching software in their computers came in second with 31%. Surprisingly, 27% of respondents said that they did not care and they would use their computer normally without taking any action. 9% also said they would do nothing because they have an anti-virus software, even if they are not sure if it is up to date or not, and 11% of respondents said they would use their computer but would not open any e-mail on the day of the virus attack. Just 2% said they would keep their computer turned off that day. The remaining 4% said they would be more cautious about opening emails and junk messages during that period (see Figure 8.10).

Internet security experts advise Internet users to download security patches for software and operating systems regularly to eliminate addressed security vulnerabilities. Just 31% of respondents said they would do that (Herzberg, 2008).

69% of the respondents indicated that they would take no action to prevent a virus attack on their machine and they would use their computer without concern over this problem. This clearly shows that Internet users are very vulnerable to attacks and, therefore, any Internet voting system should take into account this problem. 25% of these vulnerable respondents said they would respond to the Internet pop-up message and also the message on the P2P software. Furthermore, 50% of those respondents who did not care about the virus attacks would do nothing about it because they have anti-virus software, even if they are not sure if it is up to date. 50% of those respondents who are not sure if their anti-virus is up to date use P2P software.

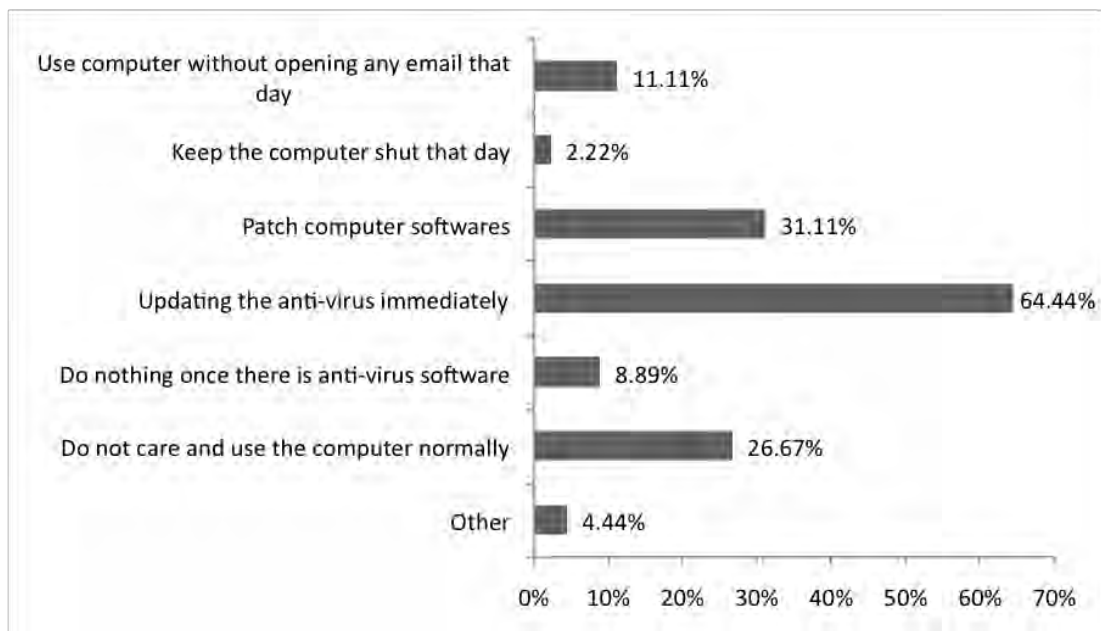


Figure 8.10: Action on hearing about virus attack imminent or on certain date.

8.6.2.11 Question 11. Opening e-mails from unknown senders

When participants were asked about whether they open e-mails from unknown senders, 44% said they do not and 20% said it depends on the e-mail subject whether they would do so. 18% said they do sometimes open e-mails from unknown senders, with 9% not sure. A 7% minority of respondents said they do open e-mails from unknown senders. One respondent gave an interesting answer by declaring that he uses a university computer to open any suspicious e-mail messages he receives (see Figure 8.11).

Moreover, 67% of respondents who do open e-mails from unknown senders do not check file extensions when they download files from the Internet. In contrast, 90% of respondents who do not open such e-mails do check file extensions before downloading any file from the Internet. Also, 33% of participants said they will use the computer and the Internet normally and would not care if there is an imminent virus attack and they would not even take action to protect their computers from being attacked. Most of those respondents (84%) use the Internet more than once a day. Experts in e-mail security who advise on deciding email legitimacy advocate not opening email attachments from unknown senders until confirmation is given that they were sent intentionally and free of viruses or malware (Downs et al. 2007).

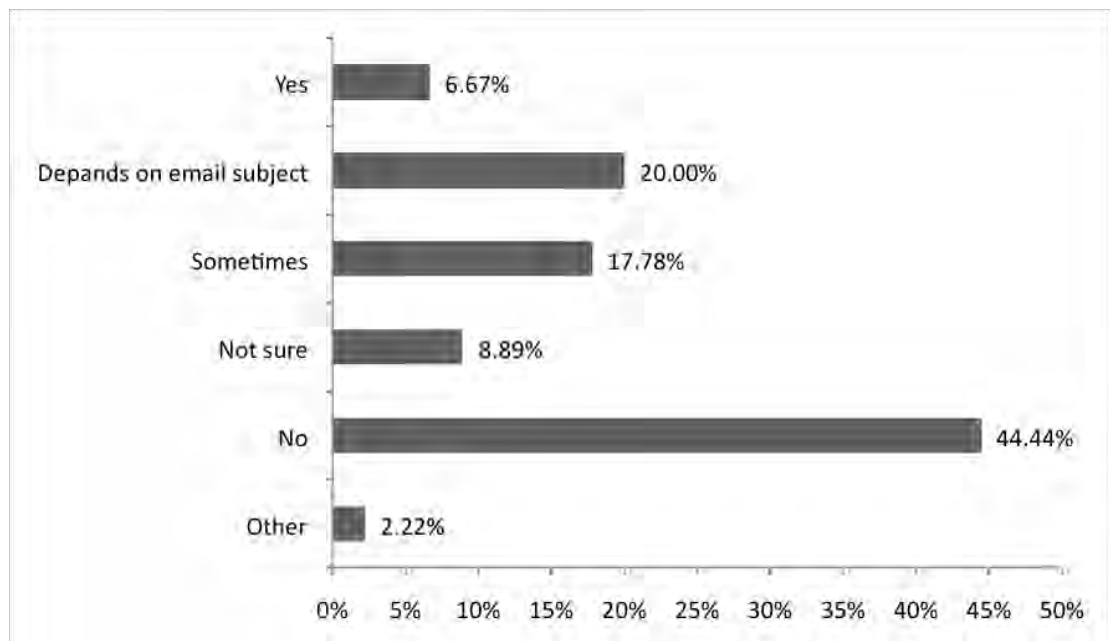


Figure 8.11: Opening email from unknown sender

8.6.2.12 Question 12. Reaction to a firewall alert

Participants were provided with a screenshot of a firewall message (see Figure 8.12) and were asked what they would do if their firewall application keeps showing them a message like that. 57% of respondents claim that they do read the messages carefully every time one appears. 20% said that they would read the message the first time and then just click OK whenever it appears again. 11% said they just would just click OK every time the message appears, with a further 7% of respondents saying they would find the message a disturbance and get fed up with it (see Figure 8.13).



Figure 8.12: Example of Firewall alert

A firewall application is important as it monitors all traffic to and from a computer to block unauthorised access and protect personal information. However, it is also important to use the firewall properly, keeping it up to date and running all the time. One of the mistakes users make is to ignore firewall messages. For example, of the respondents who said they would read the firewall message the first time and then would just click OK whenever the message appears again asking for action to be taken, one third of them would also choose to respond to the Internet pop-up message. Such behaviour would not just result in their possible infection by malware because they clicked on a suspicious link, but they would have also prevented their firewall from being able to protect them. Furthermore, that same 33% of those respondents said that they would use their computer normally and would not care if they heard about a virus attack about to strike soon (auditmypc, 2011).

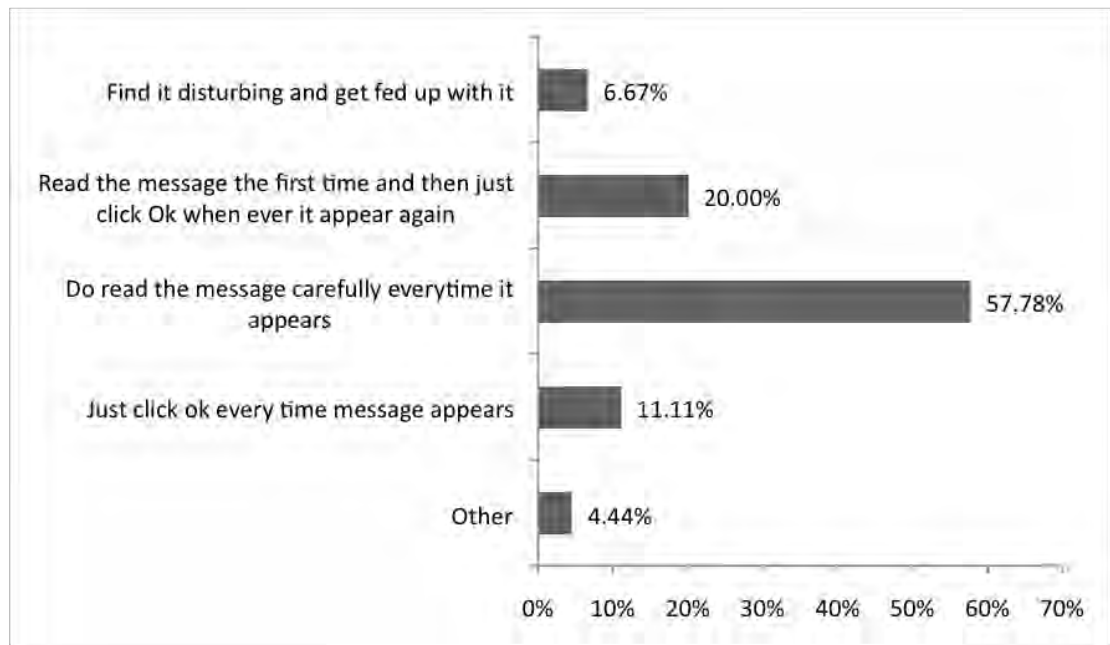


Figure 8.13: User behaviour on receiving firewall alerts

8.6.2.13 Question 13. Switching off security applications in reaction to repeated alerts

Here, participants were asked whether they switch off their firewall application or anti-virus software when notification messages keep appearing a lot. The majority of respondents (84%) said they do not, but 9% of respondents said that would do so, with the remaining 7% of respondents saying they did not know (see Figure 8.14).

Generally, people get annoyed when notification messages keep on being displayed and a number may choose to switch off their anti-virus or firewall software to stop the annoyance. However, the notification messages are trying to inform users of a security breach. The survey results show that 75% of the respondents who just do nothing and switch off their security application would also then respond to the Internet pop-up message. Furthermore, 25% of those respondents said they would use the Internet normally, even if there is a virus attack which they have been warned about, and they would not take any action to prevent the attack from happening. 75% of respondents who said they would switch off their security application use the Internet more than once a day.

In addition, 50% of respondents who said they would switch off their security application if it keeps showing notification messages also open e-mails from unknown senders. Furthermore, a quarter of those respondents (25%) do not check any file extensions before they download files from Internet.

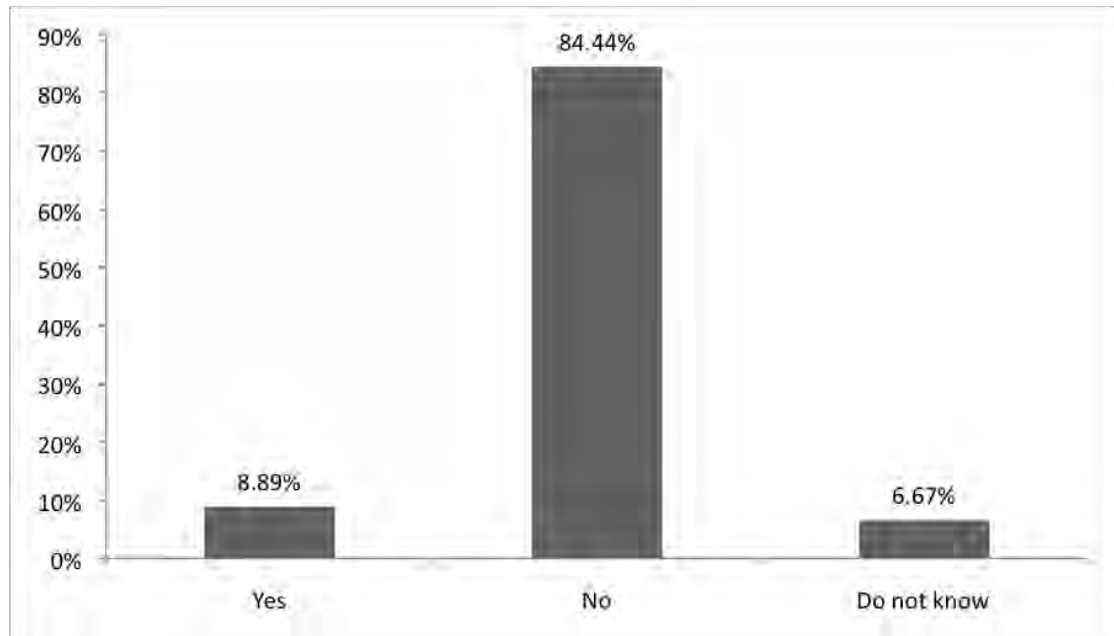


Figure 8.14: Turn off security application

8.6.2.14 Question 14. Responsibility for Internet security failure

The participants were asked about who would be responsible for any Internet security failure and were given the option to select more than one answer. The results indicate that 64% of participants claim that computer users have the responsibility, Internet service providers came second with 56%, followed by 29% of respondents who think it is a problem for big companies like Microsoft and Yahoo, 27% blame governments, while the remaining respondents think others have to be responsible, such as the web hosting companies which host virus attackers, malicious hackers and security software developers (see Figure 8.15).

The fact that nearly two-thirds of respondents indicated that Internet users are responsible for Internet security failure shows awareness that it is in their hands to

protect themselves. On the other hand, they take no action to do so. For instance, 41% of those who said users are responsible also use P2P software. However, it is advisable to download P2P on another computer, making sure it has no valuable information, to reduce possible risks. Moreover, 24% of the respondents open e-mails from unknown senders and 7% do not check file extensions before they download files from the Internet. This confirms that users need to increase their computer security awareness.

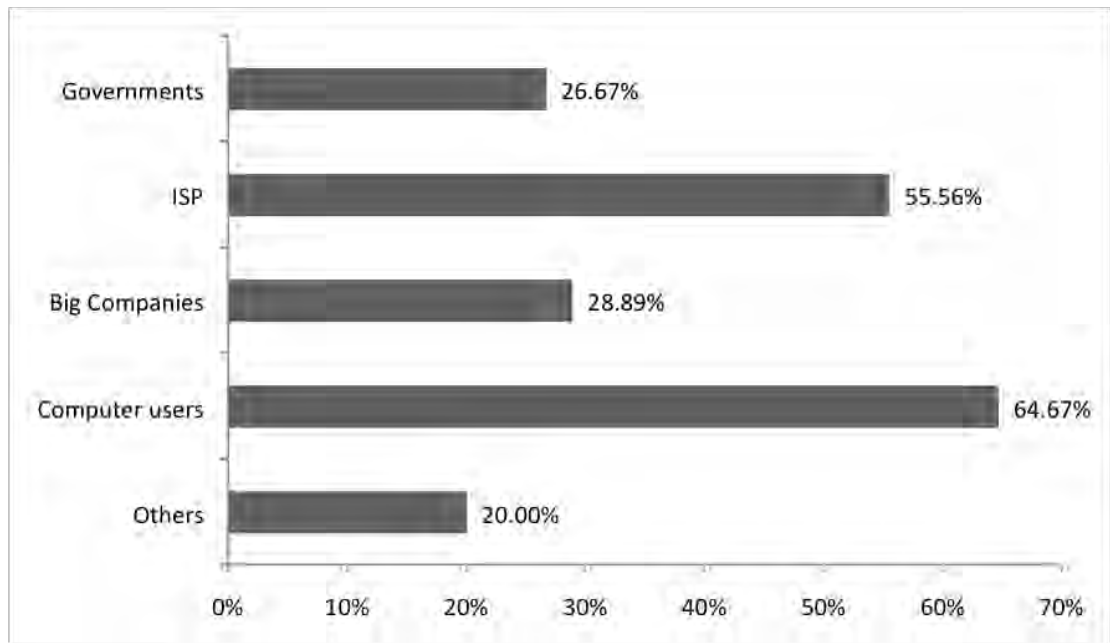


Figure 8.15: Responsibility for Internet security failure

In Section C, the last two questions focused on security awareness and training.

8.6.3.1 Question 1. Training in IT security

When asked whether they had IT security training or not, 67% of respondents said they did not have any training, while the other 33% said they did. As well as having training, 53% of respondents said they are reminded from time to time about computer and Internet security. The positive point is that 73% of the respondents who had training also used strong passwords, which is a combination of characters, words and numbers. In addition, 60% of them change their passwords every one to three months. On the other hand, 53% of respondents who had training do, nevertheless, open e-mails from unknown senders (see Figure 8.16).

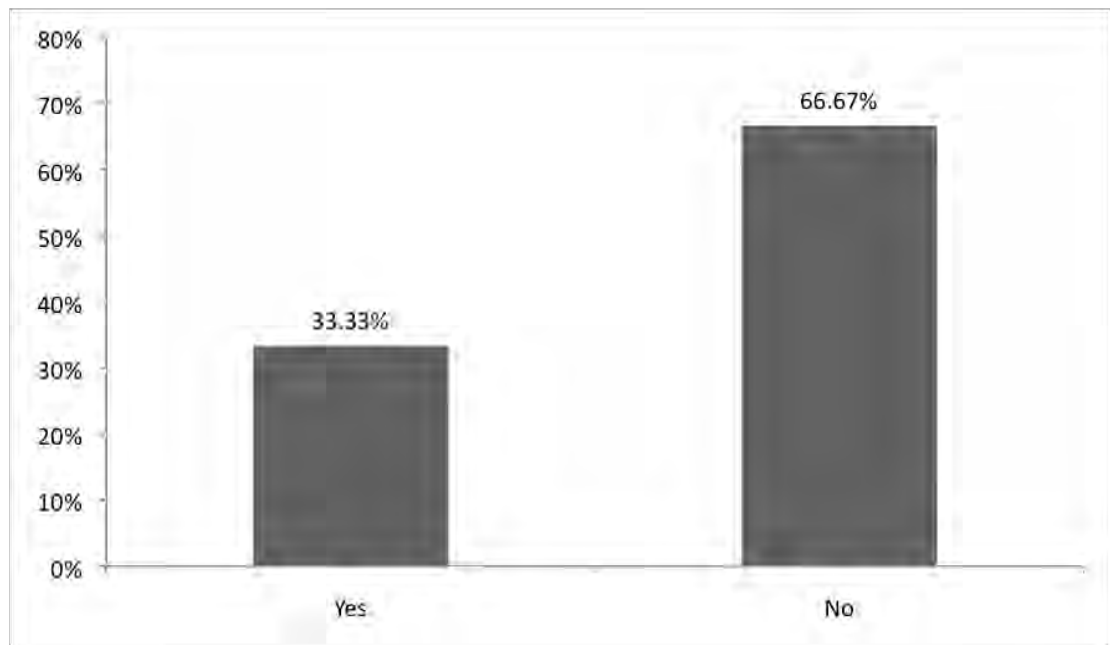


Figure 8.16: User training in IT security

8.6.3.2 Question 2. Computer security training for users

The participants were also asked about whether they think that computer users should have computer security training. 69% said that they think that they should have such training, 16% said users do not need it, while the remaining 16% said they did not know whether or not users should have that training (see Figure 8.17).

While having computer and Internet security training may be important, not all kinds of training are beneficial to computer users. However, it seems that many respondents who had training in the past feel they have benefited from it and would recommend having training to other computer users. Overall, 42% of respondents who had training in the past believe computer users should have training related to computer and Internet security.

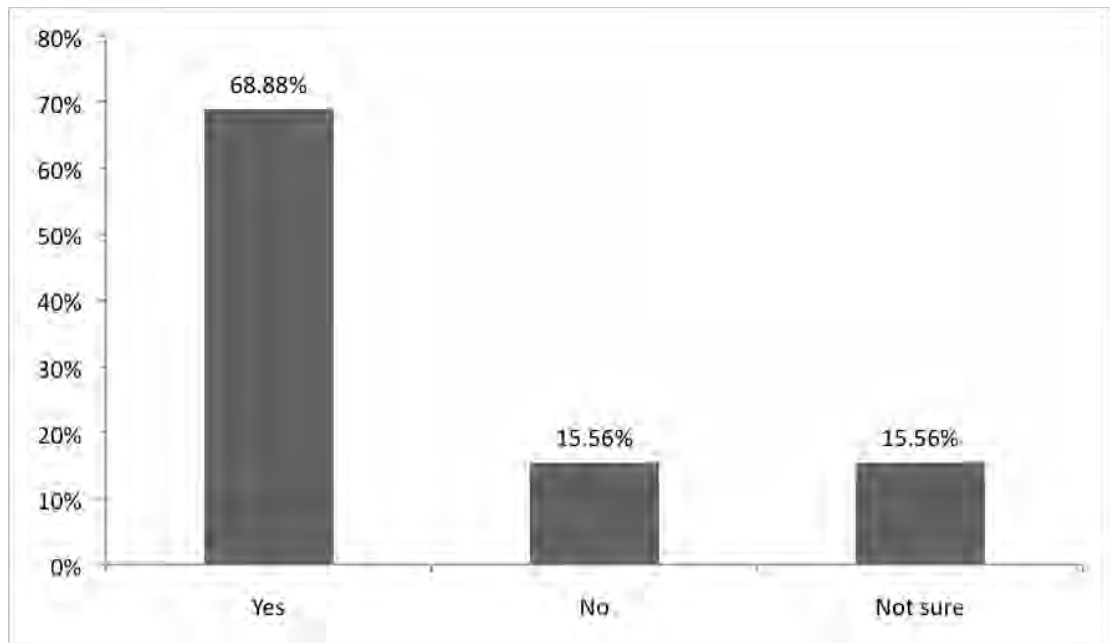


Figure 8.17: IT security training for computer users

8.7 Conclusion

The previous chapters concluded that I-voting is feasible but there might be issues associated with the client in terms of their knowledge and awareness on information security related to I-voting. Therefore, this chapter has focused on studying voters' awareness of information security and that, with I-voting, there may be a threat of manipulation by an unauthorised user. Based on a survey designed for this purpose, the research identifies the need for enhancing user awareness to attain an effective I-voting system. The survey of a sample of eligible Qatari voters aimed to measure their computer and Internet behaviour and their knowledge of information security. The conclusion from the survey is that users perform many inappropriate actions which might put them at a security risk due to lack of awareness of information security. However, the result shows that Qataris do know about methods of computer protection including virus protection and firewalls, though they may not always appreciate the need to employ these methods.

The survey shows that 22% of participants would react to a fake security warning and respond to suspicious links, putting them at risk of malware. In addition, about 38% use P2P software, putting their computer at risk of being exposed to attackers. Furthermore,

very risky actions were found, with 43% of the respondents opening e-mail from unknown senders and 58% who do not read firewall alert messages.

In contrast, the majority of participants perform some correct actions such as checking file extensions before downloading, turning on security applications and updating their anti-virus to protect their PC from viruses.

Using different levels of authentication in I-voting could provide higher security than a password, since voters might choose a weak password and may not keep it safe from disclosure to other people.

In conclusion, the survey indicates the need for enhancing awareness on information security to reduce the possible risks associated with the client in I-voting. Although user awareness and training play an important role in providing part of an overall awareness of security, technical solutions are still important to ensure secure I-voting on the client side and this is covered in the next chapter.

Chapter 9 A proposed model for I-voting in Qatar

This chapter begins with an examination of the requirements of voting systems, in particular, those for electronic voting (Section 9.2). These requirements were then re-analysed in terms of constraints upon any software system that performs I-voting tasks. Next, the model is presented in Section 9.4. Finally in section 9.5, a prototype of the proposed model is described that is used to test the implementation of the model.

9.1 Introduction

This chapter is concerned with the presentation of a new model for I-voting, one that is particularly suitable for use in elections in Qatar. The model was developed after carefully considering the views of voters and experts on an effective I-voting system that would be appropriate to elections in that country. The resulting model attempts to fulfil a number of requirements of the voting process, including that it should ensure security, privacy, transparency and accuracy and should be useable by members of the public.

The model was designed to satisfy the Qatar e-government roadmap for I-voting, which relies on the following three-pillar strategy to identify individuals accurately:

- (1) Use of a unique identification number (the QID) which consolidates the voter's credentials in a single number;
- (2) Use of a set of multi-modal biometric credentials which allow strong identification and authentication of individual voters, and
- (3) Use of a unique digital certificate to enable secure interaction with the I-voting apparatus.

As discussed in Chapter 3 (Literature review), these problems have attracted the attention of many researchers and various solutions have been produced.

Figure 9.1 shows the Qatar e-government roadmap in terms of achievements and future milestones.

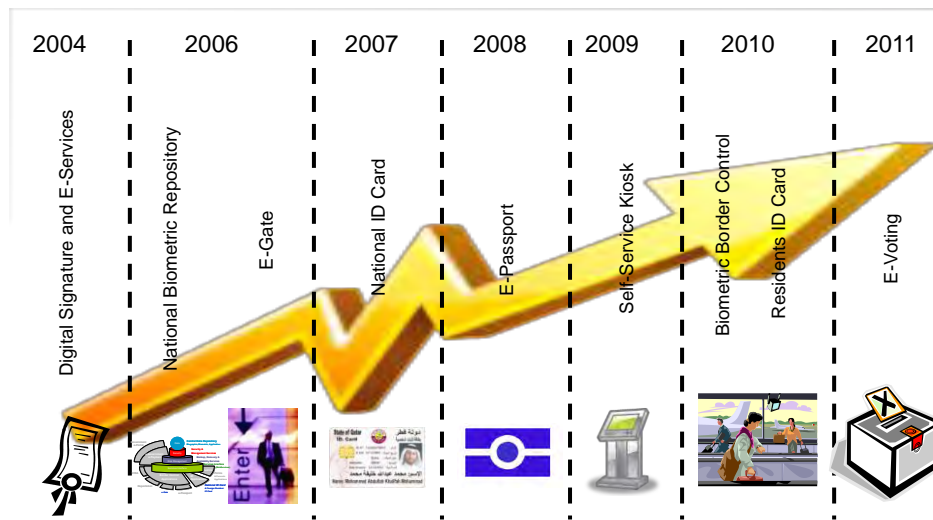


Figure 9.1: Qatar e-government roadmap

The model proposed in this chapter is a form of electronic voting in which votes are cast over the Internet. It is intended that the Qatari National ID card will be used as a credential when the voter's identity must be verified. It is also intended that the PKI credentials will be used within this smart card in order to ensure confidentiality and integrity.

9.2 Requirements of the Voting Process

The requirements imposed by the voting process amount to a challenge to the model builder. The main factor affecting election administration is security but other factors are also relevant to the evaluation of I-voting systems. Public confidence depends upon election security and integrity, but choosing a voting system must also involve consideration of other performance factors such as ease of use and efficiency.

For present purposes, accuracy refers to how voting equipment completely records and counts votes precisely, ease of use refers to how understandable and accessible the equipment is to a diverse group of voters and election workers, while efficiency refers to how quickly a given vote can be cast and counted. For more details of voting requirements, see section 3.4 and Appendix D.

9.2.1 Software requirements

The requirements stated in the previous section apply to software.

The section deals with the following aspects of the software:

- | | |
|----------------------|----------------|
| 1. Access controls | 4. Accuracy |
| 2. Physical controls | 5. Ease of use |
| 3. Audit trails | 6. Efficiency |

Each aspect is defined in detail in see section 3.4 and Appendix D.

9.3 The proposed model compared to the earlier experimental model

The earlier experimental I-voting model, proposed in chapter 7, was focusing on secure voting and measuring Qatari's acceptance to such new technology. The evaluation of this model shows a high percentage of acceptances with some concerns on the scalability of the system to perform in large scale election in terms of ensuring the reliability of the system and achieving the voting principles including security.

Therefore, the proposed model was modified to provide a comprehensive solution by securing the client machine using a customised CD to ensure the reliability of the machine. The model introduces the new idea of using a virtual private network for secure transmission of votes. It defines the detail of the end to end process of I-voting from registration, authentication, voting through to vote counting. Also, to provide more security to the process, the new proposed model uses a certificate authority to verify eligible voters. Multi-parties are used in the voting process to ensure confidentiality and integrity of the system. In addition, for authentication, a one-time-password is used to verify eligible voters, distributed through SMS and which expires after 10 minutes. Since Qatar has a tribal structure, family intimidation can occur in election where courtesy and family pressure could happen. Therefore, a revote option is supported in this model to eliminate the family pressure to vote in any particular way. In addition, the interface of the modified model is more informative and simple, compared to earlier version to ensure ease of use. However, both models use PKI for encryption, a smart card for authentication and blind signature for anonymity.

9.4 The Process of Voting

9.4.1 Introduction

In this section, the new model is presented in software and hardware terms. The description consists of a discussion of the operating system and distribution medium used to give voters the software they require to access the Internet and cast their ballot. Authentication and registration are then discussed. Anonymity and its preservation, vote casting and vote counting then follow. From this, it can be seen that every stage of the voting process has been included. Both software and hardware problems are discussed. Figure 9.2 shows the proposed I-voting stages for the State of Qatar.

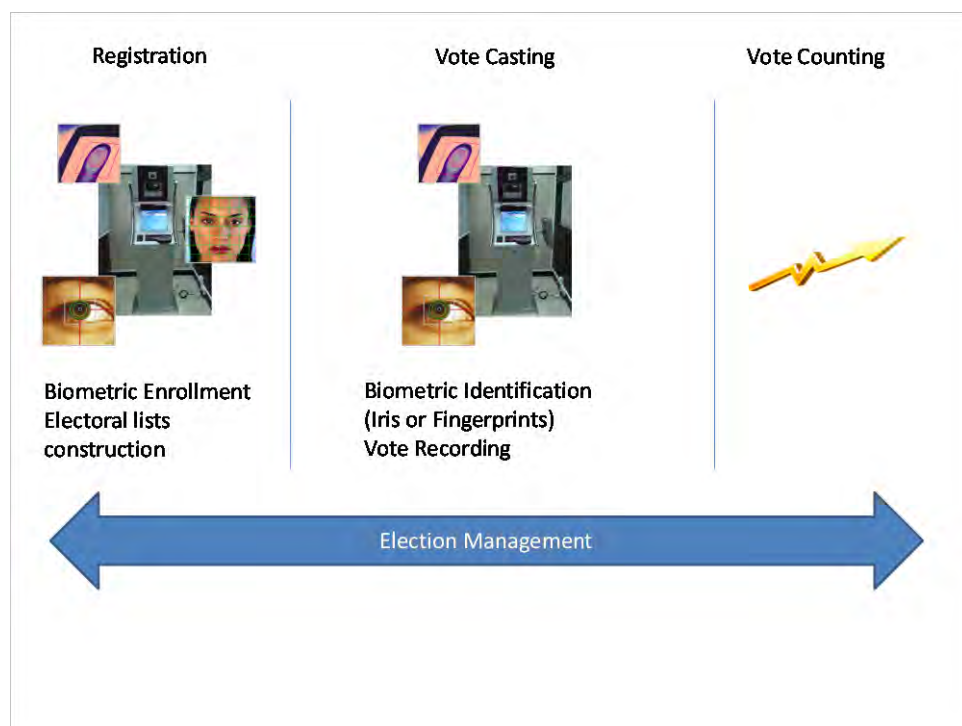


Figure 9.2: I-voting stages for the State of Qatar

9.4.2 Technical aspects of the system

The security of the proposed model depends on the security of its two main components: the servers and the client computers permitting users (voters) to connect to the election servers. The client software is clearly a critical element of the system since it is to be used by members of the public. It is also a security-critical component of the overall system and must be as reliable as possible. To this end, the Linux operating system is used to support the client software. This choice is partially motivated by the fact that Linux is available free of charge and can be downloaded easily; it is also open software, so its source code is available for inspection and/or modification, thus raising the users' level of confidence in its code. The client software will be distributed on CDs, which can be inserted directly into the voter's machine. The disk will then boot and the voting software will execute.

The choice of Linux therefore reduces the cost of client software while increasing confidence in it. The problem with Linux is that it is not very secure (Chou et al., 2001), but there are no licence problems with this system. The use of Linux will have to be different from the normal in terms of usability if it is not to let the system down from a security viewpoint.

To overcome any security problems, voters (users) will have to use Linux via a special, restricted shell, one that cannot interact with the file system and gives a highly restricted view of the operating system. The login shell should only run an interface to the voting software. It should not be possible to cause the voting software to terminate without terminating the login shell. This is very easily done on all Unix operating systems and the way to do it is well documented (Garfinkel et al., 2003).

It is also necessary to restrict the standard path so that it only looks at, say /usr/local/bin (which is on the distribution CD), where all user-runable executables are stored. The system supplied on the CD would be a cut-down version of a standard Linux system that has the necessary software to run the voting system only. All other software normally associated with the Linux operating system (such as compilers, editors, etc.) would be removed.

All executables of the distributed CDs must be signed and the signatures signed secure hash algorithm (SHA) or MD5 will do, as long as the fact is publicly known for it serves to put people off attacking) (Eastlake and Jones, 2001).

When running the I-voting software, no component should be part of the system root or equivalent. This requires a check of the software before the distribution CD is created. Just in case voters have to re-cast their vote, they should be required to change the password on their login shell. Next, SSH (secure shell) should not be used as the improved SSH2 version should be used instead (Barrett et al. 2005).

Furthermore, the IP stack is a set of communications protocols used for the Internet and other similar networks, however it presents security problems of its own. TCP, in particular, is an insecure communications medium and requires additional measures if communications using it are to be secure (Comer, 2006). TCP is prone to man-in-the-middle attacks, a widely known fact about the protocol (Comer, 2006). Instead, it is worth considering use of UDP (User Datagram Protocol) instead as it is largely used by time sensitive applications as well as by servers that answer small queries from huge number of clients. UDP is commonly used in the Domain Name System, Voice over IP, Trivial File Transfer Protocol and online games.

The operating system on the voter CD will run a firewall to enhance security. It will also run only software upgraded to run the latest security patches and all software will have been checked using anti-virus software. As noted above, signed software should be used to ensure that it has not been ‘adjusted’ since it was dispatched from the central source.

First, it should be noted that the CD’s system will almost certainly communicate with the I-voting servers using IP addresses provided by the Dynamic Host Configuration Protocol (DHCP), which is a protocol for assigning dynamic IP addresses to devices on a network. Since these will change from time to time during a session, there is no one single IP address to attack. It also means that, if any ad hoc modifications are to be made to the way UDP works, this will have to be taken into account. This will become apparent when anonymity preservation is considered in Section 9.4.5 below.

Communication between the Client and the I-voting system are done through requests, as illustrated in Figure 9.3.

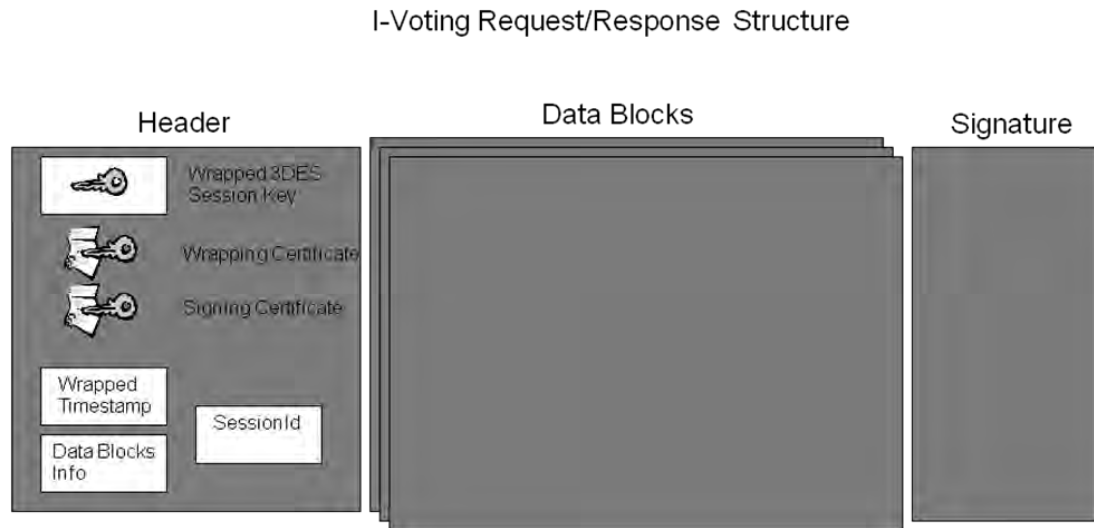


Figure 9.3: Requests and response structure for I-voting

Table 9.1 defines the structure of request/response which composed of header, data blocks and signature. It would identify what is needed to be include in the voting packets while transmitting on an Internet network.

Table 9.1: Description of Requests and response for I-voting

Group	Item	Description
Header	Wrapped 3DES Key	Encrypted session 3DES Key encrypting Data Blocks contained in the Request/Response in order to ensure their confidentiality during transit between the Client PC Module and the I-voting servers
	Session ID	Internal Session ID, associated with authentication, is send to the user a temporary session ID
	Wrapped TimeStamp	Encrypted time stamp used in order to avoid replays (where replays are the resending of information that has not been successfully received)
	Data Block Info	Structure containing information in a data block contained in a Request/Response message
	Wrapping Certificate	Client X509 Certificate (See section 3.4.2.4 .B), (depending if it is Request or Response) used to encrypt 3DES Key and TimeStamp (Halevi and Krawczyk, 1999)
	Signing Certificate	Client X509 Certificate (depending if Response or Request) used to sign Data Blocks to be used for proof of origin in order to authenticate Terminal or

Server initiating Request/Response

Data Blocks

Data Blocks

Data Blocks containing information coded in ASN.1 (Abstract Syntax Notation One) format for Request/Response

Signature

Signature

Digital Signature of content of Data Blocks using a Signing Certificate

At the level of data communication in the Network level, the model proposes a security engine using different layers of security. Figure 9.4 illustrates the I-voting Security Engine. In order to understand the functioning of the engine we need first to define the generic structure.

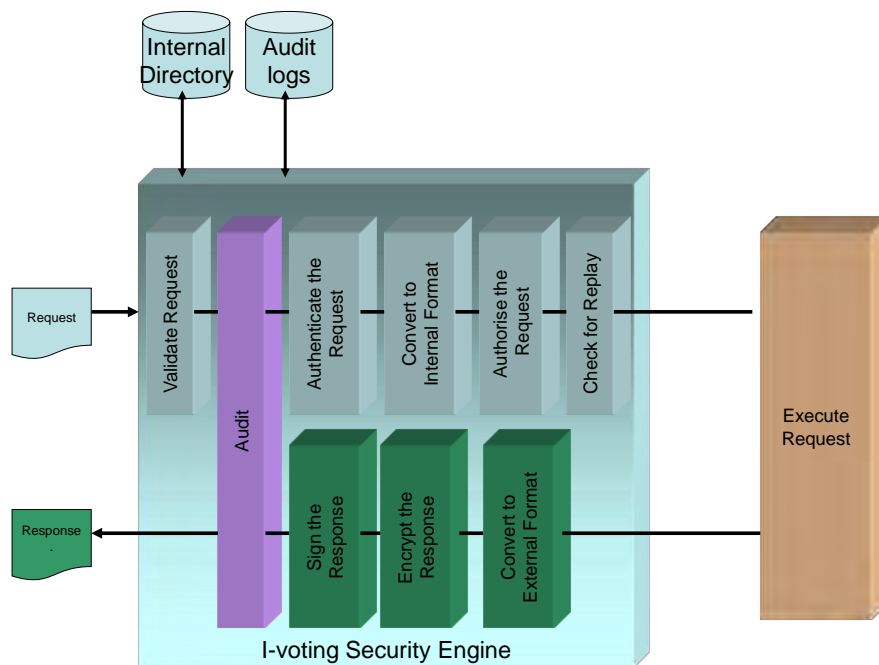


Figure 9.4: I-voting security engine architecture

Based on the above communication structure, the functioning of the I-voting Security Engine is the following:

9.4.2.1 Reception

When a request is received the security process is the following:

1. Request checked for validity in terms of adherence to the communication format in Table 9.1
2. Request logged in the I-voting Security Audit Log
3. Request authenticated on two levels:
 - a. Through digital signature to authenticate the sender's terminal
 - b. Through the session ID to authenticate the user through their ID card credentials
4. Request authenticated for voter
5. Authorisations checked by examining the internal directory containing the ID card credentials for the authenticated user through their session ID
6. Replays checked through analysis of the embedded time stamp on vote cast

9.4.2.2 Responding

When a response needs to be generated, the security process is the following:

1. The response is converted to voting application format.
2. Data blocks in the response are encrypted with a 3DES session Key.
3. Data blocks are signed with the voter's signing certificate.
4. An entry in the Security Audit log is generated.

9.4.2.3 Authentication and Authorisations

The Authentication and Authorisations are enabled by the existing infrastructure on the server. A special Request/Response authentication is used, where:

1. The user sends ID card credentials to the I-voting system through a logging process
2. The Security Engine interfaces with voter machine to authenticate the user and if successful generates the session id in the internal directory containing its authorisations levels.

9.4.2.4 Audit trails

It is important to note that extensive audit trails of two types will be implemented in the I-voting model:

1. A security audit trail containing audit logs generated by the Security Engine to log all activities.
2. An applications audit trail generated when processing the vote casting.

In both cases these audit trails will be signed with the voter signing certificate in order to ensure their integrity.

Figure 9.5 shows the proposed IT Infrastructure for the I-voting servers. It gives the list of servers that is needed along with the technology that could be used to deploy I-voting in action if the State of Qatar decided to implement I-voting .

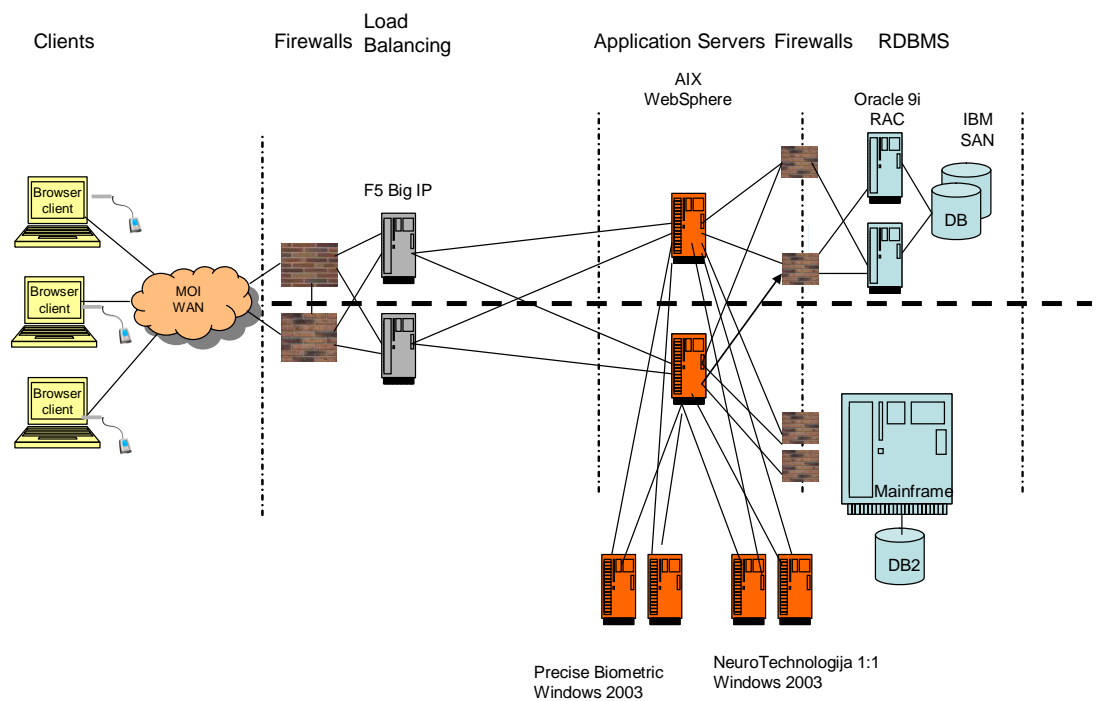


Figure 9.5: Proposed IT Infrastructure for the I-voting servers.

9.4.3 Authentication

In this model, authentication is based on three factors:

1. Something one knows (PIN),
2. Something one has (Smartcard) and
3. Something one is (Biometric).

The first system checks whether the voter is registered with the Vote Registration Server. If the voter is already logged as registered, it is taken as indicating that they have already voted.

Otherwise, the following steps are taken. The voter should obtain a national ID card (a smart card with a signing certificate). The card would contain biometric information about the voter (in which case, biometric information will be used as identification or verification of identity) and his/her public and private keys for authentication (certificate signing). The stored biographic data will validate the fact that the voter is eligible to vote.

Users prove their identity to the server through the following steps:

1. Certificate validation occurs. This validates that the certificate has not expired.
2. The issuer is validated. The issuer will be the Qatar Certificate Authority.
3. The process determines that the certificate is not in the Certificate Revocation List.
4. After passing these tests, the voter connects to a URL that is SSL V3.0 enabled. This permits him/her to download a secure applet (which is smart card middleware), which is used to assist the browser in accessing the smart card.
5. Users access something they possess (the smart card) and/or enter information that only they could know (such as a password or PIN). By providing correct information, users are granted access to the keys and certificates in the corresponding digital ID. At this stage, though, users have not yet proved their identity as far as the system is concerned.
6. Using the private signing key, the applet signs a challenge string (a text string containing numbers and letters, like a serial number) sent by the server on behalf of the user. The applet sends it plus the corresponding verification certificate to

the server. Note that the applet sends only public information, not the user's private key or PIN.

7. The server checks the signature using the verification certificate. If the check succeeds, the digital signature is verified and the server can then issue an authentication cookie to the user.

An alternative using biometrics is as follows. A USB token is used to provide a hardware approach to two-factor authentication. USB tokens help provide greater security for authentication over Web portals. Tokens are designed to store securely users' digital identities, including their digital certificates and keys. When users log into the web portal used for voting, they are prompted to connect their token to the desktop via a USB port and then to swipe their finger and provide a PIN. The PIN thus provided is matched against the one on the USB token.

USB tokens have a number of advantages:

- **Security.** Tokens cannot be duplicated and PINs are encrypted to increase security.
- **Extensible.** USB tokens provide security capabilities beyond two-factor authentication because they store the users' digital certificates.
- **Reliable.** USB tokens are durable with an average lifespan of ten years.
- **Cost effective.** The plug-and-play capabilities minimise helpdesk and training costs.

The voter is asked to scan his/her fingerprint. The system would first check the scanned fingerprint against one stored in the USB token. If it matches with a print on the main biometric server at the Ministry of Interior, the system will then prompt for a PIN.

Security can be enhanced by generating One-Time Passwords, which are sent to the voter using SMS, telephone, email, or some other means. One-Time Passwords will be stored in the Ministry of Interior database and the voter would need to enter the One-Time Password to complete the authentication process.

9.4.4 Vote Registration

In order to register a vote, first, an eligibility check is made. Each voter's certificate contains biographic information that is sent to the Ministry of Interior database to verify eligibility in terms of Qatar law.

Figure 9.6 illustrates the process through which a citizen card is printed and personalised with keys and certificates.

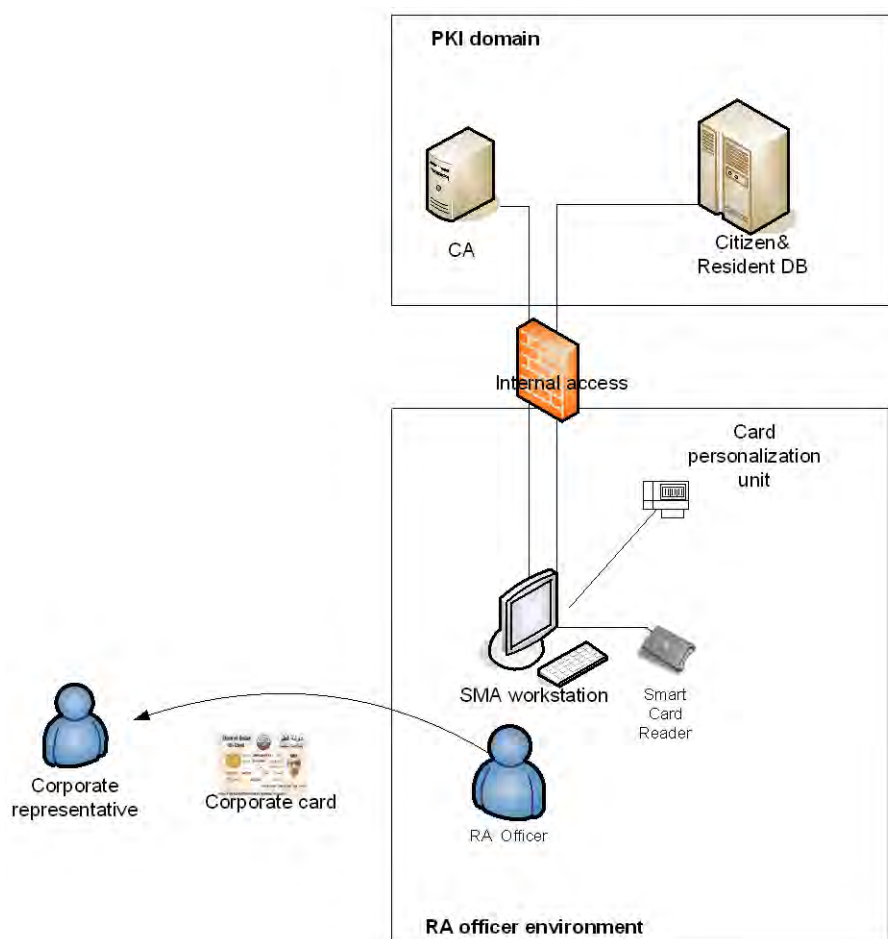


Figure 9.6: Issuing a citizen card with personalisation

Next, mutual certificate authentication occurs. That is, the system uses the PKI infrastructure to encrypt the messages between the client and server. Then a java applet sends the voter's certificate serial number to the Vote Registration Server in order to register the voter as having voted. The confirmation flag is not set at this stage (this flag is used to indicate that the voter has completed the vote-casting).

Finally, the Vote Registration Server sends a unique, random serial number to the voter. This serial number has no link whatsoever with the voter's credentials. The purposes of this function are that it (1) is used as reference for an appeal in case the voter has concern that their vote has not been properly cast (2) could be used to over-write the vote.

9.4.5 Anonymity preservation

In order to preserve anonymity, voters can use the blind signature to conceal their unique identification number and then sign the output with their private key.

A low-cost Virtual Private Network (VPN) channel using the PKI infrastructure and digital signatures for secure communication between client and server is an alternative to the above. However, it is important to note that the Secure Shell (SSH) network protocol, that allows data to be exchanged using a secure channel between two networked devices, is not as secure as was originally thought and a newer version SSH2 should be preferred as a more modern and secure alternative (Barrett et al. 2005). The client would be able to connect to a trusted computer (see section 3.4.1.3) in order to vote from a reliable computer away from possible risks related with the client side. It is suggested a hybrid solution is used to secure the client-side by using a smart card reader with a vote code. This approach has proved its effectiveness in research conducted from Helbach and Schwenk (2007) and Oppliger (2002). It is further recommended to use a matrix table for the vote code to reduce the possibility of vote changing at the client machine. Although the first approach of using a clean operating system is clearly more secure, this second approach remains as an option.

9.4.6 Vote Casting

Figure 9.7 illustrates the required end-to-end process through which a web certificate will be issued as in the second scenario above.

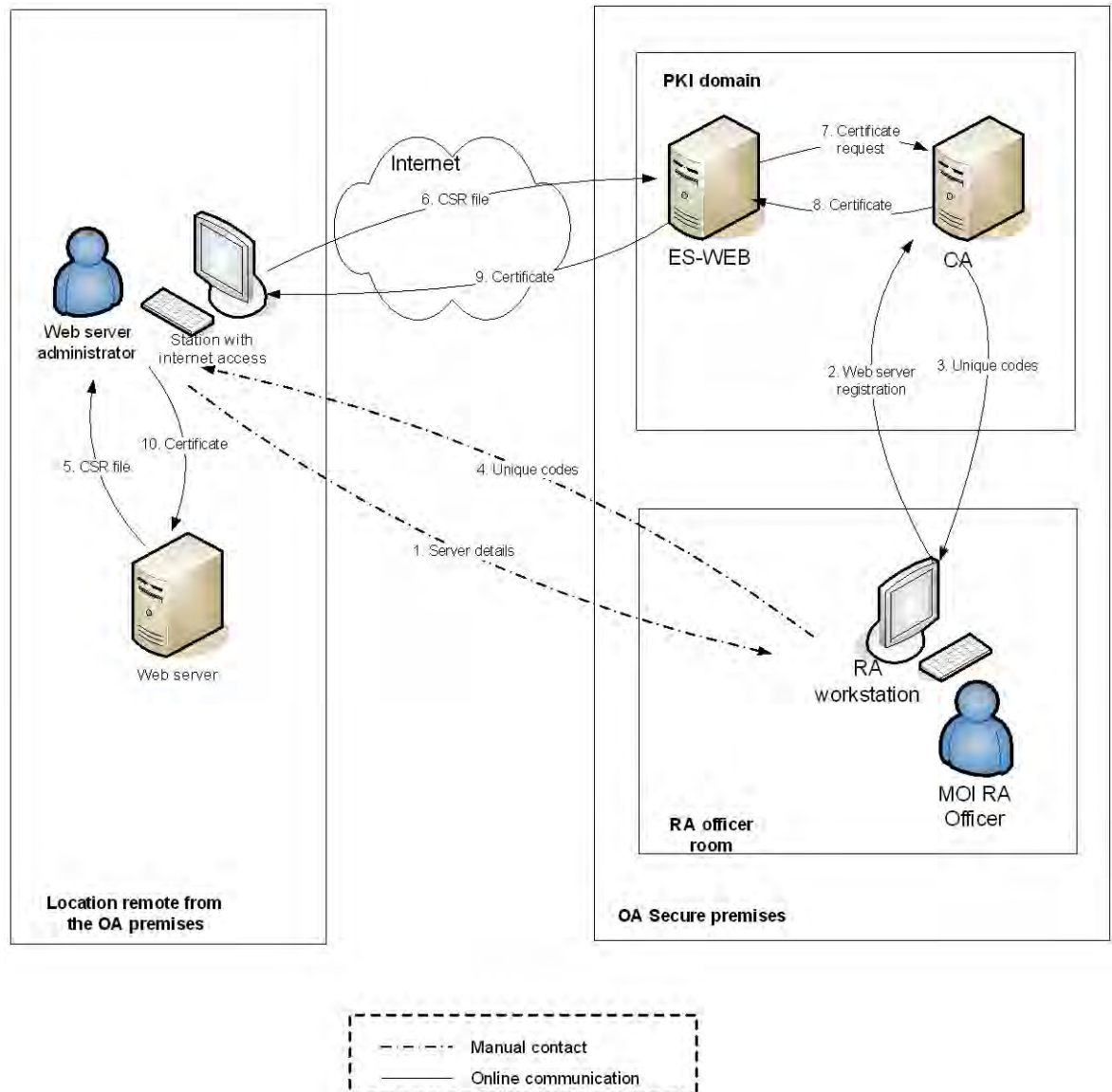


Figure 9.7: The process of issuing a Web certificate

In this stage, Hardware Security Modules (HSM) would be used for hardening the network where it would need more than one entity to access the service, thus enabling enterprises to add hardware protection to critical applications such as public key infrastructures, databases, and web and application servers. Apart from its ready integration with other applications (e.g., RSA certificate managers, various databases),

the use of hardware security modules simplifies the management of encryption and signing-key management.

1. The voter encrypts the output of the previous step using the Election Committee's public key (obtained from its hardware security module). Members of the Committee are the only ones allowed to decrypt the encrypted information for the purpose of non-repudiation to provide proof of origin of data; this data will then be sent to the Privacy Server. (The voter uses his/her digital certificate to authenticate to the Privacy Server).
2. The Privacy Server decrypts the received message using the hardware security module private key and blindly signs the voter's unique identification number using the private key from the hardware security module.
3. The Privacy Server then encrypts the signed voter's unique identification number using the voters' election-certificate public key.
4. The Privacy Server sends the encrypted, signed, unique identification number to the voter, and records the voter as an authentic voter so they cannot request another blind signature.
5. The voter receives the blindly-signed unique identification number and decrypts it using his private key, then reverses the blinding signature to obtain his signed unique identification number, which he will use as his anonymous ID. (Now the voter holds an authentic and valid ID from the Privacy Server and, at the same time, no one can link the voter's real identity to this ID).
6. The voter contacts the Voting Sever and authenticates himself using the anonymous ID.
7. The Voting Sever checks if the received anonymous ID is valid by deciphering it using the Election Committee private key. If the voter is an eligible voter, the Voting Sever allows them to cast their vote.
8. Finally, the Voting Sever records the anonymous ID as that of a voter who has voted, so in this way, each voter can vote only once.
9. The Privacy Server ensures that a voter can only obtain an ID that has been blind signed once; the Voting Server ensures that blind-signed IDs are associated with a vote once and once only.

9.4.7 Vote Counting (Tallying)

After each vote, the Voting Servers are asked to print hard copies of user votes using printers.

At the end of election, a copy of the votes is sent to the Count Server, which runs software to count the votes and also compare the count with that of the hard copies.

9.5 Prototype implementation of the model

In this section, the voting approach is described in section 9.5.1, followed by the result of an implementation is presented with some discussions in section 9.5.2.

9.5.1 Voting approach for secure I-voting architecture

This section describes the three steps for the proposed secured voting architecture using the Internet. Firstly, the vote registration process is presented. Secondly, the vote itself. Finally, the counting of votes.

The proposed method is based on combining public-key cryptography, blind signature, smart card verification, a PIN and checking of the voter's home address. Here, public-key cryptography is used not only as a communication protocol to transfer secured information from the client but also, partly, for identification. A blind signature is used for candidate selection on the ballot paper. A smart card is used to check the identity in the vote registration process. A PIN is used for identification in combination with the voting key file on polling day. A voting key file is a set of three elements: an ID record, a private key and a signature. For storing information, three databases are used to decentralise the information and improve the security. A single database could be used but it is not preferable in an actual system for security reasons.

9.5.1.1 Vote registration process for I-voting system

The full process of vote registration is described in Figure 9.8 in 11 steps.

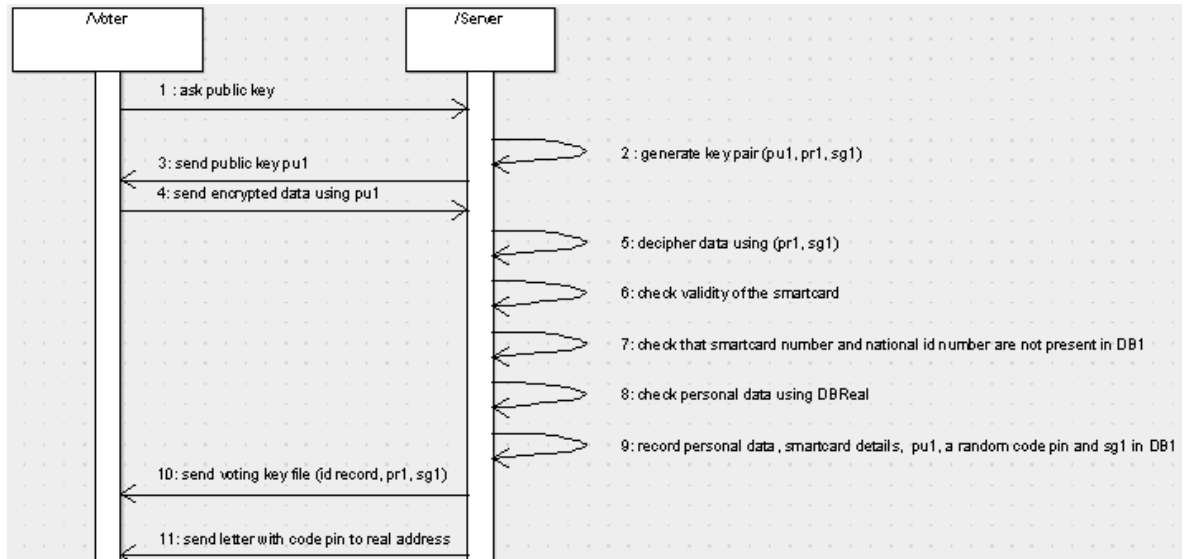


Figure 9.8: Vote registration

The vote registration starts by asking the server for a public key to encrypt the information written by the client (step 1). The server generates a pair of keys (public and private) with their associated signature and then sends the public key to the client (steps 2-3). Since the public key is received on the client side, the voter types the following information:

- Personal details: National ID, First name, Surname, Date of birth and address.
- Contact details: Telephone number and e-mail.
- Smart card details: Name, Number and PIN.

All of these are required to complete the vote registration. However, personal and smart card details are used to profile and verify the identity of the voter whilst contact details are extra information which can be used to invite the voter to vote on the polling day. Then, the typed data is encrypted and sent to the server (step 4). No one can read the information exchanged during the transfer without having the private key from the server side. In the next step, the server deciphers the information using its private key (step 5). The server then checks that the smart card information is valid (step 6). After that, the server checks that the national identity number or the number of the smart card has not already been recorded in the database 1 (step 7). Then the personal information

is checked with the database (step 8). All checking done, the personal information is recorded: smart card name, smart card number, personal information, public key and signature) in database 1 (step 9). Finally, the server sends the voting key file to the client using the ID generated by the record of step 9 (step 10). The voting key file is important and needs to be kept confidential by the client up to the vote. Then, during the time period separating the registration of voters and the polling day, a letter is sent to the client at the address (House number, Street, Postcode and City) provided (step 11). The letter contains a PIN code of 4 digits which is required to identify the voter on the polling day. Thus, two elements are needed to vote (voting key file and PIN from the letter). The letter is useful because if the voting key file is stolen, then the thief will not be able to vote without having the PIN. Also, this letter gives a certain physical security to the process and improves the confidence of voters in the architecture. The voter registration process is depicted in Figure 10.1. In the next section, the vote on the polling day is presented.

9.5.1.2 Vote on polling day by Internet

The full process of voting on the polling day is described in Figure 9.9 in 18 steps.

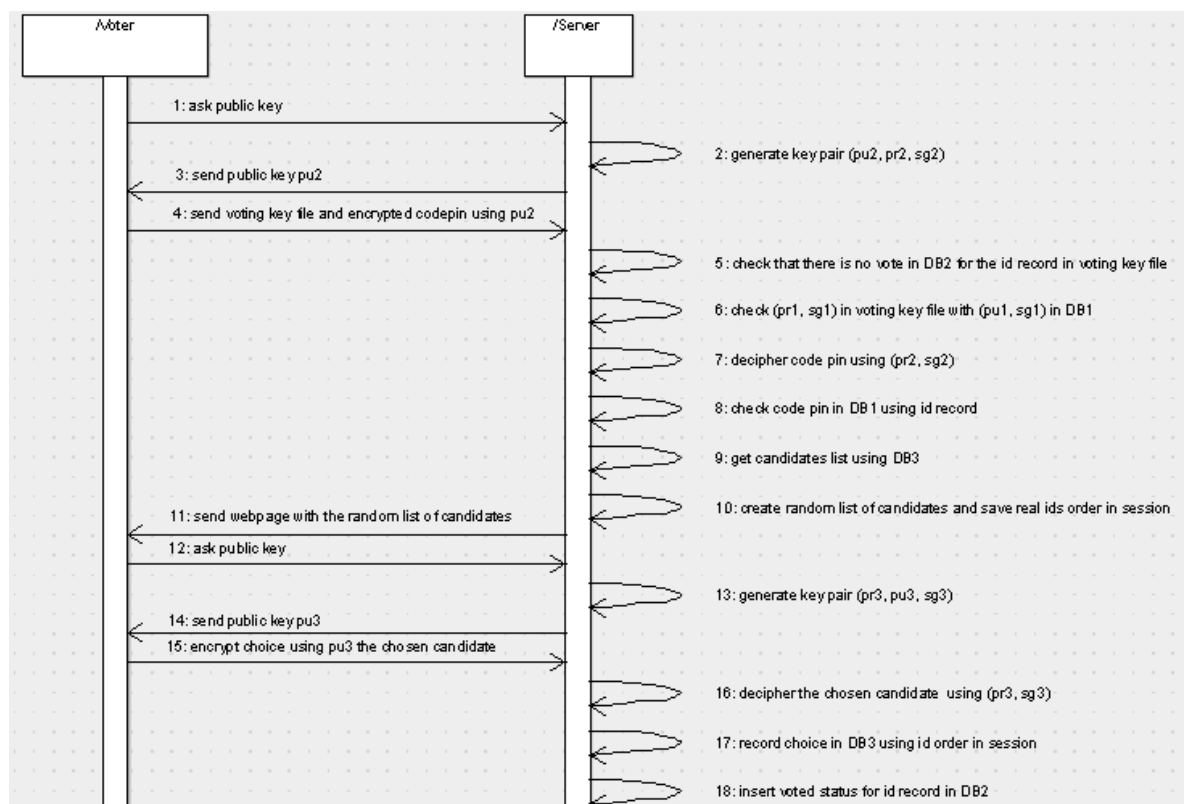


Figure 9.9: Vote on polling day for voter

On the polling day, the voter is asked to provide his voting key file and the PIN from the letter he received. Similarly to the registration process, the voter requires a public key to the server to encrypt its PIN and send it with security to the server (steps 1-3). The PIN is encrypted with the public key and sent with the voting key file. At this point, the ID record in the voting key file is used to check whether or not the voter has already voted (step 4). The latter information is stored in a different database (database 2) from that used in the vote registration process to improve security (step 5). Then the private key and the signature in the voting key file are checked with the information stored during the vote registration process in database 1 (step 6). Afterwards, the PIN is deciphered using the private key on the server (step 7). Thus, the PIN can be checked with the one recorded in database 1 during the vote registration process (step 8). Only three tries of an invalid PIN are allowed to complete the process of voting on the polling day. After all the tries, the voter is not authorised to vote. From this point, the voter is allowed to vote and the rest of the voting process consists of sending the list of candidates to the voter and inviting the voter to choose one. Firstly, the list of candidates is selected from a third database (database 3) (step 9). Finally, to improve security, a blind signature approach is used to disguise the list of candidates before the voter encrypts the chosen candidate. The simple way to realise it is by providing a list of candidates and a list of random IDs, asking the voter to send the random ID corresponding to the chosen candidate and keeping the real order of the IDs in a memory session section in the server side (step 10). Thus the voter has just to send the random ID without knowing the real one. The signature is preformed by using a pair of keys (public and private) to encrypt the selection of the voter. The voter asks for the public key (step 12), the server generates a pair of keys (public and private) and sends the public key (steps 13-14). Then the voter encrypts the random id and sends it to the server (step 15). In step 16, the server decipheres the random id using its private key and gets the real candidate id from the temporary memory session. In the end, the tally of the id candidate is updated in database 3 (step 17) and the voter is recorded as having voted in database 2 (step 18). In the next section, the counting of ballot papers after polling is described.

9.5.1.3 Counting ballot papers in I- voting architecture

Counting of ballot papers is done after the polling is over and is simply computed by querying the number of votes of each candidate from database 3.

9.5.2 Results and Discussion

In this section, a prototype is described of the approach for a secure I-voting architecture presented in the previous section. For technical reasons and simplicity, a WAMP (Windows, Apache, mySQL, PHP) server was configured and installed for the evaluation. Encryption was realised using the Jcryption library, a javascript library for encrypting strings and HTML forms. This library is easy to use, allows RSA encryption and can support encryption up to 2048 bit, these being the reasons for using it in the prototype (Hossain et al., 2011). To evaluate the proof of concept of the approach, the key length was fixed at 128 bits. Real personal and smart card information was not checked due to unavailability of the needed resources. For the prototype, four web pages were developed, one for the first step, two for the second and one for the last.

The first web page shown in Figure 9.10 is used for the registration process described in Figure 9.8. On the loading of the page, steps 1 to 3 are carried out using the Jcryption library by communication between the client and the web server using Ajax (Asynchronous JavaScript and XML) technology (W3Schools, 2011).

Personal information:	
National Identity Number:	<input type="text" value="120761324487651853"/>
Title:	<input type="text" value="Mr."/> ▼
First Name:	<input type="text" value="Alfie"/>
Surname:	<input type="text" value="Steele"/>
Date of Birth (yyyy-mm-dd):	<input type="text" value="1972-7-26"/>
Address:	
House number:	<input type="text" value="5"/>
Street:	<input type="text" value="Caxton Place"/>
Post code:	<input type="text" value="SE1 3RN"/>
City:	<input type="text" value="London"/>
Contact information:	
Telephone Number:	<input type="text" value="077 8948 3373"/>
e-mail:	<input type="text" value="AlfieSteele@vor.uk"/>
Smart Card:	
Name as written on the front:	<input type="text" value="Mr Alfie Steele"/>
Number as written on the front:	<input type="text" value="4539066540566059"/>
Code Pin:	<input type="text" value="...."/>
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

Figure 9.10: Example of voter registration using a web form

Thus, the creation of the public key for the client to encrypt the form is captured behind the view of the user and in a very short time. During this time, the form is filled by the client and checked syntactically (the birth date is higher than 18 years, only integer numbers are filled for the smartcard number, validity of the email address, etc.). This checking is realised on the client-side using JavaScript before being submitted. Afterwards, the fields are encrypted into a single one using the JCrypton library and sent to the server (step 4). The random PIN code was generated with 4 digits (step 9). A sample letter sent from the server to the home address of the voter (step 11) is presented in Figure 9.11.

Mr Alfie Steele
5 Caxton Place
SE1 3RN
London

April 19, 2011

E-voting corporation
10 Queen Road
London

Dear Sir:

Your information have been checked and validated by our personal.
Please find here your code pin:

1781

We advise you to keep it secretly.
You are now welcome on the polling day to vote on <http://e-voting.co.uk/vote.html>
using your voting key file and your code pin.

Yours Faithfully,

E-voting corporation

Figure 9.11: Example of letter

The second and the third pages shown in Figure 9.12 and 9.13 are used on polling day by the voter as described in the process in Figure 9.14.

Ready to vote

Please choose the voting key file:

Please enter the code pin from the letter:

Figure 9.12: Identification on polling day

The second page is used during steps 1 to 11 whilst the third page is operating for the rest. Note that the third page differs from the first and the second due to its dynamic content with the list of candidates.

Electronic Voting Process Cast your ballot

Welcome! Mr Alfie Steele

- Roham
- Smith
- John

Figure 9.13: Example of candidates list

The election results

Candidate	Number of votes
John	1
Roham	2
Smith	0

Figure 9.14: Example of outcome for counting the scores of the candidates list

The fourth web page in Figure 10.6 shows the counting of ballot papers after polling day. The content of the web page includes the list of candidates with their associated scores during the election. The fourth web page differs from the third, being for visualisation only. Thus, the server does not transfer the IDs of the candidates to the client.

9.6 Conclusion

There has been much interest in I-voting in recent years, but fear of a possible threat to democracy has delayed the introduction of I-voting in a general election (Aeby and Wiget, 2007; Buchsbaum, 2004; Krimmer et al, 2007). The proposed I-voting model is based on the belief that satisfying the basic requirements of voting, which are security, privacy, accuracy, availability and usability, is possible with currently available technologies and algorithms.

A secure client/server web architecture to vote through the Internet has been proposed using cryptography methods, smart card and PIN checking. This architecture has been validated using a prototype with a WAMP server (without testing a real smart card) and evaluated by an expert. The primary results, described in the next chapter, show that the architecture is feasible and is secure enough to be used for I-voting. However, the scalability of the architecture needs to be evaluated.

The next chapter justifies and evaluates the proposed model using literature and both expert and voter opinion.

Chapter 10 Justification and evaluation

This chapter begins by explaining eight assumptions on which the I-voting process is based. Using these assumptions a justification of the proposed I-voting model is given. An evaluation process was conducted by both experts and typical voters to collect feedback on the I-model's concepts and design. This is followed by an evaluation by another expert of the prototype implementation of the proposed model.

10.1 Introduction

Voting is considered as a right and a duty for citizens. It has been a physical process for an individual, which can be a hard task for disabled people, thus some people are less inclined to vote. However, the Internet boom in recent years and its omnipresence in daily life may change voting practice. Voting with a computer from home or using a mobile will be dramatically less physical in terms of going to a specific place, thus the new voting process should increase the level of participation. However, voting through the Internet may be possible if and only if it is accepted in the minds of people. To be accepted, a secure process is required. Voting can be considered as a three step problem:

- Registration to be able to vote.
- Voting on polling day.
- Counting the ballot papers.

In the proposed system, a client/server Web architecture approach is used in which the voter (as the client) interacts with the server during the first two steps.

10.2 Security assumptions and justifications

This section presents a set of eight assumptions about security for the developed model. They constitute the standards against which the system is to be measured and are based on assumptions made in the Estonian I-voting system and the US Secure Electronic Registration and Voting Experiment (SERVE). The assumptions are expressed in terms of nine points.

In order to simplify the problem, established security standards for encryption are used. Security experts have paid a great deal of attention to the digital signature problem and blind signature algorithms and other hybrid decoder or encryption algorithms used by voting systems.

The section proceeds with a statement of the assumptions. After each statement, there is a short explanation and, in some cases, some implications are drawn.

Assumption 1: *Secure signature programs are safe.* This means that the probability that an attacker with no access to secret keys can imitate the voter's electronic signature is negligible. Encryption has been widely used to deal with this, so it can be assumed that secure signature programs are safe.

Assumption 2: *Encryption programs are safe.* The probability of being able to deduce the vote by merely knowing the encrypted vote is also negligible. In other words, it is equivalent to conjecturing the vote without knowing the encrypted vote.

Assumption 3: *Attackers do not have access to the secret keys, SK and $SK[S]$.* If the keys are stored in a restricted area in order to reduce the risk of possible attacks, assumption 3 is valid. This fact has been widely discussed in the literature and has attracted a great deal of attention and research (Rubin et al., 2004a). Therefore, it is assumed that this assumption about the voting system is safe.

Although attackers do not have wide access to the voter's secret keys SK and $SK[I]$, attackers can gain the keys from a client who may be unable to protect their security. Usually, the average voter is unable to secure his/her workstation in such a way that it can keep the secret key safe and prevent possible use. The username and password need to be secret. For example, an attacker can activate the secret key in a (stolen) smart card by stealing its owner's password(s). Attackers with enough computing power can find, by calculation the passwords for any stolen ID card.

Assumption 4: *The voter-registration step is safe.* The Qatar e-government portal is based on PKI security. Public keys are used to register users for this electronic service. PKI is used to issue Qatari identity cards, certificates for legal documents and digital signatures for all uses by the country's citizens. Qatar has successfully used identity cards as identity documents. Many of the Qatar information systems use digital signatures, which have the same legal status as hand-written signatures. The digital signatures system is very robust, safe, and leads to a reliable I-voting registration system. As a consequence, it can be assumed that the vote registration phase in the I-voting model is safe.

Assumption 5: *The vote-counting step acts exactly as specified.* All votes are cast and counted correctly and recording of the data received by different servers takes place during the counting step. For this Assumption, insider threats have a greater significance than an external attacker (see Assumption 4). However, under this analysis, insider threats to vote counting are not considered. Consequently, we assume that the counting step works exactly as specified.

Assumption 6: *Each independently recoded file system in an I-voting system is safe.* The encryption process automatically links all the records in each database. It is assumed that the linkage algorithm is safe, confirmed by analyses in the literature (Internet Voting Taskforce, 2000; NSF, 2001).

Assumption 7: *If there are any signs of unreliability or a major discovery indicating the abuse of the I-voting system or of the democratic principles of an election which affects the reliability and validity of I-voting or appears to harm democratic principles, I-voting immediately stops and the result of the electronic poll will be cancelled. Discussions by a court or committee of electors will be used to perform plan B e.g. voting at polling station.*

Assumption 8: *Attackers are unable to subvert a large number of voters and thereby gain control of the election. If attackers could do this, then privacy would be violated and considerable damage to the democratic intent would be caused. In order to change votes or otherwise affect the vote, encrypted information must be deciphered using the appropriate keys.*

For example, attackers can secretly activate the secret keys held in smart cards and can thereby steal votes. Attackers who have sufficient computing power can crack stolen ID smart cards and then calculate the owner's password(s). Despite this broad attack, each voter's secret keys remain safe.

It can then be stated with justification that:

- Legitimate voters are able to vote in secret. Their vote will be used in the final count.
- Illegitimate voters are denied the opportunity to vote.
- Legal voters cannot vote more than once in a secret ballot and be counted more than once in the final calculation.
- Votes are secret. In addition, information verification and justification of other I-voting security features ensure:
 - Inspectors are able to check if all the votes have been properly counted in the final calculations;
 - Results of an election remain secret until the process is complete.
 - Repeating the calculation of vote numbers should be possible
 - All valid votes are properly counted. The final counting system, if all security features of the I-voting system are used, should ensure that the result is safe.

10.3 Justification of I-voting system based on the assumptions

In this section, the security of I-voting is considered and analysed. It is based on the assumptions derived from other security models. Possible attacks, those requiring serious consideration, are shown to be unlikely to occur. It can therefore be concluded that all the security features of I-voting systems can be justified and validated.

Wide-scale vote theft. In order that the I-voting system can act safely against a wide-scale vote theft, it should have the following two security features: ineligible voters are not permitted to vote and eligible ones cannot vote twice. Stopping ineligible voters from voting does not prevent vote theft, but it could help to reduce unauthorised access to I-voting.

There are four basic methods possible for extensive vote rigging:

- Votes can be forged
- Votes are cast by people who are not entitled so to do, and
- More than one vote is cast by eligible voters.
- Votes are excluded from a ballot.

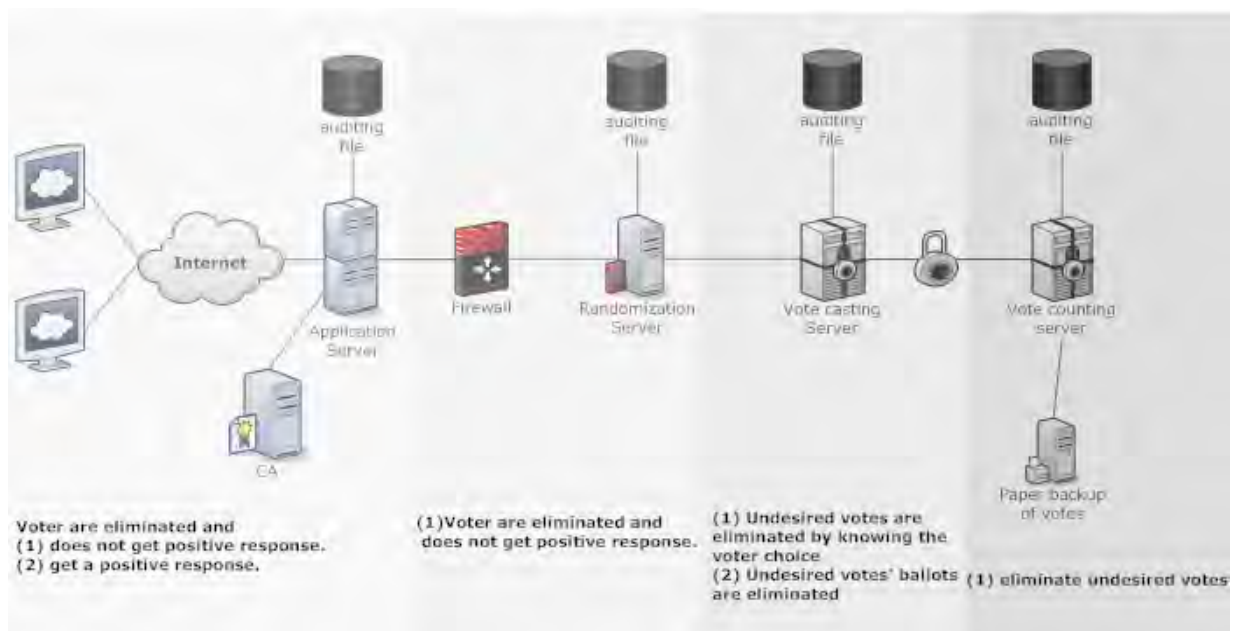


Figure 10.1: Possible ways of large-scale vote rigging identified in the Estonian I-voting system.

(EUDO, 2007; redraw by the researcher)

Below, each type of vote rigging is considered in detail.

10.3.1 Vote forgery

A voter generates vote, v , and before it can be encrypted and secured, the attacker converts it into vote, vn , where $v \neq vn$, all of this being completely unknown to the voter. In order to mount the attack, let alone for it to be successful, the attacker requires extensive control over the voter's processes. The assumption states that attackers cannot extensively control such processes. Therefore, extensive vote rigging by imposing control over the vote-casting process is almost impossible. There are opportunities for vote rigging in the network server, the vote-recording server and in the connections between the applications used by the voter, but these opportunities can occur only as long as ineligible persons are able to vote or eligible voters can do so more than once.

10.3.2 Voting by ineligible people

Instead of one vote for each voter, the attacker attempts to create, for example, 2000 new, confirmed, signed and encrypted votes. In order to create large numbers of encrypted, signed votes using voters' names, the attacker is required to have extensive access to large numbers of voters' confidential signature keys. Assumption 3 states that attackers do not have extensive access to voters' confidential keys. Furthermore, if the attacker is able to vote without access to confidential keys, it is necessary to have the means to break the signature program. Assumption 1 assumes that this is impossible. Thus, based on the assumptions, ineligible voters are unable to cast many correct votes.

10.3.3 Multiple votes by eligible voters

In the proposed I-voting system, voters can vote more than once but the system invalidates such multiple votes. In the case in which the attacker has access to the server and can alter the process that invalidates multiple votes, eligible voters would be able to vote many times.

This kind of attack is not productive. Extensive vote rigging using attacks on the vote-counting server or the connection between the vote-recording and vote-counting servers is regarded as an internal attack. The connection between servers performs data

transmission using data links, i.e., data transmission is non-linear or outside the network. The Estonian vote-counting server in the Estonian system is connected to the Internet.

The vote-counting step is secure according to Assumption 3. Let us assume that it is possible to attack the data carriers or vote-counting server before the vote-counting step. Encrypted votes are transferred to the vote-counting server. Therefore, to add new votes to the server, the attacker is not required to have confidential signature keys. This attack requires knowledge of how the voting algorithms works to create encrypted votes and to send them over the data link or to the vote-counting servers. In the network's storage (recording) server, a database registration file is present which contains all the encrypted votes and personal information about voters. Assumption 6 states that the independent file registration system in the proposed I-voting model is secure.

For a successful attack on the vote-counting server or the data links, the attacker also has to attack the vote-privacy server in order to add encoded votes and voters' personal data to the database files. This could mean that the attack also includes the vote registration and voting servers. The probability that the attack would succeed is low and it is therefore pointless. In addition, in order to change an auditing file on the vote-privacy server, the attackers would need to alter the existing log file in the network server. It is obvious that the I-voting attack is unproductive. Hence, the attack would need to access the vote-counting server outside of network or data links. Vote theft is, however, unlikely on a large scale.

The proposed I-voting model ensures that: (1) ineligible voters are deprived of the right to vote and (2) legitimate voters cannot put two votes in a ballot box and expect both to be counted towards the final result.

10.3.4 Large-scale exclusion of votes from a ballot.

Large-scale exclusion of votes from an election is another type of vote rigging which should be discussed to enhance the security of voting process. The purpose of excluding votes from an election is the deletion of votes for candidates the attacker does not want

to win. When considering the ways in which this can be accomplished, the first possibility is to attack the vote-registration stage. In the proposed model, electronic voting reference-determination certificates and digital signatures are distributed by the national PKI system to voters. By Assumption 5, the Qatar National PKI is safe. Therefore the attack against the vote-registration stage is impossible by this assumption.

In order to realise voter exclusion on a large scale using attacks on the I-voting system's components, the possibilities are votes being removed from the I-voting system either with or without receiving a positive response from the I-voting system.

Furthermore, the researcher considers points at which attacks are made on the network level. For example, this type of attack means that the votes from legitimate voters never reach the system; service attacks on the network level will deprive eligible voters of the right to vote. If voters are unable to vote, the election committee will be informed. Hence, the attack is possible but could be solved by Assumption 7.

The first possibility is that a vote is omitted but the voter still receives confirmation that the vote has been cast. In this case, the voter's voting application must be compromised to achieve successful attack without the need to compromise election servers, so that it converts an error message from the network server. This kind of attack has low profile of success., e.g. Estonia has not reported such incidence.

Secondly, if there is an attack on the network server or connections between network servers and the vote-privacy server, voters can drop their votes into the ballot box but will receive error messages. By Assumption 6, this would mean that the Election Committee will be informed about misbehaviour and will bring the electronic voting process to an end.

To carry out a vote deletion attack it would also be necessary to attack the vote-privacy server. The attacker would need information on the voters or votes to delete votes they did not want, but these are encoded, signed votes. If the attacker wants to delete votes based on their value, they need to decode the votes. Assumption 1 states that the

attacker cannot access the confidential SK, decoding key. Therefore, attackers could not delete votes they do not like using this method. In order to infer a vote's value, the attacker needs to know the random numbers in the voting papers without having access to confidential keys. Hence, the attackers cannot control the voters' processes in this way. As a result, the attack based on deleting unwanted, encoded ballots is not possible.

Another alternative for achieving this aim is to use a list of voters and to delete their votes on the vote-privacy server. The proposed model would use an independent auditing system that guarantees a fair election. If some votes are deleted without modification of the log files, the total logs cannot be confirmed. As a result the validity of the electronic vote is compromised and the voting process ends and is nullified by Assumption 6.

If it is assumed that the attacker deletes votes in the vote-privacy server so that the deleted votes do not reach the auditing system, it will also be necessary to connect to the network server in order to acquire the vote data written to the database. This kind of attack is unlikely to succeed, because vote auditing is established at each stage to guarantee the integrity of the election.

Finally, consider an attack against the vote-counting server or an attack mounted at the end of the election process when the votes are transferred to the vote-counting server. To delete specific votes, the attacker needs to know the vote value (preference) and the number of votes. Thus, the attacker will need to gain access to the confidential keys. Assumption 3 states that attackers do not have access to the confidential I-voting keys. If attackers modify the encrypted ballots so that it appears as invalid or corrupted, a routine check is made at the counting stage comparing the electronic and the paper ballots to identify invalid votes.

This analysis has shown that to decide which votes are unwanted, attackers would need considerable control over the voting process. In this case, Assumption 8 is violated. In addition, as attackers need to take control of the auditing system, this forces them to attack the network server and the vote-privacy server.

10.4 How the requirements of I-voting are met by the proposed system

This section examines the proposed I-voting model to ensure that it fulfils the voting principles in term of security as mentioned in section 3.4.2.5. Table 10.1 Shows how voting principles are satisfied by the proposed I-voting model.

Table 10.1: Fulfilling the I-voting requirements

Requirement	How the requirement is met
Eligibility	Only the eligible and authorized voter can vote. This is fulfilled by the authentication stage using a smart card and PKI.
Privacy	All votes are kept secret by encrypting each vote.
Receipt-Freeness	
Fairness	
Accuracy	The existence of two data sources for voter and candidate databases enables a double count of the vote using both sources giving a check on the results that is a guarantee high accuracy. Both individual and universal verifiability is guaranteed where a voter can check that their vote has been counted from the voters' and candidates' database.
Individual Verifiability	
Universal Verifiability	
Reliability	The security procedures are used to guarantee the reliability because the voting process cannot be completed unless all these steps are completed successfully.
Convenience	The model is convenient and can be used anywhere because of the use of the Internet
Mobility	
Flexibility and usability	The model is flexible because the voter needs only a few clicks to complete the voting process, also the use of a computer to cast vote could be useful for many individuals with disabilities since there are tools that assist disable people such as Braille keyboards and screen readers.
Transparency	All votes and credentials are kept secret but can be unambiguously retrieved at any time.
Scalability	The model is scalable in that it can cover all countries in the world because of the use of the Internet
Efficiency	The model covers almost all the principles for the secure elections, yet it does not need many resources.
Security	The model maintains security at every stage from the client machine to the servers.
Cost effective	The model could be implemented with minimum cost since the Intranet provides most of the required infrastructure for I-voting.

10.5 Evaluation

The evaluation of the proposed model was done in three phases. The concepts and design of the system were firstly evaluated by two experts. The approach was to measure their opinions on the effectiveness of the system based on a seminar followed by a questionnaire and discussion of the system. The two experts who were involved in evaluating the proposed model were a network security expert from the Ministry of Interior and one from Integralis, an IT Security Solutions company. A local and a European expert were chosen for their knowledge in IT security. The researcher took advantage of personal contacts with the experts and asked them review the proposed model and to fill out the questionnaire on their own and provide their feedback. The questionnaire covers many aspects regarding I-voting in terms of security, model architecture, confidence of I-voting and legal aspects of it.

A second evaluation of the concepts and design of the I-voting model was carried out by a sample of 75 eligible voters from different backgrounds to identify their acceptance of the proposed model and their opinion about the model design (see section 9.6.2). Their evaluation was conducted by given them a seminar on the system and then gathering their opinions by a questionnaire.

Finally, after the design of the proposed model was validated by experts and voters' opinions, the prototype implementation of the proposed model was developed to test the applicability of the model in the real world. An independent expert from University of Bristol, doing a PhD in Machine learning, volunteered to evaluate the implementation of the model.

10.5.1 Expert evaluation on the proposed model design

A summary of the experts evaluation is provided in Table 10.2

Table 10.2: Summary of expert evaluation

Topic	Ministry of Interior expert	Integralis company expert
Network bandwidth and performance, plus load balancing	<i>"It is important to note that the I-voting model is introducing extra information to be manipulated. These types of information imply more load on the network which needs to be addressed. From our experience with a previous project implemented for the MOI, the network has always been a disabler on performance. Due to the critical nature of the model, network performance will be studied and recommendations will be provided to the MOI in order to provide the necessary network capabilities."</i>	<i>"Evaluate load balancing using DRS between the client and the host server. DRS can head off a bottleneck before it happens. This allows effective use of all server resources, regardless of the server in which they are located. It also may eliminate or delay the need to purchase new hardware in the future by utilising all available hardware resources."</i>
High Availability of I-voting system		<i>"Putting several virtual machines onto one physical server is putting all your eggs in one basket. Mitigate this risk by deploying VMware High Availability to give all of your virtualised machines high availability without having to cluster each one of them."</i>
Back-Up	<i>"Your approach in auditing at each stage would not be sufficient for a back-up of each voter's vote. It would be necessary to use virtual back-up to different secure locations."</i>	<i>"Allow an administrator to backup the virtual machine from "outside" but within the server host. This allows agentless backups, backups off the production network, no concerns for open files, and backups without impacting on the performance of the virtualised server."</i>
Cryptographic algorithms	Good use of different cryptographic algorithms to harden breaking in to the system: (1) RSA, for creating and checking blind and non-blind signatures and encrypting the keys (2) 3DES Key and the TimeStamp used for encryption (3) SHA-2 used to produce message digest.	<i>"Deploying the state of art of cryptographic algorithm would be efficient for carrying out such data with the Internet network. "</i>
	<i>"Communication between servers is authenticated using SSL-3 and public key."</i>	<i>"The accuracy of vote casting and vote counting is well demonstrated with a policing signature to verify the vote correctness."</i>
	<i>"Verifiability is achieved by allowing a third party (the Election Committee) to verifying the signatures of the votes before publishing the voting result."</i>	The principle of one voter one vote is achieved due to the design of the model which guarantees $t > V/2$ All voters can vote as long as t are available in both the vote registration and privacy server.
	Both experts stated that privacy was assured through the use of a hybrid protocol (blind signature and mix networking) to established anonymity and a process using three factors for authentication (1) smart card (2) PIN (3) biometrics.	

10.5.2 Voter evaluation on the proposed model design

The experts' evaluation deduced that the proposed I-voting model could be possible and secure. However, it was also necessary to test whether people would accept the approach. For this purpose, a seminar was designed to demonstrate the approach simply through an understandable explanation. The seminar was then given to a number of eligible voters along with a questionnaire to be completed after the seminar was held. The presentation aimed to address the challenges that arise in an I-voting system, including accuracy, ease of use, efficiency and the security of such a system (i.e. identity assurance, vote confidentiality and integrity and auditability).

The proposed solution was shown to satisfy these challenges (see Section 3.4) by proposing I-voting as a specific case of remote electronic voting, whereby the vote takes place over the Internet via a web site or voting applet. The approach was demonstrated in simple steps with simplified technical terms though real examples. The seminar took about 45 minutes including questions and answers during the seminar. 75 Qatari eligible voters from different backgrounds participated in the evaluation. They were selected as convenience sample of the researcher's contacts from Qatar foundation, friends and family. The participants were representative of the total population since they were from different background and chosen carefully to cover variety of people. The seminar was delivered five times to cover the total sample population

The questionnaire consisted of 27 questions in 8 question groups, as shown with the results in figures 10.2 to 10.9.

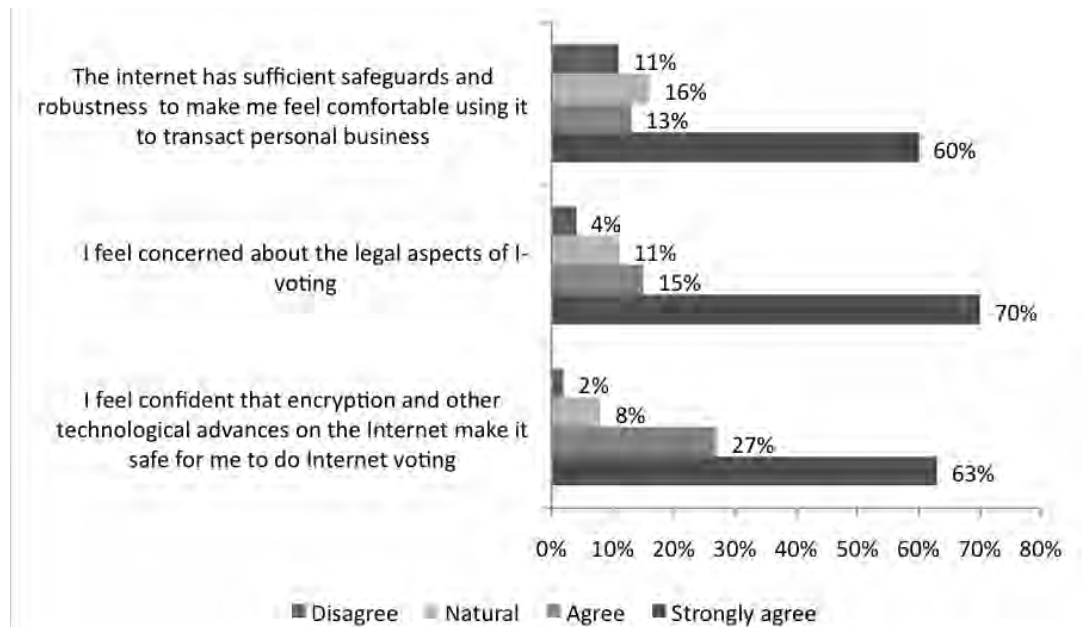


Figure 10.2: Do you agree that the Internet is safe and there are no legal issues concerned with I-voting?

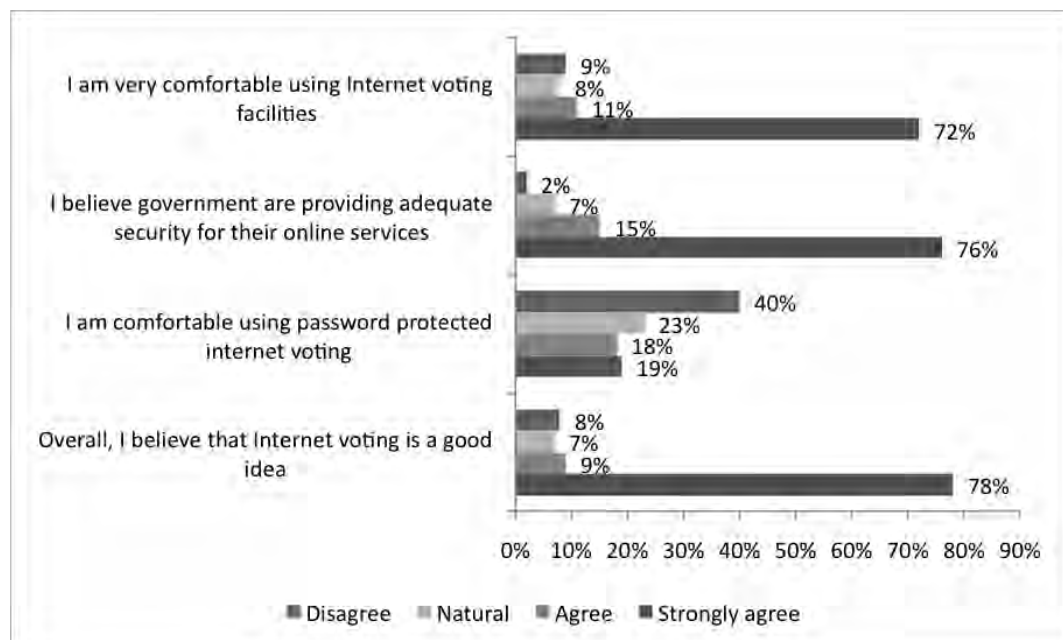


Figure 10.3: Do you agree that you are comfortable with I-voting, that it is a good idea and that e-services are secure?

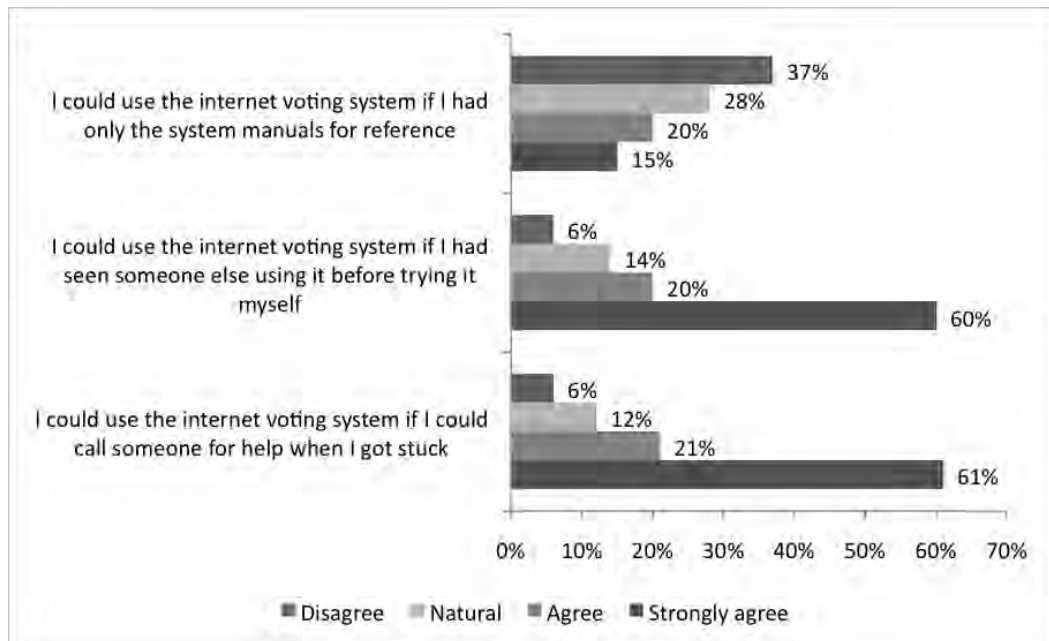


Figure 10.4: Would you agree to use I-voting with available support?

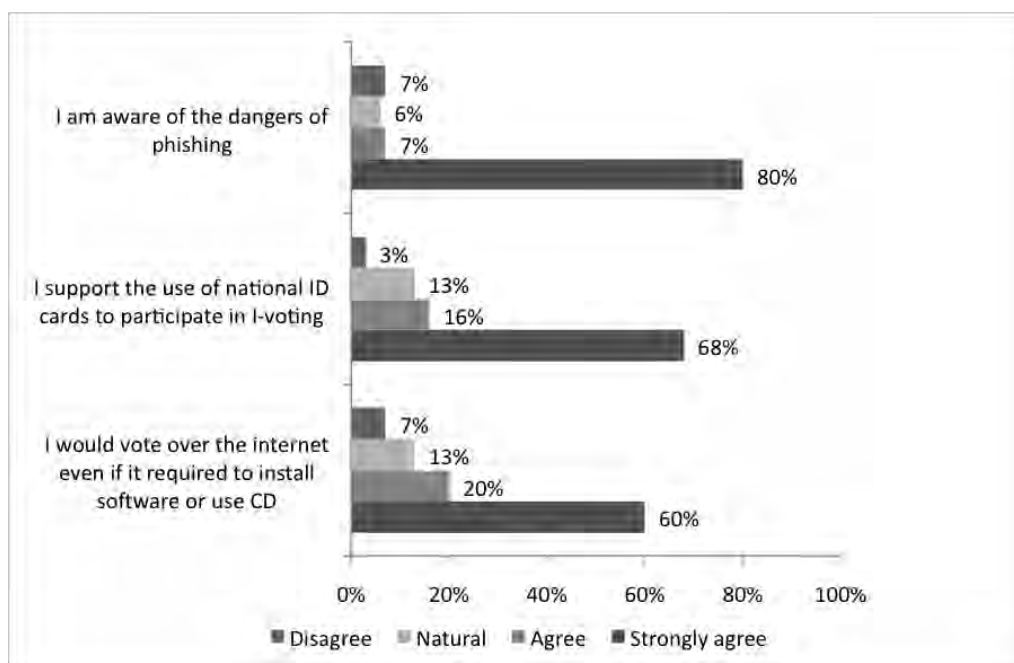


Figure 10.5: Do you agree to use your national ID, would you install software to vote and are you aware of phishing?

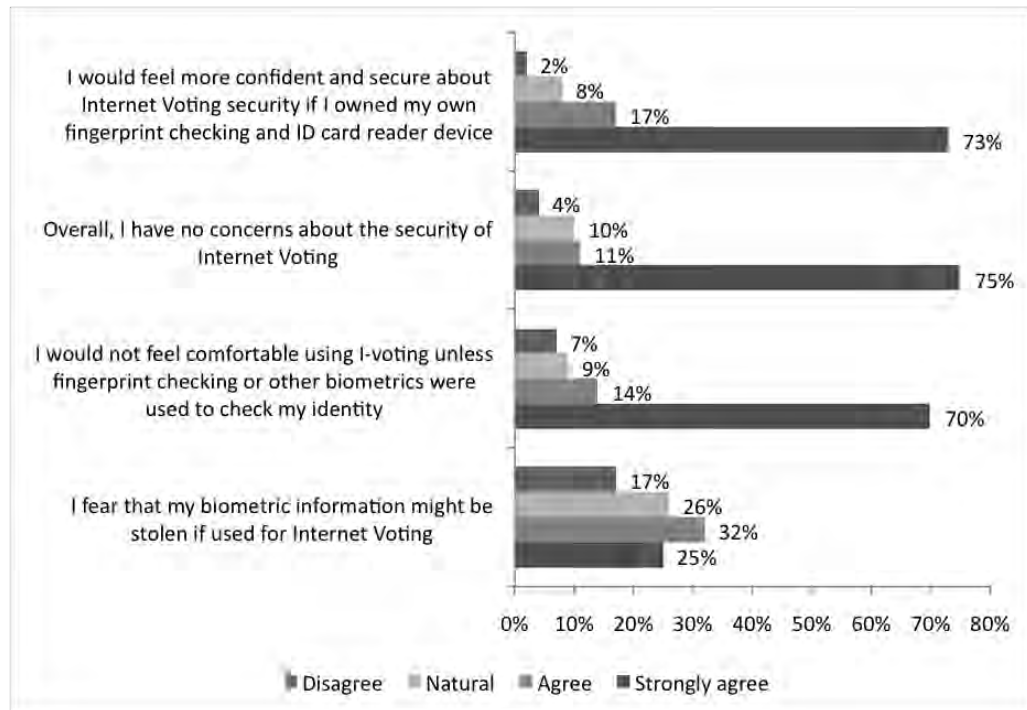


Figure 10.6: Would you agree to use biometric data to provide secure authentication for I-voting?

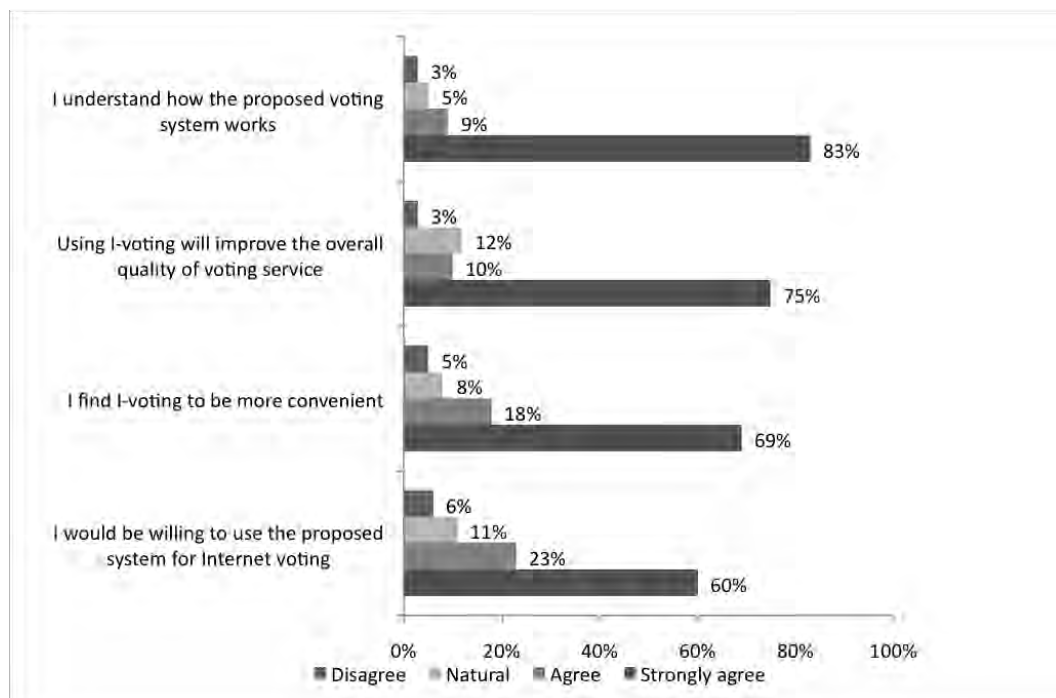


Figure 10.7: Do you agree that the proposed system is understandable and convenient?

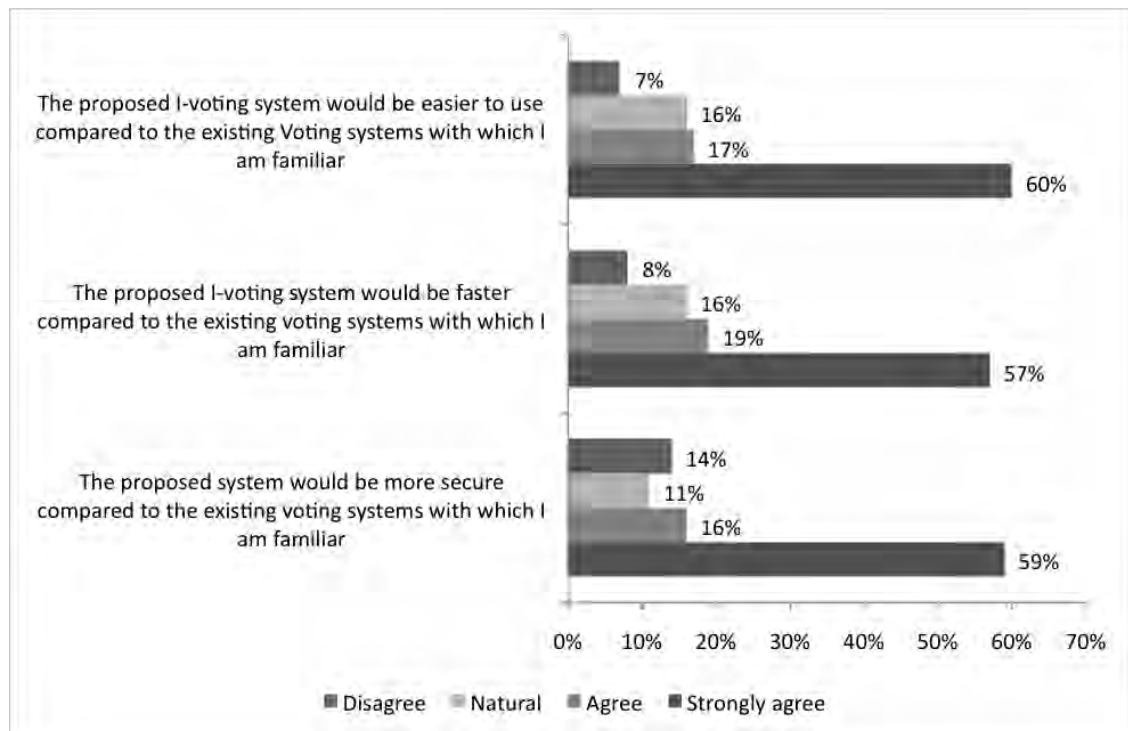


Figure 10.8: Do you agree that the proposed system is easier, faster and more secure than the existing system?

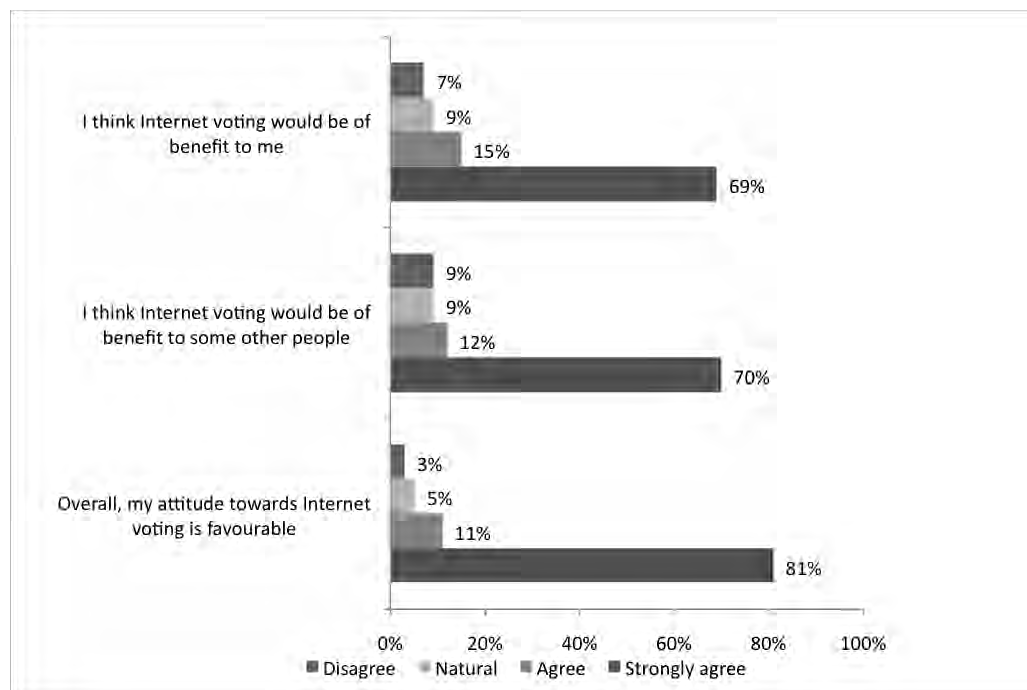


Figure 10.9: Do you agree that I-voting is desirable and beneficial for people?

A summary of the voter evaluation is given in table 10.3.

Table 10.3: A summary of the voter evaluation

	Voter evaluation
Background	Most of the participants were male (70%) and the majority (40%) were of age group from 18-29 and few (4%) were above 50 years old. The majority (80%) had Internet experience of more than two years and only 15% had no experience of information technology, a high proportion of which were older people above 45.
Security of Internet technology	<p>The assurance of the Internet was assessed in terms of the people's trust and faith in Internet security. The result was encouraging, since about 60% strongly agreed that the Internet can be a robust and safe environment if the system were built based on the ISO/IEC 27033 standard (see Figure 10.2). This belief was based the fact that banks and the government won't risk using the Internet if it was not a safe environment to run their systems. The other 40% either strongly disagreed or distrusted the security of the Internet, pointing to the history of e-crime. There was a high percentage (80%) who were cautious of the dangers of phishing and e-crimes and the intelligence of hackers in breaking any secure system (see Figure 10.5).</p> <p>About 63% did not trust the encryption process, pointing out the possibility of clever hackers breaking the process, especially with the development of computer power (see Figure 10.2). This was despite the fact that the researcher had clearly stated that there should be a very strong encryption process which would need years to break. In Internet voting, records would only need to be encrypted and secure until the official time for publishing the results, which is a limited time for hackers to break the encryption.</p>
Legal aspects of I-voting	More than 70% were concerned about the legal aspects of I-voting due to the inefficiency of the current Internet law (see Figure 10.2) despite, the researcher explaining that Qatar is in the stage of approving the new Internet law, which was designed based on worldwide best practice.
Comfort with the principle of I-voting	The result of the survey were encouraging since about 76% strongly agree that I-voting is a good idea, 55% of participants strongly agreed they were comfortable with the system and 72% strongly believe that the government are providing adequate security for their online services and therefore would provide a secure I-voting system. However, some 40% felt uncomfortable using password protected Internet voting due to the possibility of passwords being broken by hackers (see Figure 10.3).
Usability of I-voting	61% strongly agreed that the I-voting system is easy to use if there is a consistent help service or if it people were trained how to use it. However, only 15% believed the user manuals would be useful to help users to interact with I-voting. This suggests the I-voting system should be tried first in a polling station to introduce users to the system and show them how to use it. A further possibility would be a call centre, available 24 hours a day during the voting period to help users (see Figure 10.4).

Technology used in I-voting	<p>68% strongly agreed with the use of national ID cards for I-voting since they found these to be trustworthy and secure. This is encouraging as national ID cards provide a secure method of authentication containing a biometric template of the card holder and they use existing resources.</p> <p>However, more than 60% strongly disagree with the use of Internet voting when it requires the installation of software since they would find it hard to use and time consuming. This suggests a better technology is required. A possibility is an applet which will act as a middleware between the server and client, doing the CD task without the need for installation (see Figure 10.5).</p> <p>More than 70% strongly agreed with the use of a biometric technology identity checker. 73% were strongly agreed they would feel more confident and secure with Internet voting if they owned their own fingerprint checking and ID card reader device. Therefore, the use of finger print technology is encouraged, although some 25% were strongly concerned that their biometric information might be stolen if used for Internet voting. On the other hand, there is considerable trust in the government and the security of the national ID card. 75% strongly agreed with and have no concerns on the security of the proposed I-voting system because it uses multi factors of authentication which is virtually unbreakable (see Figure 10.6).</p>
Acceptance of the proposed I-voting model	<p>The process of I-voting presented in the presentation was understood by more than 80% of the users. However, half of the participants still considered I-voting to be no more secure than the voting methods currently used in Qatar. The rest thought I-voting would be more secure.</p> <p>The majority, about 60%, felt strongly encouraged to use the proposed I-voting system with its confidentiality, improvement of the overall quality of voting service, and the ease and speed of the vote casting process (see Figure 10.7).</p> <p>The majority (about 60%) strongly agreed that I-voting would be easier, faster and secure compared to existing voting system. However some (40%) still believed the existing voting system would be much easier to use than I-voting since it is more familiar (see Figure 10.8).</p> <p>About 69% of the participants strongly agreed that Internet voting would be beneficial for them and more than 70% thought it would be beneficial for other people such as older people and those with disabilities who might have difficulty getting to a polling station. Overall, 81% strongly recommend and favoured the use the proposed Internet voting as an alternative voting system.</p>

10.5.3 Expert Evaluation on the implementation of the proposed model

The expert from Bristol University was given a demonstration of the I-voting model using the developed prototype. He agreed that the system seemed to work in practice and offered the following opinions on the implementation.

The expert agreed the proposed approach offers a strong security process to register the votes by including smart card verification to complement the verification using personal information. Moreover, the approach includes a PIN verification to reinforce the security of using a single private key during the identification on polling day. By decentralising the information in different databases (DBs), the architecture can support a good workload for a large scale of users and improve the security of the database. Also, getting access to the first database or the second database in read mode would not be enough to vote on behalf of a voter since the private key is not recorded.

The expert noted that the weak point of the approach is at the end of the vote registration, as the structure of the voting key file contains the ID record as used in the table of the first database. This may simplify the process for the identification on polling day but also provides undesired information to the voter from the server. By using high performance computing, it may be possible to find the private key and the signature in the database for a particular recorded ID. Then, if the voter has not cast his/her vote then there are a number of chances for a person to vote illegally on behalf of the voter, particularly if the length of the PIN is short. The security can be easily improved by increasing the key length or the PIN length, but increasing the key length increases the computation time to generate the pair of keys and may reduce the ability of the server to manage a large number of users. Increasing the PIN length also increases the number of typing errors by the voters. On the other hand, increasing the PIN length reduces the probability of an illegal vote. One solution to avoid the computation of the pair of keys (public and private) could consist in storing a set of keys with a large key length and deleting them in the storage once selected by the server.

The discussion with the expert then turned into a small brainstorming session between the expert and the researcher to identity the possible scenarios for an illegal vote, a

deeper analysis of the architecture was carried out. This showed the following different cases for an illegal vote which have been ordered in range of importance:

1. Gaining write access to database 1, 2 or 3.
2. Obtaining read access to database 1 and generating a private key which matches a record in database 1 of a person who had not yet voted.
3. Stealing the voting key file and the PIN in the letter of a person who had not yet voted.
4. Stealing the voting key file and generating the PIN of a person who had not yet voted.
5. Generating a voting key file and a PIN which matches a record in database 1 of a person who had not yet voted.

The conclusion from the brainstorming session was that all of the above are unlikely to happen with highly secured databases and with a large key length for the private key of the voting key file. But it is interesting to note that, in all but the first case, the number of illegal votes can be more important when an attacker has read access to database 2. The reason is that with this read access it is possible to identify a voter who had not yet cast their vote. Also, it is interesting to note that the PIN code, in itself, does not provide enough information for a person to vote illegally since a vote cannot be cast without the voting key file. Finally, it is important to observe that case 3 above is a special case of 2. However, case 2 can be more secure by removing the PIN from database 1 and securely transferring it into a new database. Thus, case 4 can become a special case of 2. This decentralisation can have the benefit on reducing the workload on polling day.

This analysis has shown that the architecture is appropriate for I-voting and that the security of the databases is at least as important as the voting key file generated for a voter. It would be interesting to evaluate the scalability of the application using real checking of personal information and smart cards.

10.6 Summary of evaluation

The experts showed a great interest in the proposed I-voting model. They believed the model is effective and fulfils voting principles efficiently through a clear process that is usable by the voters. The model makes use of existing smart card technology along with strong authentication and anonymity process to ensure security, privacy and transparency of I-voting.

The voters showed a high level of acceptance (above 80%) of the I-voting concept, believing it to be beneficial, secure, usable, accessible and reliable. They were comfortable with the concept and had confidence in the system. This is a strong motivation for implementing the proposed I-voting system as an additional, alternative means of voting, and more than 80% strongly favoured doing so. However, 70% have some concerns about the legal aspects of I-voting and about 80% had some concerns about the dangers associated with I-voting, such as phishing and e-crimes. The majority, about 60%, strongly agreed with the use of national ID cards for I-voting authentication, and the use of an identity check through different technology such as biometric and fingerprint methods.

The results show the successfulness of the approach in theory and the primary results from the prototype implementation of the model show that the architecture is feasible and is secure enough to be used for I-voting. However, the scalability of the architecture needs to be evaluated.

10.7 Conclusion

The proposed model obtained a good degree of acceptance by experts, in term of satisfying these voting requirements, despite the challenges of possible attackers, which will always require further investigation to safeguard the system. In this chapter the model has been analysed and tested. However, the protection of each voter's machine still remains an obstacle as it is the most vulnerable aspect of vote casting. The use of a secure operating system or Internet browser could solve the problem but the system usability would be affected. The voter survey showed that many users would find difficulties in using the system and would not favour using it. However, use of software middleware that does the same task as the secure operating may solve the problem, but more investigation is needed to identify all possible attacks.

Possible means of meeting each threat in the proposed I-voting model are shown in Table 10.4

Table 10.4: Possible threats and solution of I-voting

Threat	Potential solutions
Network Security	Encryption Intrusion detection system Redundant firewalls Penetration tests
Privacy	Digital signatures Secure socket layers Encryption Voter identity/ ballot data separation Voter ballots data verification
Virus, Worm and Trojan horse	Anti virus scanning Digital signatures Voted ballot data verification
Spoofing	Secure socket layers Digital signatures MMQ (Message queuing) Voter ballots data verification
Denial of service	Large quantity of bandwidth, multiple carriers Multiple Internet service provider entry points

	Utilization monitoring
Voter fraud	Digital signatures
Voter authentication	PKI Digital signatures Digital certificate
Vote casting	Blind signature Tor for anonymity Mix networking (Proxy server) Ssh-2 (Create secure tunnel)
Voter Client machine	customised Linux OS boot by CD Digital signatures SHA or MD5
Availability	deploying VMware from Dell company
Vote selling	Three factor of authentication Smart card PIN (One time password) Biometric (Finger print)
Transparency	Open source (Linux OS)
Tally Process	DRE Paper backup

The expert who evaluated the prototype suggested focusing mainly on evaluating the scalability of the architecture. This will provide an insight about how many servers are necessary to manage an election in a country and, in particular, the State of Qatar. Furthermore, the expert suggested the prototype should be tested using real smart card technology. For future improvement, the expert believe that the security could be improved further by using a mix network but at the risk of losing the scalability of the architecture; this needs to be investigated and experiments carried out. In the research reported in this thesis, due to a lack of time and resources, a mix network could not be implemented. The technical resources needed to elaborate a mix network would have involved a set of servers to setup a chain of proxy servers.

The next chapter focuses on providing recommendations to help Qatar government to introduce I-voting. The recommendations include the following areas digital divide, e-literacy, I-voting infrastructure, legal aspects, transparency, security and privacy.

Chapter 11 Recommendations for introducing Internet voting in Qatar

This chapter presents recommendations derived from the study to assist the Qatar government in introducing I-voting in Qatar. The recommendations address aspects of I-voting which include the digital divide, e-literacy, I-voting infrastructure, legal aspects, transparency, security and privacy.

11.1 Introduction

Qatar is comprised of eight municipalities and had its municipal elections during the year 2007. The overall percentage of the population who exercised their vote came to around 51% of the total population who used the ballot paper system to cast their votes. The government feels that it was due to this that the percentage of people who voted was so low (Khalaf and Luciani, 2008). The country has been adopting, over recent years, new and emerging technologies aimed at its overall development and the government, therefore, feels that an electronic voting system will attract more people to exercise their voting rights (ICTQatar, 2007). This implies they believe it would be better for the country to introduce an I-voting system for future elections.

This research thus focuses on introducing I-voting in Qatar, as an addition to the current voting system, to enhance democratic processes and e-literacy. Accordingly, the research aim is to provide effective recommendations for the government of the State of Qatar to help in introducing I-voting in future elections in Qatar. The outcomes of the empirical and non-empirical research carried out in Qatar have created a basis for putting forward the recommendations for introducing I-voting. A summary of the outcomes of research reported in previous chapters is given in Table 11.1.

Table 11.1: Summary of Outcomes and Implications of I-voting Research in Qatar

Chapter	Main outcomes	Implications for the recommendations
Chapter 3: Literature review	<ul style="list-style-type: none"> • Identifies barriers and potential solutions for I-voting. • Identifies motivations for I-voting • Identifies suitable I-voting protocols • Reveals the extent of previous experience of I-voting • Highlights a deficiency in the literature in a particular area of the world, the State of Qatar. 	<ul style="list-style-type: none"> • Forms the basis of recommendations to help adoption of I-voting in Qatar • Identifies potential solutions for I-voting • Enables recommendations to take into consideration I-voting barriers and how to overcome them.
Chapter 5: Qatar	<ul style="list-style-type: none"> • Identifies the feasibility of I-voting in Qatar, covering multiple factors such as government willingness, accessibility, availability of IT infrastructure, support from Qatar law and Qatar culture, availability of Internet law to protect online consumers and the existence of an e-government project. • Identifies issues for I-voting, concerning security, privacy, usability and transparency. 	<ul style="list-style-type: none"> • Ensures recommendations take into account local conditions and are suitable and practical in the State of Qatar. • Suggests I-voting should be implemented alongside the current paper-based voting system
Chapter 6: Survey	<ul style="list-style-type: none"> • Identifies factors concerned with the Qatari people and their willingness to participate in I-voting, such as high computer knowledge, high usage of e-services, and trust in general elections in Qatar. • Discovers features of I-voting preferred by Qatari citizens. • Discovers the effect of education level on people's responses. • Reveals that one third of the population would find difficulties in using I-voting technology. • Reveals one quarter of the population is concerned about security issues and one seventh about reliability and accuracy issues associated with I-voting 	<ul style="list-style-type: none"> • Ensures recommendations take into account abilities and preferences of the local population. • Identifies areas where the population would need greater information and assurances to be comfortable with I-voting
Chapter 7: Experiments	<ul style="list-style-type: none"> • Identifies the feasibility of I-voting but reveals possible client issues in terms of knowledge and awareness of information security related to I-voting. 	<ul style="list-style-type: none"> • Identifies areas where greater information and education are needed.

Chapter	Main outcomes	Implications for the recommendations
Chapter 8: Awareness	<ul style="list-style-type: none"> • Identifies the need for enhancing user awareness in information security to avoid risks associated with clients. • Reveals that users perform many inappropriate actions which might put them at a security risk due to a lack of awareness on information security, such as 22% react to fake security warnings and respond to suspicious links, 43% open e-mails from unknown senders and 58% do not read firewall alert messages. • Reveals that, in contrast, some participants perform some correct actions, such as checking file extensions before downloading, turning on security applications and updating their anti-virus software. 	<ul style="list-style-type: none"> • Shows a need for an awareness campaign on security issues.
Chapter 9: Model definition	<ul style="list-style-type: none"> • Defines an effective I-voting model for Qatar using advanced technologies and protocols such as smart cards, biometrics and mix networking. • Defines five phases to complete the voting process: authentication, registration, anonymity, vote casting and counting. 	<ul style="list-style-type: none"> • Shows that an I-voting system that addresses all the concerns of experts and voters could be possible using appropriate technology and processes.
Chapter 10: Justification and evaluation	<ul style="list-style-type: none"> • Shows the model has a high level of acceptance (more than 80%) amongst the Qatari population who believe it fulfils voting principles effectively. • Shows the model encourages I-voting as an alternative method of voting with more than 80% strongly favouring the proposed I-voting model and about 60% strongly agreeing with its use of national ID cards. • Reveals that, in contrast, 70% were concerned about legal aspects of I-voting and 80% about Internet threats associated with I-voting. 	<ul style="list-style-type: none"> • Shows that basing recommendations on a tested model has a high level of acceptability if the model takes into account all the issues and factors identified in earlier chapters

11.2 Recommendations

Based on the findings of the previous chapters, recommendations have been defined to help the Qatar government promote and implement I-voting. These comprise recommendations on aiming to enhance reduction of the digital divide, e-literacy, Internet infrastructure, the law, transparency, security and privacy. These aspects are addressed as follows:

11.2.1 Recommendations 1: Reduction of Digital Divide in Qatar society

The digital divide is the gap between people who have access to the Internet and those who do not. *“Because of changes in technology, the digital divide is actually being defined in terms of broadband access versus telephone access.”* (White 2007, p. 120). The government of Qatar has made a large investment in reducing the digital divide by launching the free ipark project for public access to the Internet. In addition, the competition in the telecommunication market has assisted in reducing the cost of Internet access and improving the quality of service provided by the Internet service providers. Therefore the Internet has become accessible even to people with low income. According to ITU (2009), 52% of the population have access to the Internet and if we exclude the ineligible voters, this percentage could increase. Therefore, there is no problem in adopting an I-voting system in Qatar because the majority of Qataris use Internet facilities, providing the system is practical and compatible with the postal voting system.

Although there is currently a plan by the Qatar government to reduce the digital divide, the research has provided some recommendations for the government to enhance this plan, as summarised in Table 11.2.

Table 11.2: Recommendations 1 Reducing the digital divide

Recommendations	Cross reference to chapter
1.1. Provide I-voting at polling stations as an option for voters. This will provide accessibility to voters who do not have access to the Internet or who prefer not to use their own machines to cast their votes.	Chapter 3: Literature review
1.2. Use the Internet to provide training on how to use I-voting.	Chapter 8: Awareness
1.3. Encourage organisations and the public sector to donate computers through an authority taking responsibility for distributing them to people in need.	Chapter 5: Qatar
1.4. Provide the Internet free of charge in the election period, using telephone lines. This implies the government should pay the costs of Internet service providers.	Chapter 5: Qatar
1.5. Enhance free wireless Internet in public areas such as shopping malls and coffee shops.	Chapter 5: Qatar
1.6. Ensure the availability of the Internet network in all areas in Qatar.	Chapter 3: Literature review
1.7. Increase the Arabic content of the Internet, e.g. on government websites, because Arabic is the native language of Qatar and, hence, the electorate would feel more comfortable using Arabic	Chapter 3: Literature review

11.2.2 Recommendations 2. Enhance E-literacy in Qatar.

With the huge development in technology, the problem of e-literacy appears. This refers to those people who do not have enough computer literacy and knowledge to carry out online activities. The government has focused on human development as an important element for the development of Qatar. Therefore it has invested intensively in education, recognising that education is an investment for Qatar's future and it is aiming to be the centre of educational excellence in the region. Accordingly, the Minister of Education has plans to change the education curriculum to make it equivalent to that of developed nations, through a project called 'Education for the new era' (Ministry of Foreign Affairs, 2007c). This involves enhancing citizens' English and computer literacy to university level. In addition, the government has developed an educational "city", known as the Qatar Foundation, aiming to enhance education, containing educational facilities ranging from schools to some of the world's leading universities and research centres.

Computer literacy has become an important achievement required for entry to university and for many jobs since most jobs today require IT skills. Therefore, the education sector and organisations need to work on developing computer literacy for their students or employees by providing training courses on computer skills such as the ICDL (International Computer Driving Licence) (ICDL GCC Foundation, 2009). In addition, Qatar has launched an e-government project which has more than 90 e-services to transform the traditional process of dealing with government departments into electronic form. Furthermore, many non-government e-services exist in Qatar, including online banking, online payment and e-commerce. This helps to increase e-literacy in the state.

Although some steps are being taken to improve the e-literacy of the Qatari population, an increase in the overall level of e-literacy is clearly desirable for the country to adopt I-voting. To improve the level of e-literacy, Table 11.3 gives recommendations for the government, derived from this research.

Table 11.3: Recommendations 2 E-literacy

Recommendations	Cross reference to chapter
2.1 Make the Internet widely available in the country (see reduction of the digital divide recommendations)	Chapter 3: Literature review
2.2 Provide e-training or e-learning on how to use the I-voting application. Also, in polling stations, provide a helpdesk where help can be given for people in need without interfering with the voting process	Chapter 3: Literature review
2.3 Promote awareness of I-voting by involving different parties, including the education sector, private and public organisations and the media, by means of newspapers, radio and television. An awareness programme should introduce I-voting technology to citizens, teaching them the benefits of boosting the democratic process and, at the same time, reducing the resistance to change to the new I-voting system. Further training on how to use I-voting system can be provided through posters, leaflets, and seminars.	Chapter 8: Awareness
2.4 Ensure the I-voting application is accessible for people with disabilities and easy to use by all voters. The government should define a legal requirement to introduce the technology to help people with disabilities in their daily life activities, including voting. For example, people with visual disability could, perhaps, be assisted with use of speech recognition technology.	Chapter 3: Literature review
2.5 Evaluate the e-literacy of the nation using defined criteria and measures to enable refinement and continued development of e-literacy enhancement methods.	Chapter 3: Literature review
2.6 Ensure information on the I-voting process itself and the supporting training and awareness information is available in the official Arabic language of Qatar. Include pictures and use speech technology along with understandable text, taking into account all the latest HCI (Human Computer Interaction) principles.	Chapter 3: Literature review

11.2.3 Recommendations 3. Enhance Internet Infrastructure Development

Many countries have found difficulties in developing basic I-voting infrastructure. However, Qatar has a strong infrastructure base available from the e-government project, which has advanced technologies, including smart cards, biometrics and network infrastructure. This research has led to some recommendations to help create an I-voting infrastructure which will fulfil voting principles effectively:

Table 11.4: Recommendations 3. I-voting infrastructure

Recommendations	Cross reference to chapter
3.1 Develop I-voting in Qatar using current telecommunication infrastructure and available resources, also taking into consideration past world-wide experience in applying I-voting in national elections such as in Austria, Canada, Estonia and France (ACE, 2010).	Chapter 3: Literature review
3.2 Learn from the e-government project's current use of technology, including its failures and successes, to assist in introducing I-voting.	Chapter 3: Literature review
3.3 Provide telecommunications in under-served areas and ensure sustainability of I-voting in the whole state.	Chapter 3: Literature review
3.4 Establish a plan for I-voting in cooperation with experts from the Ministry of Information, ictQatar, Q-CERT and The Election Committee, to provide integrity and effectiveness in the I-voting infrastructure.	Chapter 5: Qatar

11.2.4 Recommendations 4. Provide laws to support I-voting

The current election law in Qatar is not clear with regard to I-voting technology. This implies that for I-voting to be feasible in Qatar a new law is required. Interviews with members of the Election Committee, who showed an interest in I-voting, support this view (see Chapter 5). Some recommendations on legal aspects to support I-voting are therefore made in Table 11.5.

Table 11.5: Recommendations 4. I-voting law

Recommendations	Cross reference to chapter
<p>4.1 Consult current election law to assess how the existing law might work with the introduction of I-voting.</p> <p>E-law has been recently introduced in Qatar, but due to the limited scope of this research it has not been intensively reviewed. However the e-law was designed from worldwide experience. This e-law should, therefore, make I-voting more secure.</p>	Chapter 5: Qatar
4.2 Clarify and simplify the process of appeal for a recount in I-voting	Chapter 3: Literature review
4.3 Provide the legal right for a voter to verify that his/her vote was cast, without revealing the voter's choice of candidate. This should reduce vote selling.	Chapter 3: Literature review
4.4 Provide election law giving procedures and regulations to eliminate vote selling, for example laws should require a combination of technologies for authentication and limit the election duration to reduce cyber attacks.	Chapter 3: Literature review
4.5 Clarify the laws and regulations, making them available for independent agencies to consult and review the effectiveness of the law.	Chapter 3: Literature review

4.6 Reform the voting process by simplifying regulations and procedures to make I-voting preferable to traditional voting.	Chapter 3: Literature review
4.7 Adopt legislation related to information security management, with laws that criminalise cyber attacks and enable effective investigation and prosecution of such activities (UN, 2005).	Chapter 3: Literature review
4.8 Use privacy or network security laws or regulations to take action against misuse of ICT resources (similar to 4.7).	Chapter 3: Literature review

11.2.5 Recommendations 5. Ensure transparency of I-voting

A lack of transparency can lead to low participation and dissatisfaction with government projects, therefore transparency should be present in I-voting to build trust. The recommendations in Table 11.6 address the need for transparency.

Table 11.6: Recommendations 5. Transparency of I-voting

Recommendations	Cross reference to chapter
5.1 Make details of the law, regulations and voting process available online for citizens.	Chapter 3: Literature review
5.2 Use government trusted officials and organisations (e.g. The Ministry of the Interior and ictQATAR) to administer the I-voting process and ensure they provide the information required by citizens.	Chapter 3: Literature review
5.3 Introduce a method of vote verification (see Recommendation 4.2).	Chapter 3: Literature review

5.4 Provide effective training for citizens on I-voting to promote understanding of the process to enhance transparency.	Chapter 3: Literature review
5.5 Keep I-voting regulations, processes and procedures simple to enhance transparency for citizens. This would be similar to the Plain English Campaign (2011) which seeks to make sure public information is as clear as possible. .	Chapter 3: Literature review
5.6 Develop open source software for I-voting, but with access to the source limited to trusted worldwide experts to reduce misuse of the transparency concept by hackers who could abuse knowledge of the system algorithms and data flow.	Chapter 3: Literature review
5.7 Employ independent third parties in the election process to monitor the election to ensure voting principles are met and maintained.	Chapter 3: Literature review

11.2.6 Recommendations 6. Enhance the security and privacy of I-voting

I-voting requires access to the citizens' database, therefore it becomes important to ensure the privacy of citizens' personal information while interacting with the I-voting system. Similarly, security should be ensured and addressed while designing the system. If security or privacy is breached, it will affect public trust in I-voting and reduce turnout. Therefore the recommendations shown in Table 11.7 are made to ensure privacy and security in I-voting.

Table 11.7: Recommendations 6. Enhancing the security and privacy of I-voting

Recommendations	Cross reference to chapter
6.1 Make voters aware of the importance of security, privacy and keeping their personal information private to minimise the security risks associated with client errors.	Chapter 8: awareness
6.2 Design I-voting to preserve privacy using different advanced technologies, such as anonymous algorithms.	Chapter 3: Literature review
6.3 Minimise the amount of personal information required for I-voting.	Chapter 3: Literature review
6.4 Restrict access to the database to only trusted, high officials to avoid disclosure of information.	Chapter 9: Model
6.5 Assign a team of security experts to monitor the Internet network during the election, giving them the required authority to take action to stop attacks by, for example, blocking access by certain organisations if necessary, and giving them the responsibility for investigating any attack.	Chapter 9: Model
	Chapter 3: Literature review
6.6 Make available a special secure browser allowing users to only access the Qatar voting website. This Internet browser should limit features to a minimum, blocking any feature which may result in allowing the user pc to be controlled. This will be necessary because Internet attackers never use their own identities to start an attack, so blocking the source of the attack will, therefore, create another problem.	Chapter 5: Qatar
6.7 Ensure all e-technology used is verified and certified by the Election Committee and computer experts to show its trustworthiness.	Chapter 3: Literature review
6.8 Restrict use of I-voting to Internet users within the country as making I-voting accessible worldwide will create many technical and security challenges. This will eliminate many attacks and more control would be gained. The possibility of committing fraud from distant locations, such as from a foreign country, is high in I-voting. For Qatari citizens abroad,	Chapter 5: Qatar

voting could be carried out in Qatar embassies using secure dedicated leased line network connections so that all data can be transferred securely.	
6.9 Provide an automated backup of systems, ensuring storage is in a safe place, and enabling reference to this backup when necessary, such as on discovery of security breaches.	Chapter 3: Literature review
6.10 Ensure all related agencies work together. This can be achieved through standardisation of the procedures required to integrate different internal processes. This will demand very clear prior definition of leadership and respective function.	Chapter 5: Qatar

11.3 Evaluation of Recommendations

To evaluate the recommendations, relevant senior officials were interviewed to review the recommendations. Interviewees were recruited by direct personal contact. Five evaluators were gathered from different organisations in Qatar from the Ministry of Interior (MOI), ictQATAR, Qtel and the Supreme Judiciary Council. The interviewees were as follows:

1. Hassan Al-Sayed, Gov. IT Platform Manager, ictQATAR
2. Abdul Rahman Al-Sulaiti, Assistant Director of Elections Department, MOI
3. Jassim Alswadi, Head of ISP, Qtel
4. Mohanad alabad, Internet Security Consultant, MOI
5. Mohamad Alobaidli, Judge participating in election monitoring, Supreme Judiciary Council (SJC)

The purpose of the interviews was explained and confidentiality was assured in writing. In addition, interviews were held in a semi-structured form, where each interviewee was interviewed individually for about 30 to 45 minutes and notes were taken by the researcher. The interviewees were first provided with the recommendations to read and then they were asked the following questions:

Q1. Do you believe the researcher's recommendations will be effective for introducing I-voting in Qatar?

Q2. After reading the recommendations, would you encourage Qatar to introduce I-voting?

Q3. Do you believe that the recommendations satisfy voting principles of security, privacy, transparency, etc.?

Q4. Do you think the recommendations could help to increase voting turnout?

Q5. Do you think the recommendations on the legal aspects are valuable?

Q6. Is Qatar ready to introduce I-voting in terms of its infrastructure? And, are the recommendations for enhancing infrastructure development adequate?

Commenting on I-voting, most of the interviewees acknowledged that some countries had attempted to adopt e-voting. The experts from the MOI and ictQATAR believed that a system of I-voting can be made fully reliable and authentic because these days many tasks are done through computers and people can fully rely on these systems. They added that the security agencies can take the help of suppliers of the online voting system for administering the votes authentically. As Avaliktos (2004, p.152) states, *"Safeguards can be provided through the establishment of computer security procedures that prevent unauthorized individuals from seeing the contents of a ballot."*

All evaluators believed the recommendations would be very effective for the government of Qatar in assisting in the uptake of I-voting. The experts from the MOI, ictQATAR and Qtel believed the recommendations are comprehensive, clear, consistent and well-structured. Moreover, the Internet Security Consultant and the Assistant Director of Elections Department believed that the recommendations were very valuable, relevant and well designed since they are based on grounded research in the field. Most commented on the importance of the research since it sheds light on a new technology which has not been introduced before in Qatar.

The majority of evaluators would encourage the introduction of I-voting since they believe it would enhance voting participation, provide accessibility and facilitate the voting process. However, they pointed out the security, privacy and trust issues raised from such system. On the other hand, the judge from SJC does not favour introducing I-voting in Qatar, believing that it is impractical, since people have used paper-based voting for a long time without problems and most would find difficulties in using the I-voting system. He added that worldwide experience of I-voting has shown many associated issues in terms of security, privacy and getting people's acceptance. Although he thought it is a good area of research, he warned that the government have to make a careful decision on introducing I-voting, making sure it would be an effective voting system for Qatar elections in the future, taking into considerations its possible impacts. Furthermore, the SJC expert felt there was a need to prove the effectiveness of the proposed I-voting model in ensuring its fulfilment of voting principles in practice and getting acceptance and the confidence of Qatari citizens.

While the majority of experts believed that most of the recommendations would satisfy voting principles including security, privacy and transparency, they however felt the recommendations needed to be put into practice to ensure they would work in the real world.

The expert from ictQATAR stated that I-voting is highly dependent on aspects like the political, social and economic situation of a state. I-voting will not actually have much effect on the operation of the political process or the distribution of power in advanced societies. Most of the experts agreed that it would be a good idea to introduce supervised I-voting in polling stations, so that Qataris could become familiar with using such new technology.

The MOI Internet Security Consultant expert suggested that the I-voting stations should not be configured, requiring each voter to open the application and type in the URL for security reasons. Although this would be too difficult and confusing for some users, the online tutorial would guide them in how to access the system or, alternatively, they could be provided with an easy step-by-step user manual. Most of the interviewees

commented that education and training should be recommended to build the citizens' acceptance and trust. They recommended having I-voting alongside paper-based voting, so citizens who are still not comfortable with I-voting could choose to vote at the polling stations. However, they believed the government should distribute information on how to use I-voting from home so they can follow all the security procedures to ensure securing the client-side machine. As in the Qatar e-government project (Hokomati), whenever there is a problem with one of the e-services in government, the user should be able to call the e-government team who should be able help to solve the problem. Similarly there should be an Incident and Response Team available 24 hours a day during the election period to assist voters in casting their votes by I-voting, without knowing who the user is going to vote for.

The Assistant Director of the Elections Department commented on the need for a trusted third party to inspect the I-voting process to ensure the fairness of system. This complies with the proposed model design (see Chapter 9) where the Election Committee act as a third party where it issues a secret key to each voter, this is used to ensure that the voting process has not been manipulated at any stage. In order to access the system there would be a need for more than one party to access it.

Moreover, he added that some countries such as the USA and the UK have not gone further in developing I-voting due to technical and non-technical issues and, therefore, it would be hard to gain political approval for using such system in Qatar with a risk of affecting citizens' confidence in the government. Also, some parties fear that I-voting would ignore the needs of some voters who have no knowledge of using the computer or the Internet.

The Assistant Director of Elections Department pointed out that I-voting could simplify the voting processing, for example the registration stage could be disregarded if the voter has an ID card and the voting process could be done straightforwardly with a few clicks. However, there are some political concerns on the security, anonymity and privacy of I-voting. On the other hand, the SJC and MOI evaluators believed that I-voting will boost the political agenda.

The MOI and ictQATAR experts stated that government should make an effort to make citizens knowledgeable about I-voting. Moreover, the experts commented, the public adoption of government electronic systems has been satisfactory in Qatar. This was confirmed in the literature by Shafi and Vishanth (2010) who state, *“The Qatari e-government initiative was launched in 2003. In global terms, the UN e-government readiness report (2008) ranked Qatar’s e-government project as number 53 worldwide.”* As in many countries, the national e-government focus in Qatar is to achieve the highest performance in executing governmental transactions electronically, through streamlined business processes and integrated Information Technology (IT) solutions (ictQATAR, 2009). The public organisations in Qatar have set themselves a target to commercialise their technologies with the new developments (Qatar Science & Technology Park, 2009). The advantage is that this implies there is a solid infrastructure available to introduce I-voting.

The experts from Qtel and ictQATAR emphasised the need to ensure that the I-voting system is connected to the election server to ensure a secure and trusted system. This agrees with Avi Rubin (2001) who stated, *“The infrastructure does exist right now for computer security specialists, who are suspicious that they could be communicating with an imposter, to verify that their browser is communicating with a valid election server.”*

The expert from ictQATAR stated that in order to make I-voting practical and widely adopted, it should come with proper hardware to facilitate a reliable connection between the user and the election server. Malevolent code to infiltrate the normal functioning of voting systems has to be strictly prevented.

Most evaluators believed that further trials should be held before adoption of I-voting, to measure the effectiveness of such a system in reality. Also, this will help to assess I-voting against other systems. Furthermore, the system should be tested to ensure it is equipped with the proper security measures to decrease possible hazards, and there should also be a comparative economic analysis of this system. Some experts suggested

the development of new procedures for continuous testing and certification of election systems and test methods for election systems, pointing to the need to consider usability in the design of I-voting. However, any certification of I-voting should be able to adapt to technology changes in the hardware, operating systems, browsers, plug-ins, crypto standards, authentication mechanisms and technology threats. Therefore it is hard to certify something that is always changing. In addition, some experts suggested the need to develop a protocol for preventing vote selling and reducing coercion.

11.4 Conclusion

The recommendations on I-voting presented in this chapter have included aspects concerning the digital divide, e-literacy, I-voting infrastructure, the law, transparency, security and privacy. These recommendations were derived from the research outcomes reported in previous chapters. They were judged to be valuable, according to a number of expert evaluators who, as a result, would encourage the introduction of I-voting in Qatar as they believed it would be feasible, if care was taken over issues such as security, privacy and people's acceptance. The evaluators believed that the proposed model and recommendations need to be implemented in reality to confirm their effectiveness, taking it from theory into real world practice. It is recommended that the government of Qatar should boost e-democracy by implementing the proposed I-voting model (see Chapter 9) in phases, alongside paper-based voting, starting with an experimental trial in specific places (e.g. universities, polling stations, and some organisations) to evaluate the success or failure of I-voting in Qatar and investigate the problems encountered to help in improving the system.

Apart from the Judge from the SJC, the evaluators were clear that an I-voting system should be introduced in Qatar. It is therefore recommended that the government of Qatar should make efforts to implement such an I-voting system, ensuring proper security of systems being used for the purpose, and educating the voting population of the advantages of the system and of the security and privacy measures being used to protect their vote.

Chapter 12 Conclusions and Future work

This chapter presents the contribution, implications, achievements and limitations of this research, along with the overall conclusion and proposed continuation work.

12.1 Research contributions

The research provides a significant contribution to knowledge by shedding light on improving a voting system by adopting I-voting in a particular area of the world which has not been covered before in the literature, the State of Qatar. The research contributes by identifying the willingness and barriers of government and citizens to adopting I-voting in Qatar and proposes a secure I-voting model for the Qatar government that address issues of I-voting which might arise due to the introduction of such new technology. It also makes recommendations to the Qatar government to assist the introduction of I-voting.

The research is valuable not only for the Qatar government but also for Qatari citizens and I-voting research scholars. The lessons learned from the Qatari case study could also be useful for other nations, if account is taken of the cultural and country-specific factors, especially those countries with a culture similar to Qatar's, such as the Gulf Co-operation Council (GCC) and Arab countries.

12.2 Research implications

This work was based on a variety of data gathering methods, including interviews, questionnaires and experiments to determine the possibility of introducing I-voting in Qatar, taking into account the possible barriers which might be faced and proposing an effective I-voting model, along with recommendations, to help the Qatar government to introduce I-voting.

This research has had many positive implications for the researcher in both personal and professional terms. It was an inspiring and knowledge enhancing experience which has

improved the researcher's knowledge professionally, academically and personally in many aspects: problem solving, communication skills, research skills, management skills and gaining experience and knowledge in the field of I-voting. This research will make a valuable input in the researcher's approach to professional work in the Ministry of Interior in Qatar in being responsible for improving the voting system in Qatar as part of the government's e-government initiative, ensuring the fulfilment of voting principles and the willingness of the Qatar government and citizens to introduce such an improvement.

12.3 Research achievements

The research aim and objectives (see Section 1.5) were achieved in this thesis through empirical and non-empirical research in the State of Qatar as a case study of introducing I-voting in this part of the world.

The research followed a carefully planned progression through the intended objectives which built on each other, towards finally fulfilling them by investigating the readiness of the Qatar government and willingness of citizens to take part in the initiative of I-voting. Also, it discovered the barriers that would deter I-voting in Qatar. Furthermore, it proposes an effective I-voting model for the state of Qatar, based on best practices and country-specific factors to overcome the investigated I-voting challenges. Finally, it proposes effective recommendations for Qatar government to help the introduction of I-voting.

12.4 Research limitations

This research faced many limitations in terms of resources, time and access. It was not possible to produce large-scale interviews, questionnaires and experiments, due to the limitation in resources and difficulties in obtaining authority for access and support from responsible organisations. Also, unwillingness of some respondents to contribute to the research by participating in interviews, surveys and experiments was a further constraint. Consequently, the researcher took advantage of personal contacts to gather the participants. Nevertheless, the researcher tried to take positive steps to encourage people to participate, for

instance by inspiring them by showing them the importance of their input to the research and ensuring their privacy and confidentiality.

It was not possible to introduce the proposed model and recommendations in reality due to difficulties in getting government acceptance to implement the proposed solution in the time available. However, the effectiveness of the proposals was tested by experts from a range of private and government organisations in the field of voting, information security, Qatar culture and the law. Furthermore, due to the lack of resources and access to organisations, as well as the time constraint, there was a limit to the extent that world-wide experience could be reviewed. However, it was possible to review the adoption and experiences of I-voting in Estonia which provided a good example for the uptake of I-voting in Qatar, although it would have been beneficial to proceed with more detailed comparison between Qatar and Estonia to investigate the similarities and differences between each country, considering country-specific, social and cultural aspects.

12.5 Conclusion

This thesis has aimed to assess the willingness of Qatari citizens to take part in the initiative of I-voting and identify the barriers that would inhibit I-voting in Qatar and the means to overcome them by proposing an effective Internet voting model for the State of Qatar to be used for future elections and make recommendations for the Qatari government to introduce and encourage I-voting.

The research presents a literature review of I-voting experience, identifying the willingness and barriers of such a system and best practice and models used in creating I-voting that fulfils voting principles. Based on the literature and interviews with representative experts and a sample of candidates and voting experts, it is concluded that I-voting is feasible with government readiness and willingness, due to multiple factors: voting experience, educational development, telecommunication development, the large number of Internet users, Qatar law which does not bar the use of I-voting, and Qatar culture which supports I-voting introduction. The interviewees considered the government willingness to provide I-voting for reasons of accessibility, availability of IT infrastructure, availability of Internet law to protect online consumers and the existence of the e-government project. However, most interviewees

pointed to the need for considering the possible barriers to introducing I-voting in Qatar needing to be resolved, such as ensuring security, privacy, usability and transparency. Therefore, a proposal was made for providing I-voting as an alternative method of voting alongside the current paper-based voting system to ensure the voting process fulfils voting principles.

A survey has assisted in discovering Qatari citizens' views on the barriers and willingness to participate in I-voting and the features they would like to have in I-voting. Most participants were comfortable with I-voting and were confident that their privacy and security would be ensured. In general, a high percentage of people indicated a preference for I-voting over traditional methods, especially for citizens abroad. The willingness to participate was considerably higher for people with high computer knowledge, high usage of e-services and those with a trust in general elections in Qatar. However, the surveys have highlighted some barriers to I-voting needing to be considered, including security, reliability and accuracy of I-voting, vote selling, difficulties with using the technology and preference for personal interaction. There was clearly a great deal of uncertainty by participants on whether to support I-voting or not, which suggests the need to see I-voting in reality in order to assess its acceptability. With regard to I-voting features, about half suggested the essential need for vote confirmation and verification to ensure voters have successfully cast their votes and to support a vote audit.

An experiment was made to assess Qatar's acceptance of I-voting, which involved developing a trial version of an I-voting system based on Qatar election requirements and taking into account the best practice of successful I-voting models. It benefited mainly from the I-voting experience in the Republic of Estonia which provided a reference to compare the results from the experiment. The experiment's participants were 86 Qatari citizens and two IT experts from Almajaz Telecommunication. The results showed a high user acceptance of I-voting in Qatar, and highlighted some improvements required in terms of the design of the system, the use of best practice to ensure the security and privacy aspects and consideration of the legal issues of I-voting. However, the experiment showed some concerns about I-voting security and the threat of manipulation by an unauthorised user mainly on the client-side where user awareness plays an important factor.

Therefore another survey was carried out to assess Qatari voters' awareness of information security. This survey showed the necessity for enhancing user awareness on information security to achieve an effective and secure I-voting system, mainly on the client-side. It discovered that users have a lack of awareness of information security and, therefore, take several incorrect actions which might put them at a security risk, such as reacting to fake security warnings, replying to suspicious links, using peer to peer software with people the user does not know and responding to unknown senders. The survey participants also confirmed that the use of different levels of authentication in I-voting to provide higher security was a good idea.

An effective model for I-voting appropriate for Qatar elections was then proposed, based on outcomes from the previous data collections. Opinions from a sample of voters and experts were used to evaluate the model. The model attempts to satisfy voting principles including security, privacy, transparency, accuracy and usability. The model introduced a secure platform for I-voting using the Linux operating system booted from a CD which uses the Qatari National ID to verify eligible voters, and PKI credentials within the smart card to ensure confidentiality and integrity, along with a unique digital certificate to enable secure interaction with the I-voting apparatus. The proposed model shows a good degree of acceptance by experts in terms of satisfying voting principles, although there is a need to consider possible cyber-attacks and risks associated with the client side which could be reduced by enhancing user awareness on security and using secure operating systems or Internet browsers.

A prototype of the proposed system was implemented with a WAMP server and evaluated by an expert. The expert was very interested in the system, and agreed that the system provided a secure client/server web architecture for a prototype, but he did not favour it for real practice, advising that the security could be improved with mix networking and smart card technology. The expert was also concerned about the scalability of the architecture for real elections, where a sufficient number of servers and advance technologies would have to be applied to meet the Qatar election requirements to provide an effective I-voting system.

Recommendations then emerged from the grounded theory based on the findings from the research carried out in the field. These were defined for the Qatar government to assist the introduction of I-voting in Qatar. They concern the aspects of I-voting of the digital divide, e-literacy, I-voting infrastructure, legal issues, transparency, security and privacy. Five experts in the field of IT, information security and the law, found the recommendations to be valuable. The recommendations were believed to provide an encouragement for governments on how to introduce I-voting, ensuring fulfilment of voting principles. The experts showed interest in introducing I-voting in Qatar to boost e-democracy and, apart from a Judge from the Supreme Judicial Council, have recommended that the government should introduce I-voting in general elections. However, those recommendations could be evaluated more effectively when the government of Qatar puts them into practice with an experimental trial of the proposed I-voting system; this would evaluate the success or failure of such new technology in Qatar.

12.6 Future work

This research has made a major contribution to the field of research. Although the research has successfully achieved its stated aim, there is still scope for further work as follows:

1. Confirming research outcomes

Due to the limitation of time and resources, the small number of participants contributing to this research has limited the certainty of the outcomes. Therefore, increasing participation in the interviews, questionnaire survey and experiments would obtain more reliable results and reduce the margin of error. This would increase confidence in the research outcome since it would be a better representative sample of the population.

2. Applying real trials

Although many I-voting schemes were proposed in the literature, a significant number of them rely on theory rather than real-world trials. Similarly, the researcher was unable to perform real world trials of I-voting in Qatar due to the limitation of resources and difficulties of getting approval from responsible personnel to conduct such research on a real election.

However, in this research, experiments were carried out to assess the proposed model under laboratory conditions. Nevertheless, applying real trials of the proposed I-voting model would be beneficial to test the model's applicability and effectiveness in practice and could be used to measure more effectively the willingness and barriers for I-voting in Qatar in real life.

3. Establishing a research team

This research could be used as a concrete start for further studies on I-voting in Qatar. Further work could be done by the government of Qatar to initiate a team of experts responsible for improving the voting system and further investigating the adoption of I-voting. The proposals and recommendations in this thesis could then become the basis for any further research that is carried out.

4. Investigating the cultural considerations of I-voting

The huge development in IT raises the question of whether Qatari people have fully absorbed this development and its associated threats. This also suggests the need to look at the cultural considerations which are also of interest, where customs, traditions and the Islamic religion form the Qatari culture in which Islam has a major influence on people's behaviour and responses in their daily life. The Qatari people are generally trustful, helpful and generous, which comes from their culture. This might lead to putting trust in malicious messages, making them more susceptible to security vulnerabilities on the client side of I-voting.

5. Providing appropriate legislation

Appropriate legislation to accommodate I-voting should be considered before the deployment of I-voting in Qatar. For example, some voting features would be beneficial to include in the voting system such as override voting and vote verification. However, there are some constraints on these features in terms of increasing vote selling. To eliminate vote selling issues, voters should be able to verify their vote without the system revealing knowledge of their choices. This needs further investigation by experts in law who would need to take into account the country-specific factors of Qatar.

6. Assessing applicability of the proposed solution in other countries

Although this research has focused on studying I-voting in Qatar as the main case study, it would be beneficial to further investigate I-voting experience in other countries to provide comparative results, learn from others and assess the applicability of the proposed solution. However, due to limitations of time and available resources, this has not been possible. However, advantage has been taken of the reported experience of I-voting in Estonia, which shares many of the same characteristics as Qatar.

12.7 Success of this PhD Research

Although this research is a first step in introducing I-voting in the State of Qatar, there is still scope for future work in extending investigations. However, the research has been very successful since the aims and objectives were achieved. Although there were some limitations, they were not serious and useful results have been obtained.

The research is original and introduces a valuable contribution to knowledge, particularly in relation to improving the voting process in Qatar. The greatest success of this research would be to get it into reality, where the proposed I-voting model and recommendations would be introduced in the succeeding municipal election as an alternative voting system to assess the willingness towards and acceptance of such new technology in practice. In this research, several councils and ministries of the Qatar government (e.g. central Municipal Council, Supreme Council for Communications and Information Technology (ictQatar), the Ministry of Interior and the Ministry of Foreign Affairs) have shown interest in promoting I-voting in Qatar as an improvement in the current voting system. They appreciate its advantages in terms of accessibility and convenience, and recognise the need to assess the effectiveness of the proposed I-voting model in ensuring conformance to voting principles. As a result, the researcher has prepared a business case for the Ministry of Interior upon their request (see Appendix F) to support their decision to introduce I-voting and to further explore the Estonia case study to learn from its successful experience in I-voting.

Appendix A Interviews

A1 Consent Forms

CERTIFICATION BY PARTICIPANT

I, certify that I am voluntarily giving my consent to provide information for the above described project entitled: **Introduce I-voting in the State of Qatar**, being conducted at Loughborough University, UK by: Mr. Jassim AL-Hamar.

I certify that I have agreed to be interviewed in the subject of as previously explained by Mr. Jassim AL-Hamar and that that I freely consent to participate in this project. I have had the opportunity to have any questions answered, I have been fully explained the procedures of interview and that information gathered will be only used for the benefit of the entitled research and will be confidential and kept strictly private.

Signed:

Date:

For any queries about the research topic please don't hesitate to contact the researcher (Name: Mr. Jassim AL-Hamar, ph. +974 55558105, E-mail: j.alhamar@hotmail.com).

A2 Example of signed consent Forms

CERTIFICATION BY PARTICIPANT

I, certify that I am voluntarily giving my consent to provide information for the above described project entitled: **Introduce I-voting in the State of Qatar**, being conducted at Loughborough University, UK by: Mr. Jassim AL-Hamar.

I certify that I have agreed to be interviewed in the subject of as previously explained by Mr. Jassim AL-Hamar and that that I freely consent to participate in this project. I have had the opportunity to have any questions answered, I have been fully explained the procedures of interview and that information gathered will be only used for the benefit of the entitled research and will be confidential and kept strictly private.

Signed: 

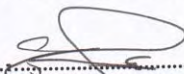
Date: 20/12/2009

For any queries about the research topic please don't hesitate to contact the researcher
(Name: Mr. Jassim AL-Hamar, ph. +97455558105, E-mail: j.alhamar@hotmail.com).

CERTIFICATION BY PARTICIPANT

I, certify that I am voluntarily giving my consent to provide information for the above described project entitled: **Introduce I-voting in the State of Qatar**, being conducted at Loughborough University, UK by: Mr. Jassim AL-Hamar.

I certify that I have agreed to be interviewed in the subject of as previously explained by Mr. Jassim AL-Hamar and that that I freely consent to participate in this project. I have had the opportunity to have any questions answered, I have been fully explained the procedures of interview and that information gathered will be only used for the benefit of the entitled research and will be confidential and kept strictly private.

Signed: 

Date: 21/12/2009

For any queries about the research topic please don't hesitate to contact the researcher
(Name: Mr. Jassim AL-Hamar, ph. +97455558105, E-mail: j.alhamar@hotmail.com).

A3 Interview questions

The seven representative experts interviewed were as follows:

1. Head of IT department, Ministry of Foreign Affairs (MOFA)
2. Manager of Patient Care department, Ministry of Health (MOH)
3. Head of IT, Ministry of Interior (MOI)
4. Manager of e-services, IBQ Bank (IBQ Bank)
5. Head of ISP, Q-Tel (Q-Tel)
6. Manager of Incident Management, Supreme Council of Information and Communication Technology (ictQATAR)
7. Head of Prosecution, Supreme Judiciary Council (SJC)
8. A random sample of 4 candidates from the 2007 election and 6 voters, from different backgrounds

They were asked questions on the following 10 topics, according to their level knowledge and level of expertise:

1. The feasibility of I-voting in Qatar
2. Election procedure with or without I-voting
3. Willingness to participate in and barriers to I-voting
4. Government opinion and readiness
5. Legislation and laws regarding the e-project (I-voting)
6. The ability of the IT Infrastructure in Qatar to adopt I-voting
7. Political opinions on introducing I-voting that can contrast voting system
8. I-voting implications of security, privacy, accessibility, vote selling and the digital divide and the research recommendations to overcome those problems
9. Increased turnout of voters.
10. The results of the survey conducted earlier in this research

A4 Examples of interviews

Interview 1

Date of interview: 11-Aug-2009

Duration: Approximately 30 minutes

Interviewee: Tariq Al-Othman, Head of IT department, Ministry of Foreign Affairs (MOFA)

Q1: How do the abroad Qatari voters vote? Do they vote through the embassy?

Currently they can vote through the embassy of Qatar where Qatari citizens comes to the embassy and we provide them with voting box to vote to their preferred candidates safely and securely. Then we send it through diplomatic bag into Qatar.

Q2: In case there is no embassy in the country what would be the solution?

At the moment no recorder incidence, however Qatar do incorporate with some other countries to perform some of the Qatari embassy duties.

For example in kazakhstan there no Qatari embassy but we do incorporate with Oman embassy. If the Question is about what extend at the moment I don't have answer regarding this.

Q3: Does running the election in the embassy would meet all voting principles (e.g. security)?

Yes, Qatar embassy would provide safe election environment even though it's abroad. Every embassy has very secure system for sending and receiving document, however Qatar is

Q4: Lately some countries and global institutions use I-voting (e.g. FIFA), would you consider an I-voting as an option for abroad Qatari voters?

Indeed, Qatar is fast growing country in term of technology, of course it would be looking forward to have such system, but from my understanding the I-voting project still facing problem to provide free error election. I- voting would be a superior option for abroad Qatari voters where they can vote remotely and securely through the internet.

Q5: Ministry of Foreign Affairs is currently developing a project to implement a secure communication between embassies and Qatar, such project make internet voting more feasible in terms of security?

Yes it is, currently the ministry is working on developing a secure communication between Qatar embassies. All the information is encrypted and transferred into a MPLS line or either satellite communication towards covering all embassies around the world.

In addition, all communications are monitored and controlled in the ministry of foreign affairs in Qatar. This implies that I-voting through embassies would ensure reliable and secure I-voting.

Q6: Qatar have experienced a huge development in economy, technology, telecommunication, education and other sectors, as a result would this support the introduction of Internet voting?

Yes of course, this huge shift in the country might make I-voting feasible and acceptable especially that Qatar aim to lead the development in technology in the region.

Q7: What are the major barriers faced or expected to be faced in the uptake of I-voting in Qatar?

There might be a problem on getting people's acceptance on such technology with paying intention to the security and privacy issues especially with the huge possibilities of threat available nowadays. In political point of view, it will affect on measuring voting practice were a lot won't go to polling stations to vote. Basically, the country and people will miss voting experience including media coverage of voting practice.

Interview 2

Date of interview: 17-Aug-2009

Duration: Approximately 20 minutes

Interviewee: Ahmed Ali, Manager of Patient Care department, Ministry of Health (MOH)

Q1: What are the average numbers of Qatari patient in hospital?

Well, there no excite number it's hard to determine Qatari number, however Qatar have two main hospital Hamad and alkor with 1000 bed capacity and there is five main private hospital with capacity of 500 bed, currently ministry of health are in process to expand this number to reach 5000 bed.

Q2: How patient participate in election while he is hospital?

At the moment, the hospital can arrange it upon patient request, Simply the judge will come to collect the votes

Q3: Is internet connection are available in hospital?

Yes , it's available for the staff and with small cost for the patient, however there is telephone point at each patient room therefore they can connect at the internet using dial-up 'Ebhair'

Q4: Lately some countries and global institutions use I-voting (e.g. FIFA), would you consider an I-voting as an option for patients and staff?

Well I'm not expert of the field but my personal openion that internet voting might solve some problem but it will also introduce other the question now is going to be secure like traditional voting

Q5: What are the major barriers faced or expected to be faced in the uptake of I-voting in Qatar?

I believe that older people would experience really problem with dealing with computer, in the other hand, new generation would welcome such system. Therefore, they need to involve in training sessions on how to use such system successfully and securely.

Interview 3

Date of interview: 4-Aug-2009

Duration: Approximately one hour

Interviewee: Abdulla Al-Noaimy, Head of IT, Ministry of Interior (MOI)

Q1: What are the roles of MOI in e-government project?

MOI hold the responsibility belongs to their services such as traffic violation payment. About 15 out of 64 is responsible for MOI. Our responsibility is integration, back end support and sharing population database.

Q2: Is there a plan any plan for e-democracy?

Yes there is currently a plan for e-voting by kioks but we have not run not because of technical issues but because of political issues.

Q3: Lately some countries and global institutions use I-voting (e.g. FIFA), is it possible to have I-voting in Qatar? and why?

I think it is possible but not at the mean time, may be in the future were people would be capable to use such technology.

Q4: Do you suggest using e-government infrastructure as a base for e-democracy (I-voting)?

Yes indeed actually e-democracy is part of e-government initiative. MOI have a plan for e-voting using kioks machine. For i-voting it would be even more utilizing e-government infrastructure since it could work at the same platform.

Q5: How do you suggest I-voting could be implemented in Qatar with ensuring voting principle are fulfilled (e.g. security, transparency)?

Regarding the security technically it can be implemented with acceptable percentage of error. However, political, law and transparency still remain as barriers to implement such system. However, currently Q-CERT with MOI have developed n e-law from best of practice and own country rules but it has not yet been approved by the government. Regarding transparency, Qatari government has developed strong relationships with its citizens there is a coherent trust on the government. As a political there is a fear of failure such system which might consequence negatively on government trust.

Q6: What are the difficulties might be encountered with I-voting (cost, resources, people acceptance, security issues, missing voting experience)?

I do agree on the factors you've mentioned. I think the main difficulties we might face are people acceptance to I-voting and missing voting experience. Also it is important to ensure the reliability and security of such system. However, MOI has a strong profile in developing such critical system, for example e-gate, e-passport and e-government.

Q7: What do you think I-voting could add compared to the current voting system?

Currently Qatar is using paper ballot system for voting, introducing Internet voting as an option would increase the voting participant and would add new channel to vote. There are many people who are not participating because of the long line or because there work

Q8: Is it worth introducing I-voting? And why?

Yes, it's worth if we can provide I-voting without violating voting principle, however in my opinion Qatar is capable of doing such system due to the political willingness and technical capability and most important the absent of strong law for election this would help that any future law would take in consideration I-voting requirements

Q9: Do you think people would accept I-voting?

I think Qatar is taking huge step to improve the education and to make computer lectures as priority for example all school have Computer subject at different level also most employee in the country are asked to join computer courses, this would show that majority would have no problem dealing with I-

voting the only remaining people is the older people who unable or refusing to change. However this won't be big issues for I-voting since it's introduced as an option. It is better to carry out i-voting as an experiment to measure people's acceptance. I think old people and people with low computer literacy might find difficulties on using i-voting. However, the government is working on enhancing computer literacy through schools and jobs by carrying out ICDEL and computer courses.

Q10: Do you think I-voting will increase the participation level?

Well yes, many people now a days interested in performing tasks online rather than physically doing it.

Q11: MOI Provide e-services to citizen using smart card and biometric, How and why and success and failure?

Overall, it record 99% success and there was just one incident that one of the passenger using e-gate service had burn with his finger but we are here in Qatar recording all 10 finger and having all the scenarios into consideration. Using smart card and finger print provide vary secure authentication

Q12: Is it possible to use Smart card and biometric in internet voting?

Technically yes, for example e-government using smart card and e-gate using smart card and finger print what work for those system should work for other and what is most important is that I-voting is part of e-government

Q13: Some of the countries recognise Digital signature as the person signature, how about Qatar?

Yes, with the e-government we are using Digital signature as the person signature.

Q14: E-government Project attract make hackers to attack their service, Is MOI capable to secure such system.

So far e-government website had never been dawn because of attacker, yes we are receiving many attacks from different countries, however all team in Qatar Q-cert and ICT and MOI and Qtel are taking part to prevent and eliminate the attacks

Q15: What are the challenges and opportunity to introduce I-voting

People acceptance and Vote selling are the main challenges. The main Opportunities for I-voting are Government willingness and E-government project infrastructure.

Q16: What are the number of eligible voters

At the moment I don't have the eligible voter number since there are many conditions to be valid voter

Q17: What is the number of Smart card holder

At the moment about 120,000 card has been printed which almost 55% percent of the population, however the number are increasing by 100 card per day

Q18: What are the major barriers faced or expected to be faced in the uptake of I-voting in Qatar?

People acceptance and ability to vote successfully and securely using such system especially that there is a large portion of Qatari voters have low computer literacy. Although ipark will facilitate the process of internet voting but still it is not accessible to all people and some might not have computers or even the knowledge to use such system. Also verification of voting and ensuring security, transparency and privacy are top barriers. Moreover, accessibility and usability have to be assured.

Q19: It is predictable that fear and trust issues occur with any e-solution. How do you plan to cope with this challenge?

We have taken into account to these issues; we have built our trust on our sold reputation. Also we have involved the society in evaluation the system and to measure the effectiveness and people's acceptance.

Q20: Do you find any difficulties with the current voting system (e.g. accessibility especially for disable people)?

There is sort of accessibility, but still disable people who wish to vote have to come to the polling station and then we can then help them and take their votes and register it by a trusted person such as a judge. However, we have face a difficulty before with deaf legable voter who come to vote but we were not able to understand him through sign language. Therefore, I think the current system is not accessible especially to disable people, I recommend to have in each polling station a person who can deal with people of special needs and assist them in their votes. Also in case of disable people who can't come to polling station they have to be assisted and went to their homes and take their votes if they wish to.

Q21: Do you think some of these difficulties in the current voting could be resolved with adapting the technology (i.e. I-voting) were for examples accessibility and automate counting for voting is available in I-voting?

Yes, I think so it will make voting more accessible especially for disable people who are not able to come to polling stations. However, i-voting I think would be an optional voting system along with the traditional paper based voting. But then

comes the issues of integrating the votes and ensure that there are no redundant votes. I-voting would facilitate voting process for use were votes are counted automatically so this will avoid human errors and reduce the time and effort spent on counting votes.

Q22: How much would it cost to setup and run an election in Qatar?

I'm not certainly sure; however, cost is not the main concern for the governments, we are rich country and would like to invest in all sectors especially the democracy. The country does not think of the cost as a main factor, so even if i-voting is less cost than traditional voting system the government might still not accept i-voting if it does not fulfill voting fundamentals.

Q23: Past election records shows a low participation, could you indicate the reasons? And do you think I-voting could increase participation level?

Voting in Qatar is fairly new; it is now in its third revenue that may be why there was low participation. But in the future voters will get use to voting experience. The country has work on motivating voters to vote and practice their right on democracy through media and some activities. I think i-voting will increase participant level especially for people who are not able to go to polling stations and wait for long times in queues were then voters especially disable people can vote flexibly from anywhere and at any time through fast and easy system.

Q24: Do you think I-voting could be feasible in Qatar? Why?

Yes, but we have to ensure people's acceptance and that such system would fulfill all voting fundamentals. Therefore, if it would be approved by the government then it would be used as an alternative way of voting along with polling stations. Before that we have to perform a study on i-voting and look at other experience on i-voting and then perform a feasibility study with looking at the country specific factors. I can't judge on its feasibility it is subject to a lot of factors.

Q25: Does the Qatar law permit I-voting to be introduced as an option of voting?

I'm not in the position to verify this; you can refer to experts in the law. But as far as I know there is nothing says that i-voting is not allowed if it approved that it fulfill all of voting fundamentals then why not it could be applied, but I still think it could be applied as an experiment for while to assess its effectiveness a long with traditional voting system towards assess as well people acceptance and get use to it.

Interview 4

Date of interview: 14-Aug-2009

Duration: Approximately 25 minutes

Interviewee: Abdulla Al-Malki, Head of Prosecution, Supreme Judiciary Council (SJC)

Q1: Does Qatar law permit I-voting to be introduced as an option of voting?

The law does not prevent the technology of e-voting or i-voting. The law states the need for practicing voting through a system that fulfills all of voting fundamentals such as security, privacy and transparency.

Q2: Does the Qatar law have an e-law?

Currently, e-law is in the way of approval. The law involves all topics associated to electronic communications. It is developed by ICT Qatar and in cooperation with other related institutes including us and ministry of interior. The law will protect online consumers' right.

Q3: Do you allow voter to have a receipt to verify their vote casting? And why?

With regard to verification, the law does not allow it for voting because it may be used for vote selling. Although it is required to ensure that voters have vote successfully, but because of that risk the law avoid it.

Q4: Does Qatar law permit override voting?

Override is complex feature, the current law does not allow it because it could be used for vote selling as well were voters might change their vote several times for the purpose to sell it to different candidates. The voter have got only one choice and once to choose their preferred candidate. Although some might say override is a valid option especially for people who might be intimidated and forced to vote to specific candidate. However, this is difficult to be approved and therefore we still believe overriding is not a valid option.

Q5: Does Qatar law permit open source voting system or not? And why?

We does not allow open source to public to avoid voting been used by malicious people who wish to hack into system and manipulate voting results.

Q6: Some scientist claims that i-voting could cause Digital divide, how do this could be resolved?

It could be resolved by carrying out training sessions and holding awareness for public on how to use i-voting through effective method of education and learning principle through different tools e.g. seminars, media, video.etc.

Q7: What are the major barriers faced or expected to be faced in the uptake of I-voting in Qatar?

Ensuring security is an issue especially with the possible huge threats available in the internet. In addition, people acceptance and the usability are main issues. Still government approval on such system and ensuring trust on the system is essential to achieve successful system. Also since the technology is new, we expect that voters and candidates might not accept and trust such technology and therefore might distrust the result of votes.

Q8: Have you discuss e-voting to be option for voting in Qatar? And why

No, we have not discuss i-voting, but we've examine the implementation of e-voting as an option using kiosk, but it has been paused because of the need for more research carried out on kiosk technology and the need for approvals.

Interview 5

Date of interview: 27-Aug-2009

Duration: Approximately 15 minutes

Interviewee: Rashid Al-ali, Head of ISP, Q-Tel (Q-Tel)

Q1: Lately some countries and global institutions use I-voting (e.g. FIFA), is it possible to have I-voting in Qatar? and why?

Yes, it is possible, Qatar is always leading in the technology revolution and applying such technology in voting system will be interesting and effective with concerning its issues and how to avoid it.

Q2: What are the difficulties might be encountered with I-voting (cost, resources, people acceptance, security issues, missing voting experience)?

Security, privacy, transparency, gaining people acceptance and trust and missing voting experience all are the top issues might be encountered with i-voting. Therefore, the government have to plan for those issues to ensure effective voting system that fulfill the voting fundamentals

Q3: Is it worth introducing I-voting? And why?

This is hard to measure, I can guess that it is worth but we have to consider the security issues and getting people acceptance since this might affect on trust of voting results. In terms of cost, i-voting will save effort, time and staff working in process voting.

Q4: Do you think people would accept I-voting?

Yes I do if they have trust on the system and they find it usable then they would accept it with no problems. However, this would take time, i-voting could be started as an alternative and optional voting system as a trial to measure its effectiveness.

Q5: Do you think I-voting will increase the participation level?

It might be, this could only been know if it was implemented in reality. In some countries i-voting was successful and have increased participant level and others not, each country have its own special factors which might differ in the successful of i-voting system.

Q6: What are the major barriers faced or expected to be faced in the uptake of I-voting in Qatar?

As I've mentioned earlier security, missing voting experience, people acceptance and trust on i-voting are main difficulties might face with i-voting technology.

Q7: It is predictable that fear and trust issues occur with any e-solution. How do you plan to cope with this challenge?

This could be resolved by assuring an effective and secure system were then will be no fears of using i-voting and trust will be built then gradually. These could be assured practically when voter interact with the system.

Interview 6

Date of interview: 6-Aug-2009

Duration: Approximately 10 minutes

Interviewee: Fahad AL-Abdullah, Manager of e-services, IBQ Bank (IBQ Bank)

Q1: The bank provides I-banking service, how secure is this technology?

It is very secure; we applied a lot of security measures that is approved internationally in banks towards ensuring a very secure system. We also aware customers on how to use such system as well as how to ensure their security to avoid possible threats which intend to miss use their accounts.

Q2: Do you think the current security applied in I-banking could be implemented in I-voting to achieve a secure voting?

Yes, I think so. I-park has approved its security and people accept it and trust it so I think using such technology on i-voting would be effective.

Q3: What is the number of I-Banking users and are they increasing?

They are a lot, about 70% of the customers use i-banking and it is increasing because it approve its security and effectiveness in processing services online, faster and easier.

Q4: It is predictable that fear and trust issues occur with any e-solution. How do you plan to cope with this challenge?

Yes, we have tried to build people's trust on e-solution and this was based on awareness we provide on the benefit and effectiveness of e-solution. Also the trust was built by ensuring a secure and effective e-solution.

Interview 7

Date of interview: 20-Aug-2009

Duration: Approximately 20 minutes

Interviewee: **A Voter**

Q1: What are the difficulties might be encountered with I-voting (cost, resources, people acceptance, security issues, missing voting experience)?

I agreed with you, people acceptance, usability, security, privacy issues and missing voting experience are the main difficulties might be faced in i-voting.

Q2: What do you think I-voting could add compared to the current voting system?

It will add accessibility especially for voters who can't come to polling stations where they can vote online at anytime. Also it facilitate effort of voting committee since votes are counted automatically through the website and this might reduce human errors and save time and effort required for counting votes. However, there is possibility as well for hackers to hack the i-voting and manipulate results.

Q3: Do you find any difficulties with the current voting system (e.g. accessibility especially for disable people)?

The main difficulty is the time and effort spent in verifying voters, collecting, counting votes manually. Also, there is a problem of accessibility especially for old and disable people to reach polling stations and cast their votes.

Q4: Could i-voting be feasible?

Yes, it could be in the future but not know because people have to be ready for such technology and have to accept it. Also the issues associated with i-voting have to be resolved especially security, privacy and usability. There is also a issue of missing voting experience which have to be taken into account, therefore we think i-voting could be applied as an alternative option of voting along with traditional voting system.

Q5: Do you think people would accept I-voting? Why?

It is hard to measure this, I think having i-voting as an experiment would give an estimation of people acceptance.

Q6: Do you think I-voting will increase the participation level?

It might be for people who find difficulties to come to polling stations, however this could be estimated if i-voting were applied as an experiment along with traditional voting.

Appendix B: Questionnaires

B1 Questionnaire 1: Exploring I-voting acceptance in Qatar

B1.1 First version of questionnaire

1. What age group are you in?

- 18-25 26-35 36-45 45-60 over 60

2. Gender

- Male
- Female

3. Level of education

School Further or Higher Education Post Graduate Others

4. Your computer knowledge

- Novice Average Advanced Expert

5. How well do you know about eVoting

None Poor Average Good Expert

6. Do you think that voting in Qatar is held democratically?

Definitely probably probably not definitely not don't know

7. What is the best way to cast the vote through e-voting?

- By using Website
- By using touch-screen
- By using buttons around the screen (like in the ATM)
- Other

8. What way of voting is the most suitable for you?

- Paper-based voting Electronic voting

9. Do you think there is a need of implementing e-voting system in Qatar?

Definitely probably probably not definitely not don't know

10. If you do not believe there should be electronic voting in Qatar, please state why:

- The technology would be too difficult for some people to use.
- The technology may not be reliable.
- A computer hacker may be able to affect the results
- There would be no easy check that the results are correct and have not been manipulated.
- Other, please specify:

11. Do you think paper base elections may be easily cheated or miscounted

12. Is Political parties influence voting results by appointing their members as staff on the polling booth

13. Does the Government can affect results of the voting by manipulating votes

14. Evoting is more accurate.

15. Evoting increase the potential for fraud

16. Evoting is prone to unintentional failures.

17. In your opinion which of the following authentication is the most appropriate for e-voting?

Login and Password

Scratch-codes

Issued certificates to access government's system

Digital signature

Biometrical access (thumb-scans, eye-scans)

Other, please specify:

Don't know

18. Who in your opinion should have access to the voting Database to retrieve the results?

Election commission

Judiciary

Military

Immigration (id-card issuing department)

Other, please specify:

19. Who should develop the machines of evoting?

Local companies

Government bodies

Foreign companies

Other, please specify:.....

20. Regarding the Qatari citizens who are abroad, how do you think they should vote?

Going to Qatar embassy

Through the website

Phone

Others, please specify.....

B1.2 Questionnaire after first review

Section 1 – Background

1.1 What is your age?

18 – 24	25 – 29	30 – 39	50 – 59	60 – 64	65+
---------	---------	---------	---------	---------	-----

1.2 What is your gender?

Male	Female
------	--------

1.3 Which Level of education are you currently studying?

School	College	University	Postgraduate	Others
--------	---------	------------	--------------	--------

1.4 Self rating of computing knowledge?
--

Absolute beginner	Some knowledge	Average knowledge	Pretty knowledgeable	Expert
-------------------	----------------	-------------------	----------------------	--------

Section 2 – Use of the Online Banking

2.1 On average, how often do you use the internet for Online banking or making online purchases?

Once a week or more	2-4 times a month	Once a month	Less than once a month	Not at all
---------------------	-------------------	--------------	------------------------	------------

2.2 Why don't you use the internet for online banking or making online purchases more often? What are your reasons? <i>(Please fill all that apply)</i>
--

Don't think it is very safe/ secure	Things restricting internet use	No need for it	Prefer personal interaction	Unsure
-------------------------------------	---------------------------------	----------------	-----------------------------	--------

[Asked of those who use online banking or make online purchases less than once a month:]

Section 3 –Confidence in management and accuracy of general elections

3.1 Rate how confident are you that general elections in Qatar are managed fairly and that vote counting is accurate.

← Not Confident

Mid-Range

Very Confident →

(0 – 3)

(4 – 6)

(7 – 10)

3.2 Regarding abroad citizens, how do you think they should vote?

Going to Qatar
embassy

Through the website

Phone

Others

Section 4 – Online Voting

4.1 How strongly do you agree or disagree with the following statements about online voting in Qatar general elections, assuming that it would use security systems similar to internet banking and reputable online retailers?

Rate the following:

← **Strongly
Agree**

Mid-Range

Strongly

(4 – 6)

Disagree →

(0 – 3)

(7 – 10)

4.1.1 - I would choose to vote online instead of visiting a polling place

4.1.2 - I would be comfortable with voting online

4.1.3 - I would be confident that I could vote online without anyone seeing who I was voting for

4.1.4 - I would be confident that I could vote online without anyone else unduly influencing my vote

4.1.5 - I would be confident that vote online is more accurate

4.2 If you were to vote online, would you regard the following security features as essential, nice to have or not important?

	Essential	Nice to have	Not important	Unsure
A screen which would ask you to confirm who you were voting for before it was made final.				
Being able to revisit the voting website to confirm that your vote has been received but not who you have voted for.				
Being able to request confirmation using a different means of communication, such as text				
Other, please specify:				

4.3 If you do not believe there should be Online voting in Qatar, please state why:

The technology would be too difficult for some people to use.	<input type="checkbox"/>
The technology may not be reliable.	<input type="checkbox"/>
There would be no easy check that the results are correct and have not been manipulated.	<input type="checkbox"/>
A computer hacker may be able to affect the results	<input type="checkbox"/>
Vote selling	<input type="checkbox"/>
Other, please specify:	

B1.3 Questionnaire final version (after pilot-test)

Covering letter

Dear Fellow Citizen,

I am a PhD student at Loughborough University in the UK and I am doing my research on “Internet Voting” which is part of e-democracy project that make use of IT infrastructure to introduce easy way to perform election.

I have designed a questionnaire to examine people acceptance and concern about Internet voting and how to defend against it challenges. This questionnaire is intended only for Qatari. Therefore, if you are Qatari above 18, please help us by completing the questionnaire, otherwise just ignore it. It is important that participants answer the questionnaire honestly.

The questionnaire will take no more than 2 minutes of your time to complete. I hope you will contribute. It is intended to use the results in developing secure Internet voting to be used in future election, so the people can benefit from voting anytime any where in there convenient.

Please bear in mind that participants should be only Qatari citizens above 18. I assure you that all responses will be confidential and kept private.

Thank you in anticipation of your involvement.

Yours sincerely,

Jassim Al-Hamar

For any questions about the research topic please do not hesitate to contact me by e-mail: j.alhamar@hotmail.com.

Internet Voting Survey

Section 1 – Background

1.1 What is your age?

18 – 24

25 – 29

30 – 39

50 – 59

60 – 64

65+

1.2 What is your gender?

Male

Female

1.3 Which Level of education are you currently studying?

School

College

University

Postgraduate

Others

1.4 Self rating of computing knowledge?

Absolute
beginnerSome
knowledgeAverage
knowledgePretty
knowledgeable

Expert

Section 2 – Use of the Online Banking

2.1 On average, how often do you use the internet for Online banking or making online purchases?

Once a week or
more2-4 times a
month

Once a month

Less than once
a month

Not at all

2.2 Why don't you use the internet for online banking or making online purchases more often? What are your reasons? *(Please fill all that apply)*

Don't think it is
very safe/ secureThings restricting
internet use

No need for it

Prefer personal
interaction

Unsure

[Asked of those who use online banking or make online purchases less than once a month:]

Section 3 –Confidence in management and accuracy of general elections

3.1 Rate how confident are you that general elections in Qatar are managed fairly and that vote counting is accurate.

← Not Confident

Mid-Range

Very Confident →

(0 – 3)

(4 – 6)

(7 – 10)

3.2 Regarding abroad citizens, how do you think they should vote?

Going to Qatar
embassy

Through the website

Phone

Others

Section 4 – Online Voting

4.1 How strongly do you agree or disagree with the following statements about online voting in Qatar general elections, assuming that it would use security systems similar to internet banking and reputable online retailers?

Rate the following:← **Strongly
Agree****Mid-Range****Strongly**

(4 – 6)

Disagree →

(0 – 3)

(7 – 10)

4.1.1 - I would choose to vote online instead of visiting a polling place

4.1.2 - I would be comfortable with voting online

4.1.3 - I would be confident that I could vote online without anyone seeing who I was voting for

4.1.4 - I would be confident that I could vote online without anyone else unduly influencing my vote

4.1.5 - I would be confident that vote online is more accurate

4.2 If you were to vote online, would you regard the following security features as essential, nice to have or not important?

	Essential	Nice to have	Not important	Unsure
A screen which would ask you to confirm who you were voting for before it was made final.				
Being able to revisit the voting website to confirm that your vote has been received but not who you have voted for.				
Being able to request confirmation using a different means of communication, such as text				
Other, please specify:				

4.3 If you do not believe there should be Online voting in Qatar, please state why:

The technology would be too difficult for some people to use.	<input type="checkbox"/>
The technology may not be reliable.	<input type="checkbox"/>
There would be no easy check that the results are correct and have not been manipulated.	<input type="checkbox"/>
A computer hacker may be able to affect the results	<input type="checkbox"/>
Vote selling	<input type="checkbox"/>
Other, please specify:	

B1.4 Electronic version of questionnaire

Dear All,

I'm writing this email regarding distributing the survey (Online Voting in qatar) among qatari citizen, currently I'm second year PhD student at loughborough university. The purpose of this survey is to obtain your opinions about Online voting.

Please click on the link below (or type the address into your browser), fill in your answers to the 11 questions, and submit them electronically by **30 April 2009**. When you are responding, think of your country as it is today.

It is important that you respond openly and honestly to the survey for accurate results. Your responses are completely confidential and will only be presented as part of the overall research profile or subgroup.

English

<http://www.questionpro.com/akira/TakeSurvey?id=1200782>

Arabic

<http://www.questionpro.com/akira/TakeSurvey?id=1201420>

B1.5 Questionnaire participants

4000 thousand of hard copy were distributed among participants institutions In Qatar, 2,567 Qatari e-mail users over 12 participated in the questionnaire survey, as follows:

- Carnegie Mellon University
- Commercial Bank of Qatar
- Doha Bank
- Friends and relatives
- Georgetown University
- ICT Qatar
- International Bank of Qatar (IBQ)
- Ministry of Defence
- Ministry of Economy & Commerce
- Ministry of Foreign Affairs
- Ministry of Education
- Ministry of Interior
- Ministry of Municipal and Agriculture Affairs
- Qatar Foundation
- Qatar Petroleum (QP)
- Qatar Telecommunication (Qtel)
- Ras Gas
- College of the North Atlantic (CAN)
- University of Qatar

B1.6 Questionnaire support

Hello Jassim,

I just wanted to let you know that Dr. Hal Jorch , the President of CNAQ has now received approval from Dr. Latifa Al-Houty, the Vice Chair, Executive Committee, (in other words the Representative of the State of Qatar) that you can send your questionnaire to our students at CNAQ.

We can send out your message, which would contain the link to your survey, by email to all students. We would not be using the instructors, and not use paper questionnaires, just an email and the students can reply to you directly .

If you send me the message and the instructions of how the students can either contact you to get the survey, or otherwise have the survey link embedded in your message, I can send then send it to the students. I can also assist you by sending a reminder a week or so later to remind them and encourage them to complete the questionnaire.

I understand this was a frustrating experience for you, but we have a certain protocol that we are expected to follow in order to obtain approval from the State.

I thank you for our patience and your understanding



Gerlinde Sarkar
Director, Research & Planning
College of the North Atlantic - Qatar
Building 3, Room 3.2.43
tel: + 974 495-2045

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Ministry of Interior
Human Resources Department



وَدَارَةُ الْإِذَاجِدِيَّةِ
لِإِدَارَةِ الْمَوَارِدِ الْبَشَرِيَّةِ
قسم التدريب والبعثات

التاريخ: ٢٠١٤/٠٤/٠٣

الرقم: د.إ.م.ب.ق.ب.م.ش.ض. / ٢٣١٤ / ٨٦٦

الموافق: ٢٠١٤/٠٣/٣٠

إلى من يهمه الأمر

تشهد وزارة الداخلية بأن الملازم رقم: ٢٣١٤ جاسم خالد جاسم محمد الحمير أحد منتسبي الوزارة ومبتعث حالياً للدراسة بجامعة (Loughborough) بالمملكة المتحدة للحصول على درجة الدكتوراه في مجال الحكومة الإلكترونية إعتباراً من تاريخ ٢٠٠٨/٢/٥ م ولمدة (٣) سنوات، ويقوم حالياً بإعداد استبيان في مجال دراسته، آمليين تفضلكم بتسهيل مهمته.

أعطيت له هذه الشهادة بناءً على طلبه دون أدنى مسؤولية على وزارة الداخلية.

والسلام عليكم ورحمة الله وبركاته،



العقيد: S

حسين حسن الجابر
مدير إدارة الموارد البشرية



B1.7 Samples of completed questionnaire

Internet Voting Survey

Section 1 – Background

1.1 What is your age?

18 – 24 25 – 29 30 – 39 50 – 59 60 – 64 65+

1.2 What is your gender?

Male Female

1.3 Which Level of education are you currently studying?

School College University Postgraduate Others

1.4 Self rating of computing knowledge?

Absolute beginner Some knowledge Average knowledge Pretty knowledgeable Expert

Section 2 – Use of the Online Banking

2.1 On average, how often do you use the internet for Online banking or making online purchases?

Once a week or more 2-4 times a month Once a month Less than once a month Not at all

2.2 Why don't you use the internet for online banking or making online purchases more often? What are your reasons? (Please fill all that apply)

Don't think it is very safe/ secure Things restricting internet use No need for it Prefer personal interaction Unsure

[Asked of those who use online banking or make online purchases less than once a month:]

Section 3 – Confidence in management and accuracy of general elections

3.1 Rate how confident are you that general elections in Qatar are managed fairly and that vote counting is accurate.

← Not Confident Mid-Range Very Confident →

(0 – 3) (4 – 6) (7 – 10)

3.2 Regarding abroad citizens, how do you think they should vote?

Going to Qatar
embassy

Through the website

Phone

Others

Section 4 – Online Voting

4.1 How strongly do you agree or disagree with the following statements about online voting in Qatar general elections, assuming that it would use security systems similar to internet banking and reputable online retailers?

Rate the following:

← Strongly Agree (0 – 3) Mid-Range (4 – 6) Strongly Disagree → (7 – 10)

4.1.1 - I would choose to vote online instead of visiting a polling place

✓

4.1.2 - I would be comfortable with voting online

✓

4.1.3 - I would be confident that I could vote online without anyone seeing who I was voting for

✓

4.1.4 - I would be confident that I could vote online without anyone else unduly influencing my vote

✓

4.1.5 - I would be confident that vote online is more accurate

✓

4.2 If you were to vote online, would you regard the following security features as essential, nice to have or not important?

Essential Nice to have Not important Unsure

A screen which would ask you to confirm who you were voting for before it was made final.

✓

Being able to revisit the voting website to confirm that your vote has been received but not who you have voted for.

✓

Being able to request confirmation using a different means of communication, such as text

✓

Other, please specify: Send SMS

4.3 If you do not believe there should be Online voting in Qatar, please state why:

The technology would be too difficult for some people to use.



The technology may not be reliable.



There would be no easy check that the results are correct and have not been manipulated.



A computer hacker may be able to affect the results



Vote selling



Other, please specify: *prefer personal voting.*

Internet Voting Survey**Section 1 – Background**

1.1	What is your age?					
	18 – 24	25 – 29	30 – 39	50 – 59	60 – 64	65+
1.2	What is your gender?					
	Male			Female		
1.3	Which Level of education are you currently studying?					
	School	College	University	Postgraduate	Others	
1.4	Self rating of computing knowledge?					
	Absolute beginner	Some knowledge	Average knowledge	Pretty knowledgeable	Expert	

Section 2 – Use of the Online Banking

2.1	On average, how often do you use the internet for Online banking or making online purchases?				
	Once a week or more	2-4 times a month	Once a month	Less than once a month	Not at all
2.2	Why don't you use the internet for online banking or making online purchases more often? What are your reasons? <i>(Please fill all that apply)</i>				
	Don't think it is very safe/ secure	Things restricting internet use	No need for it	Prefer personal interaction	Unsure

[Asked of those who use online banking or make online purchases less than once a month:]

Section 3 – Confidence in management and accuracy of general elections

3.1	Rate how confident are you that general elections in Qatar are managed fairly and that vote counting is accurate.		
	← Not Confident	Mid-Range	Very Confident →
	(0 – 3)	(4 – 6)	(7 – 10)

3.2 Regarding abroad citizens, how do you think they should vote?

Going to Qatar
embassy

Through the website

Phone

Others

Section 4 – Online Voting

4.1 How strongly do you agree or disagree with the following statements about online voting in Qatar general elections, assuming that it would use security systems similar to internet banking and reputable online retailers?

Rate the following:

← Strongly Agree (0 – 3) Mid-Range (4 – 6) Strongly Disagree → (7 – 10)

4.1.1 - I would choose to vote online instead of visiting a polling place

✓

4.1.2 - I would be comfortable with voting online

✓

4.1.3 - I would be confident that I could vote online without anyone seeing who I was voting for

✓

4.1.4 - I would be confident that I could vote online without anyone else unduly influencing my vote

✓

4.1.5 - I would be confident that vote online is more accurate

✓

4.2 If you were to vote online, would you regard the following security features as essential, nice to have or not important?

Essential Nice to have Not important Unsure

A screen which would ask you to confirm who you were voting for before it was made final.

✓

Being able to revisit the voting website to confirm that your vote has been received but not who you have voted for.

✓

Being able to request confirmation using a different means of communication, such as text

✓

Other, please specify:

4.3 If you do not believe there should be Online voting in Qatar, please state why:

The technology would be too difficult for some people to use.



The technology may not be reliable.



There would be no easy check that the results are correct and have not been manipulated.



A computer hacker may be able to affect the results



Vote selling



Other, please specify: Difficulty to Access Internet.

B2 Questionnaire 2: Assessing client-side security awareness

B2.1 Questionnaire final version

Security Awareness Survey

Section A

1: 1/31: Gender

Please choose only one of the following:

Female

Male

2: 2/31: Age

Please choose only one of the following:

Under 17

17-29

30-59

Over 60

3: 3/31: Education

Please choose only one of the following:

School

Further Education

Higher Education

Post Graduate

Other

Section B

1: 4/31: How often do u use internet?

Please choose only one of the following:

More than once every day

Once everyday

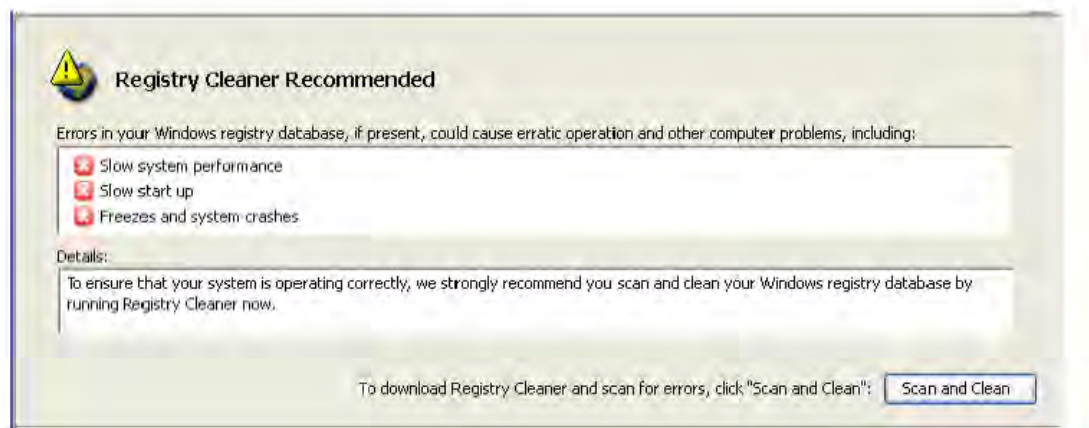
More than once a week

Once a week

Other, Please Specify

Make a comment on your choice here:

2: 5/31: What are you going to do if you see a warning message box like the one below, while you browsing the internet?



Please choose only one of the following:

Response to it

Ignore it

Make a comment on your choice here:

3: 6/31: What do you think is the best way to protect your computer? By using..

Please choose all that apply

Virus protection software

Firewall

Patching your operating system

Not Accessing to Internet

Other, Please Specify

Other:

4: 7/31: How often do you back up your important information, and files?

Please choose only one of the following:

Never

Everyday

Once a week

Once a month

Three to four times a year

Other

5: 8/31: Do you use the same password for more than one application and e -mail?

Please choose only one of the following:

Yes

No

6: 9/31:What do you do to remember your passwords?

Please choose only one of the following:

Write it down and keep it in safe place

Write it down and stick it on the computer monitor or close to your pc

Save it inside your computer in a document

Save it in your mobile phone

Use software to manage your passwords

You don't find problem memorising passwords

Other

7: 10/31: How many characters you use for your passwords?

Please choose only one of the following:

5 characters

6-7 characters

8 characters

9 characters

Other

8: 11/31: Which one of following describes most of your password?

Please choose only one of the following:

Using a memorable word

Combine words and numbers

Combine words, numbers, and characters

Use a strange word even if it's short

Other

9: 12/31: How often do you change your passwords, including what you use for online banking?

Please choose only one of the following:

Never

Every month

Every three months

Once every year

Other

10: 13/31: How important do you think it is to changing your passwords time to time?

Please choose only one of the following:

Not Important

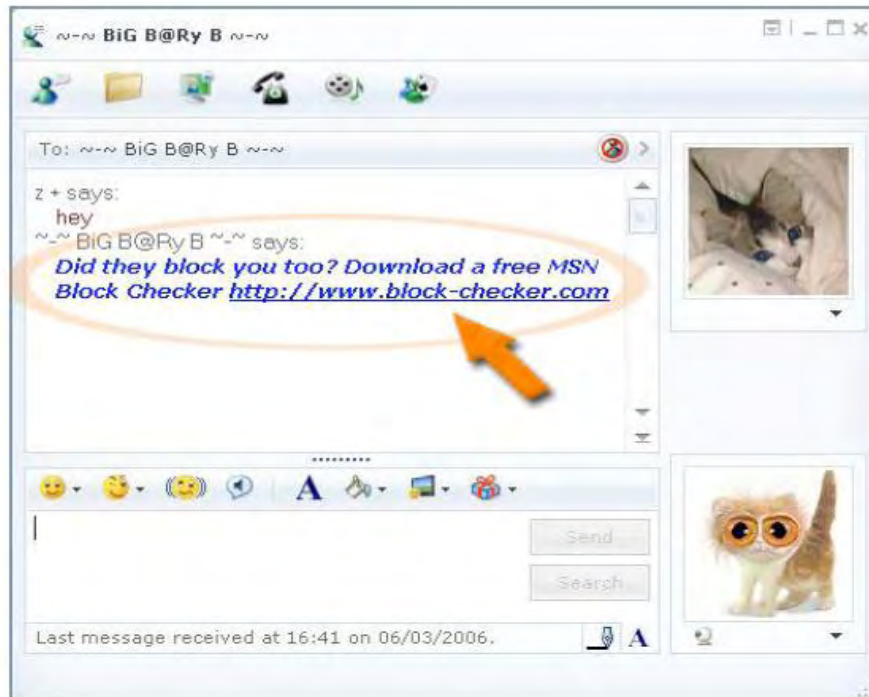
Important

Very Important

Don't Know

Make a comment on your choice here:

11: 14/31: What do you think of the link appears on the Instant Messaging window?



Please choose only one of the following:

Normal message send from friend

Suspicious

Suspicious but you still going to click it

Don't know

Make a comment on your choice here:

12: 15/31: Do you use P2P software?

Please choose only one of the following:

Yes

No

Don't Know

13: 16/31: Do you check files extension before you download any files or music from the internet?

Please choose only one of the following:

Yes

No

Don't Know

14: 17/31: What do you do when you hear about virus attack going to struck soon, or in certain date?

Please choose all that apply

Don't care and use the computer normally

Do nothing because you have anti-virus software even if you are not sure if it's updated or not

Update your anti-virus software immediately

Patch software in your computer

Keep the computer shut at that day

Use computer but you don't open any emails at that day.

Other:

15: 18/31: Do you open e-mails from unknown senders?

Please choose only one of the following:

Yes

Depends on e-mail subject

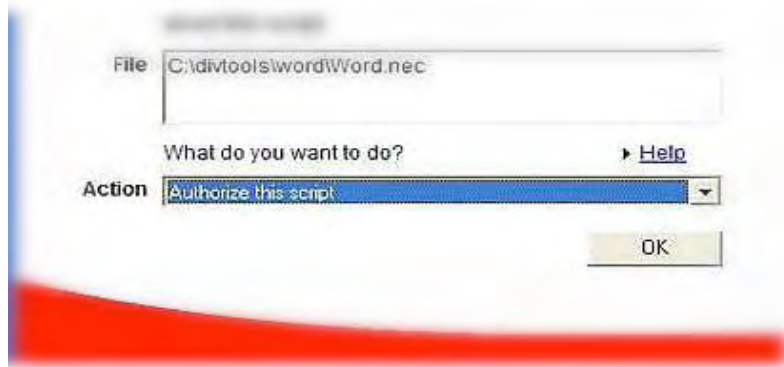
Sometimes

Not Sure

No

Other

16: 19/31: What do you do when your firewall keep showing you messages like the messages below?



Please choose only one of the following:

Just click OK every time message appears

Do read the message carefully every time it appears

Read the message the first time and then just click OK whenever it appears again

Find it disturbing and get fed up with its

Other

17: 20/31: Do you switch off firewall application or anti-virus software when notification messages keep appearing to you a lot?

Please choose only one of the following:

Yes

No

Don't Know

18: 21/31: Who should act, and who's to blame for Internet Security?

Please choose all that apply

Governments

Internet providers

Big companies problem e.g. Microsoft, Yahoo

Computer users

Other, Please Specify

Other:

B2.2 Sample of completed questionnaire

Security Awareness Survey

Section A

1: 1/31: Gender
Please choose **only one** of the following:

Female
Male

2: 2/31: Age
Please choose **only one** of the following:

Under 17
17-29
30-59
Over 60

3: 3/31: Education
Please choose **only one** of the following:

School
Further Education
Higher Education
Post Graduate
Other

Section B

1: 4/31: How often do u use internet?
Please choose **only one** of the following:

More than once every day
Once everyday
More than once a week
Once a week
Other, Please Specify
Make a comment on your choice here:

2: 5/31: What are you going to do if you see a warning message box like the one below, while you browsing the internet?

Please choose **only one** of the following:

Response to it
Ignore it
Make a comment on your choice here:

3: 6/31: What do you think is the best way to protect your computer? By using..

Please choose **all** that apply

Virus protection software

Firewall

Patching your operating system

Not Accessing to Internet

Other, Please Specify

Other:

4: 7/31: How often do you back up your important information, and files?

Please choose **only one** of the following:

Never

Everyday

Once a week

Once a month

Three to four times a year

Other

5: 8/31: Do you use the same password for more than one application and e-mail?

Please choose **only one** of the following:

Yes

No

6: 9/31: What do you do to remember your passwords?

Please choose **only one** of the following:

Write it down and keep it in safe place

Write it down and stick it on the computer monitor or close to your pc

Save it inside your computer in a document

Save it in your mobile phone

Use software to manage your passwords

You don't find problem memorising passwords

Other

7: 10/31: How many characters you use for your passwords?

Please choose **only one** of the following:

5 characters

6-7 characters

8 characters

9 characters

Other

8: 11/31: Which one of following describes most of your password?

Please choose **only one** of the following:

Using a memorable word

Combine words and numbers

Combine words, numbers, and characters

Use a strange word even if it's short

Other

9: 12/31: How often do you change your passwords, including what you use for online banking?

Please choose **only one** of the following:

- ☒ Never
- ☐ Every month
- ☐ Every three months
- ☐ Once every year
- ☐ Other

10: 13/31: How important do you think it is to changing your passwords time to time?

Please choose **only one** of the following:

- ☐ Not Important
- ☒ Important

Very Important

Don't Know

Make a comment on your choice here:

11: 14/31: What do you think of the link appears on the Instant Messaging window?



Please choose **only one** of the following:

- ☒ Normal message send from friend
- ☐ Suspicious
- ☐ Suspicious but you still going to click it
- ☐ Don't know

Make a comment on your choice here:

12: 15/31: Do you use P2P software?

Please choose only one of the following:

- ☒ Yes
- ☐ No
- ☐ Don't Know

13: ^{16/31} Do you check files extension before you download any files or music from the internet?

Please choose only one of the following:

Yes

No

Don't Know

14: ^{17/31} What do you do when you hear about virus attack going to struck soon, or in certain date?

Please choose all that apply

Don't care and use the computer normally

Do nothing because you have anti-virus software even if you are not sure if it's updated or not

Update your anti-virus software immediately

Patch software in your computer

Keep the computer shut at that day

Use computer but you don't open any emails at that day.

Other:

15: ^{18/31} Do you open e-mails from unknown senders?

Please choose only one of the following:

Yes

Depends on e-mail subject

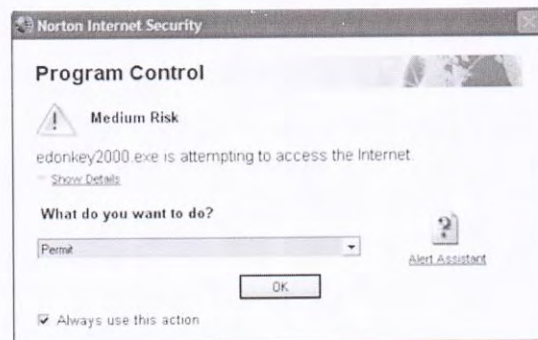
Sometimes

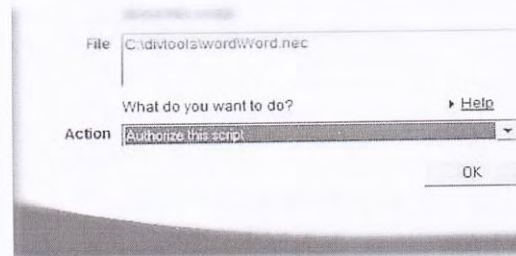
Not Sure

No

Other

16: ^{19/31} What do you do when your firewall keep showing you messages like the messages below?





Please choose **only one** of the following:
 Just click OK every time message appears
 Do read the message carefully every time it appears
 Read the message the first time and then just click OK whenever it appears again
 Find it disturbing and get fed up with it
 Other

17: 20/31: Do you switch off firewall application or anti-virus software when notification messages keep appearing to you a lot?

Please choose **only one** of the following:
 Yes
 No
 Don't Know

18: 21/31: Who should act, and who's to blame for Internet Security?
 Please choose **all** that apply

Governments
 Internet providers
 Big companies problem e.g. Microsoft, Yahoo
 Computer users
 Other, Please Specify
 Other:

B2.3 Questionnaire results

Q1	
Male	91.00%
Female	9.00%
Q2	
Under 18	0%
18-29	80.00%
30-59	20.00%
Over 60	0%
Q3	
Virus protection software	91.11%
Firewall	62.22%
Patching OS	37.78%
Not accessing the Internet	15.56%
Others	12.00%
Q4	
Everyday	13.33%
Once a week	17.78%
Once a month	24.44%
Three to four times a year	20.00%
Never	24.44%
Q6	
Do not have problem memorising passwords	73.33%
Use password management system	4.44%
Save it in mobile phone	2.22%
Save it in a computer document	4.44%
Write it down and stick it on monitor or next to PC	6.67%
Write it down and keep it safe	6.67%
Other	2.22%
Q7	
5 Characters	6.67%
6-7 Characters	28.89%
8 Characters	17.78%
9 Characters	17.78%
Other	28.89%
Q8	
Use strange word even if it's short	4.44%
Using a memorable word	31.11%
Combine words and numbers	20.00%
Combine words and numbers and characters	35.56%
Other	8.89%
Q9	
Every month	2.20%
Every three months	37.78%
Once a year	4.44%

Never	46.67%
Other	8.89%

Q 11 Importance of changing passwords

Very important	31.26%
Important	33.26%
Not important	33.26%
Do not know	2.22%

Q11- Trustworthiness of suspicious link

Suspicious	68.89%
Suspicious but still going to click at it	8.89%
Normal message sent from friend	13.33%
Do not know	8.89%

Question 12. Use of P2P software

Yes	37.78%
No	44.44%
Do not know	17.78%

Q 13 Checking file extensions before downloading.

Yes	75.56%
No	17.78%
Do not know	6.67%

Q 14 Reaction to virus attack, imminent or on certain date

Use computer without opening any email that day	11.11%
Keep the computer shut that day	2.22%
Patch computer software's	31.11%
Updating the anti-virus immediately	64.44%
Do nothing once there is anti-virus software	8.89%
Do not care and use the computer normally	26.67%
Other	4.44%

Q15 Opening e-mails from unknown senders

Yes	6.67%
Depends on email subject	20.00%
Sometimes	17.78%
Not sure	8.89%
No	44.44%
Other	2.22%

Q16 Respondents' reaction to repeated firewall notification messages

Find it disturbing and get fed up with it	6.67%
Read the message the first time and then just click Ok when ever it appear again	20.00%

Appendix B: Questionnaires

Do read the message carefully every time it appears	57.78%
Just click ok every time message appears	11.11%
Other	4.44%

Q17 Switching off security application	
Yes	8.89%
No	84.44%
Do not know	6.67%

Q 18 Blame for Internet security problems	
Governments	26.67%
ISP	55.56%
Big Companies	28.89%
Computer users	64.67%
Others	20.00%

Appendix C: I-voting Experiment

C1 Plan and Design

The system is a prototypical I-voting system which receives votes from citizens over the Internet. The votes are encrypted. This encryption system is based on private and public keys. A public key is given to the citizen in order to secure their data. The private key is used by the server to identify and confirm the eligibility of the voter. It also uses this key to determine, which voting area the citizen belongs to. The votes are stored on the administrative computer, while the key is stored on the server. However, the server does not store the votes. Therefore, the information connecting any particular person to a specific vote is in two different places and resistant to security breaches. This is an additional safeguard to the encryption.

The I-voting process can be described as follows:

1. The voter will login to the system and use an ID number along with a password for identity.
2. The system will check the eligibility of the voter (i.e., voting age, constituency).
3. The voter sees only the candidate list with useful information about them (i.e., short biography, action plan, an invitation for meetings, speech and clips, etc.).
4. The voter chooses a candidate. This information is encrypted and e-signed for security and anonymity purposes.
5. The voter confirms their choice and attaches their digital signature. This enhances security and maintains anonymity. The following illustration gives an idea of the encryption techniques.

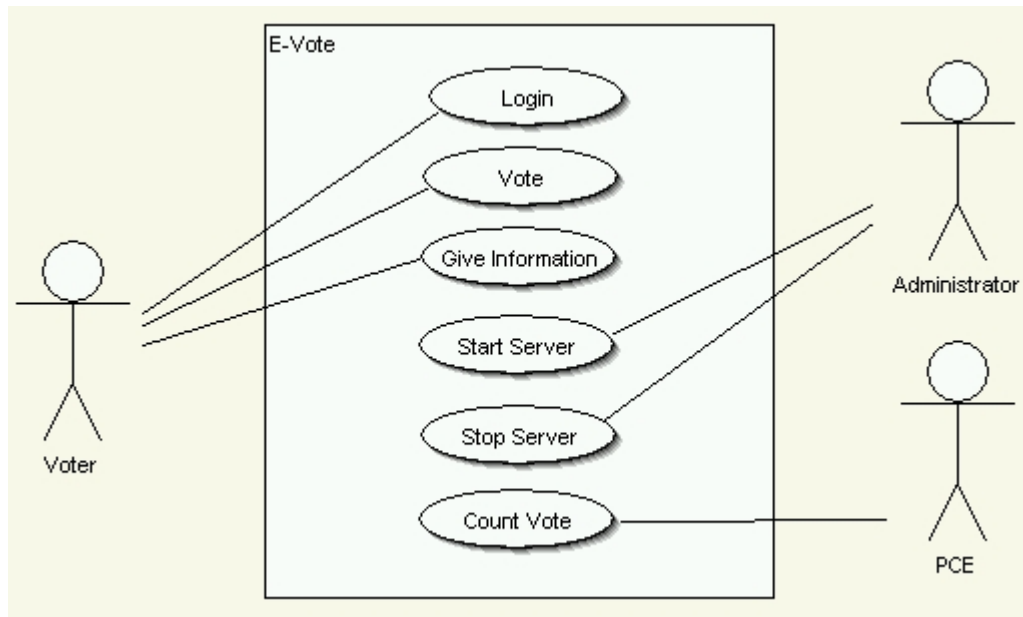


Figure C1 - Use case demonstrates system operations.

Voter: a person allowed to vote in the election.

Administrator: responsible for starting and stopping server.

PEC: responsible for counting votes of each candidate.

Registration: create pass

Login: (Login to the system)

- Voter starts the system, and enters his/her ID and PIN. Password provided by Election board.
- Voter presses Login button.
- System checks ID and corresponding PIN for validity.
- If ID and PIN are correct, system will take a voter to the voting page.

Failed Login: Failed

- Voter starts the system and enters his ID and PIN.
- Voter presses Login button.
- System checks ID and corresponding PIN for validity.
- If ID and PIN are incorrect, system will refuse voter and will not let him/her in.

Give Information:

- Voter will be asked about some personal information for verification.
- Voter will enter the information and press Next button.
- System holds his/her information.

Vote: (Casting Vote)

- Voter chooses a candidate from his/her area.
- Voter clicks on Vote button.
- System validates data and casts the voter's vote.
- System shows a message to the voter that the vote was successful.

Failed Vote:

- Voter enters wrong information about him/herself.
- System refuses the operation.

PEC: (Monitoring and counting votes)

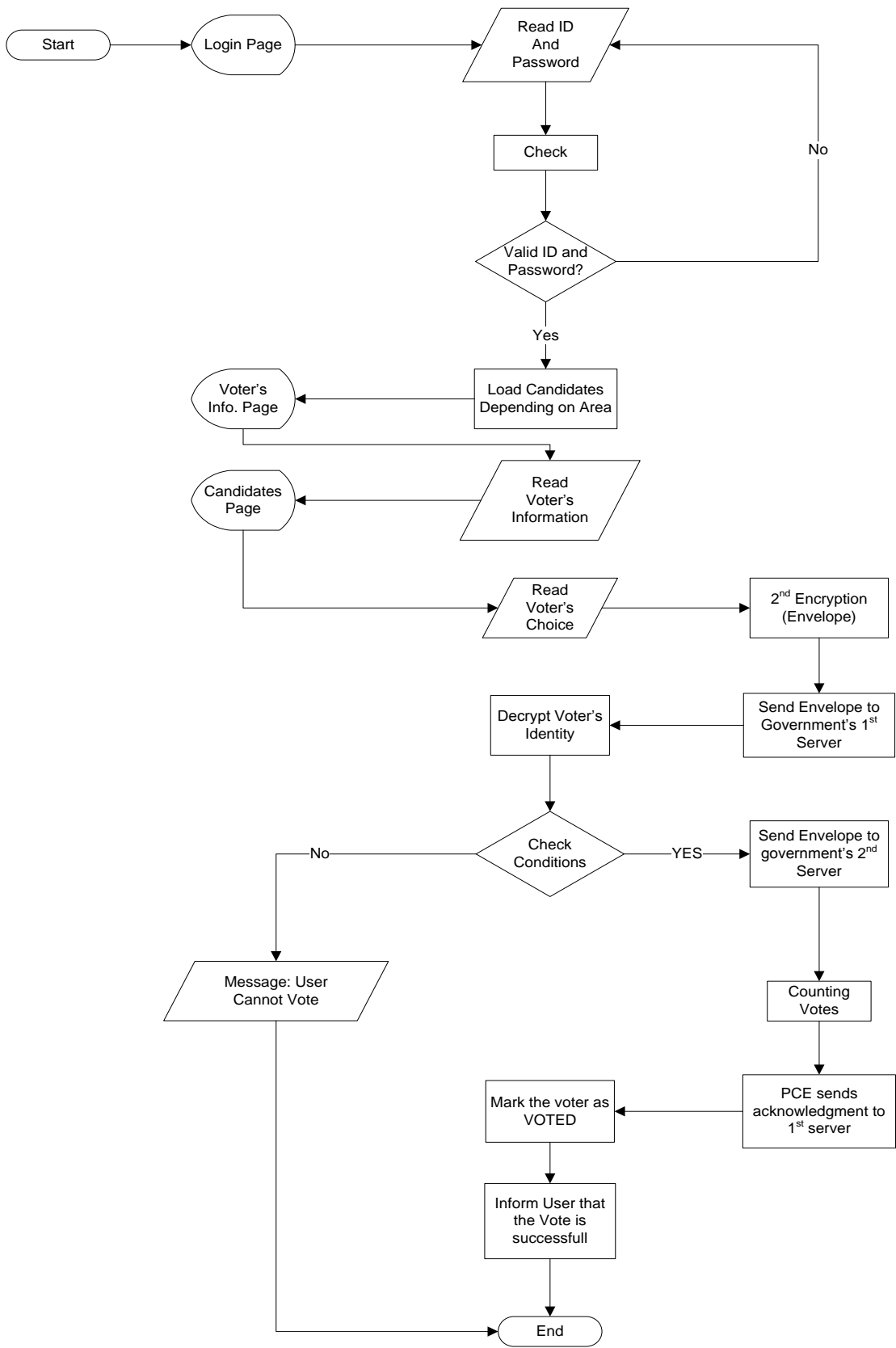
- Observation of the change of number of votes for each candidate.

Start Server:

- Make server ready to accept votes.

Stop Server:

- Close system so no votes can be accepted.



B

Figure C2 - System flow chart

C2 Preparations

The Qatari Interior Ministry has called on the Qatari citizens registered in the election lists to vote in the elections of the Municipal council and drew their attention to the following:

- The election will be held be secret ballot.
- A voter should not publicly declare the name of the candidate to whom he voted.
- A voter who cannot use the ballot may tell the members of the committee, openly or secretly, the name of the candidate he wanted to vote for, after which the chairman of the committee would write the name of the candidate in the ballot.
- The Ministry warned against the use of the various forms of election propaganda inside the election premises.
- The election committees start the vote counting and the declaration of the results at the end of the balloting process. The winner in the election is the candidate who gets the largest number of correct votes. If votes are equal for more than one candidate, the committee would vote on who is the winner in their presence.

Appeals procedure.

The period of appeals begins on the second day of elections and continues for 15 days. During this period, each candidate or voter may request the declaration of the candidate elected in his constituency as non-authentic. The request shall be submitted in writing to the election department to be referred to the chairman of the committee investigating the appeals and grievances.

The state is gradually increasing popular participation in public affairs.

Those aged 18 or above, both men and women, can vote in the municipal elections while those aged 21 years or above can become candidates. The specific rules for the legislative assembly were still to be announced, the official pointed out.

During the last Municipal Council elections, there were 28,139 registered voters and 13,959 of them cast their votes. The new law under consideration would spell out who would be eligible to vote in the general elections, Lt Col Sulaiti said.

The elections will be the first of its kind to be held under a new state constitution. Under it, two-thirds of the 45-member legislative assembly will be elected while the rest would be nominated by HH the Emir.

C3 Implementation

An investigation was made regarding currently available programming languages. In most cases, the researcher found that technologies such as Visual studio and Oracle offered highly optimized and efficient tools for creating a Voting system.

The experiments were carried out at ALMAJAZ Computer Lab, In ALMAJAZ. The computers have the following specification: Intel Core™ 2.8 Quad 2 Duo, 4GB memory and 500GB HDD. Based on available resources and skills, I-voting system was implemented successfully. Some screen shots of the system are shown below:

Voter Interface



1. Voter's ID number. Each voter was asked to enter their ID number for authentication.

2. Pin number given by Government to a voter

Login Button. However, in the experiment a unique Pin was given manually to each voter in order to log in to the system.

Voter Information Interface



- 1. Voter’s region which is defined based on voter living area.
- 2. Candidate’s region
- 3. Vote button to encrypt vote and send It securely.

PEC Interface

Election committee and 3rd party are allowed view vote counting according to areas without the ability to manipulate voting results.



Permanent Elections Committee (PEC), aims at activity participation in Qatari Community. The PEC seeks to accomplish some of the following goals.

- 1) Activating political participation in the Qatari community through holding meetings, seminars, training courses and other activities necessary to achieve this.
- 2) Raising awareness of voters about their rights and obligations and introducing them to the mechanisms of the election process.
- 3) Encouraging candidates to acquire skills of democratic elections process.
- 4) Evaluating the election process.
- 5) Rehabilitating women and girls to participate in elections.
- 6) Working towards establishing a national center for rehabilitating women and girls for elections.

A law has yet to be drafted specifying what powers will be delegated to the parliament. Voters, including women, will be able to choose 30 of the 45 members of parliament while the emir, Sheikh Hamad bin Khalifa al-Thani, will appoint the rest. The Gulf Arab state is home to some 850,000 people, about 150,000 of them Qatari nationals. Qatar currently has an advisory Shura council whose members are all appointed by the emir.

C4 Screenshots

I-Voting Server Interface



Voter Interface



Voter Information Interface

Voter Information

Name

Hamed Saad

ID.

25963404231

D.O.B.

1994/08/12

Next

Candidates List Interface

Candidates List

Al Markheya

☒ Mahmood Saad

☐ Mesaal abdulla

☐ Ahmad Mohammad

Vote

PEC Interface:



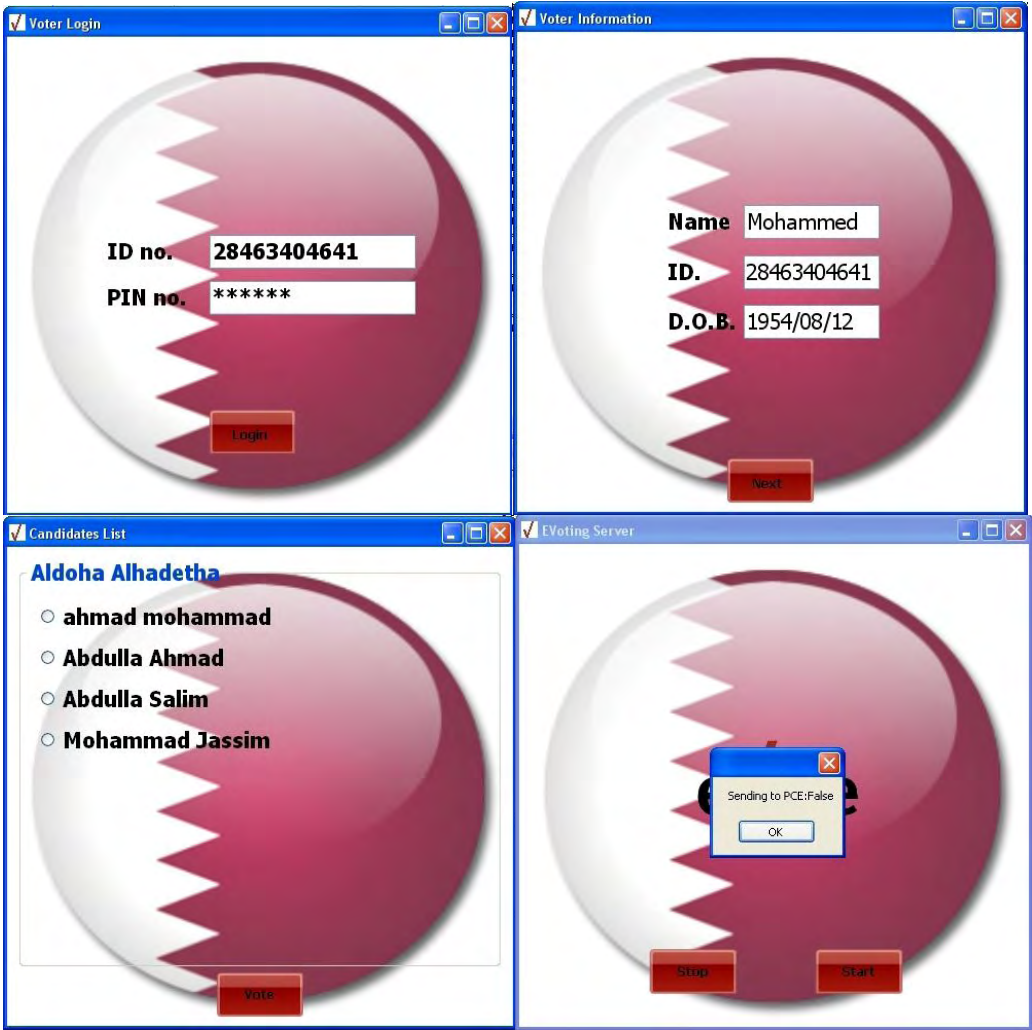
C5 Unit Testing

Unit testing is the procedure used to validate that the individual units or subsystems are working properly. The goal of unit testing is to test each function of the system separately to ensure functioning correctly. Parts of the program are tested first individually. As a result, testing the whole system, i.e. integration testing, will become much easier. The following are some selected examples of unit testing:

Example (1): The entry data in the login screen was in a wrong type.



Example (2): A person who is younger than 18 years old.



C6 user manual

E-Voting Server Interface



- 1- Start Button to Start the Server
- 2- Stop Button to Stop the Server

Voter Interface

The image shows a screenshot of a web application window titled "Voter Login". The window has a blue border and standard window controls (minimize, maximize, close) in the top right corner. The main content area features a large, stylized circular graphic with a white and maroon color scheme, resembling the flag of Qatar. Overlaid on this graphic are two input fields and a button. The first field is labeled "ID no." and contains the text "25463404641". The second field is labeled "PIN no." and contains the text "*****" followed by a cursor. Below these fields is a red button labeled "Login". Three callout lines with circular endpoints point to these elements: callout 1 points to the ID number, callout 2 points to the PIN number, and callout 3 points to the Login button.

Voter Login

ID no. 25463404641

PIN no. *****

Login

1

2

3

- 1- Voter's ID Number
- 2- Pin Number Given by the Government to the Voter
- 3- Login Button

Voter Information Interface

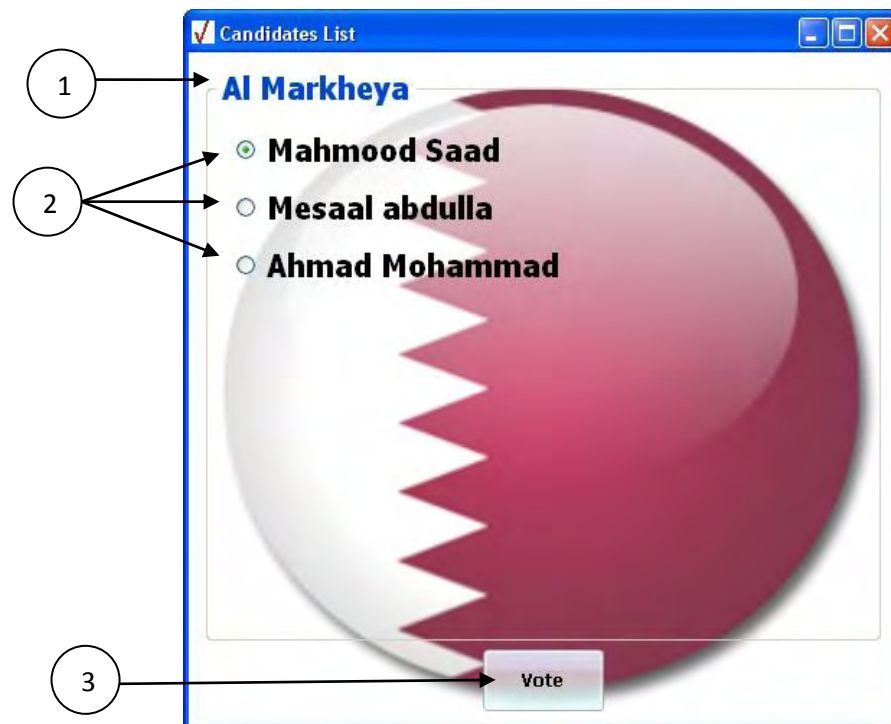
The screenshot shows a window titled "Voter Information" with a blue border. Inside, there is a large, stylized Qatari flag. Overlaid on the flag are three text input fields and a red "Next" button at the bottom. Arrows from numbered circles (1-4) point to these elements: 1 points to the "Name" field, 2 points to the "ID." field, 3 points to the "D.O.B." field, and 4 points to the "Next" button.

Field	Value
Name	Hamed Saad
ID.	25963404231
D.O.B.	1994/08/12

Next

- 1- Voter's Name
- 2- Voter's ID
- 3- Voter's Date of Birth
- 4- Next Button to Candidate List Interface

Candidates List Interface



- 1- Voter's Region
- 2- Candidate's Region
- 3- Vote Button to Encrypt the Vote and Send It.

C7 Experiment evaluation

C7.1 Questionnaire first version

For the following questions, please tick or circle the number that best represents your experience when exploring the Electronic Voting.

- 1). Please rate, on a scale of 1 to 7, your sense of being in the Electronic Voting, on a scale of 1 to 7, where 7 represents your normal experience of being in a place.

I had a sense of “being there” in the Electronic Voting:

1	2	3	4	5	6	7
Not at all						Very much

- 2). How much were you able to control events in Electronic Voting?

How much were you able to control events:

1	2	3	4	5	6	7
No times						Almost all the time

- 3). When you think back to the experience, do you think of the Electronic Voting more as images that you saw or more as somewhere that you visited ‘Poll station’?

The Electronic Voting seemed to me to be more like:

1	2	3	4	5	6	7
Images that I had seen						Somewhere that I had visited

- 4). During the time of the experience, which was the strongest on the whole, your sense of being in the Electronic Voting or of being elsewhere?

I had a stronger sense of:

1	2	3	4	5	6	7
Being elsewhere						Being in Electronic Voting

- 5). How aware were you of events occurring in the real world around you

I think of the Electronic Voting events were so clear:

1	2	3	4	5	6	7
---	---	---	---	---	---	---

Appendix C: I-voting Experiment

Not at all						very much
------------	--	--	--	--	--	-----------

- 6). How compelling was your sense of moving around the Electronic Voting?

How compelling was your sense of moving around the Electronic Voting:

1	2	3	4	5	6	7
Not very often						Most of the time

- 7). During the time of your experience, did you often think to yourself that you were actually in the Electronic Voting?

During the experience I often thought that I was really standing in the Election:

1	2	3	4	5	6	7
Not very often						Most of the time

- 8). How was your experience while using the electronic voting, do you think it was easy to use or difficult to use

I found the electronic voting:

1	2	3	4	5	6	7
Easy to use						Difficult to use

- 9). How much were you able to read the content in Electronic Voting?

Electronic voting content seem to me to be more like:

1	2	3	4	5	6	7
Easy to Read						Hard to Read

- 10). When you think back to the experience, do you think to content of the Electronic Voting was well presented or more confusing?

The organization of information in Electronic Voting seemed to me to be more like:

1	2	3	4	5	6	7
Very Clear						Confusing

- 11). During the time of the experience, how was the voting process, did you had the sense of being in long procedure voting?

I found that vote casting process:

1	2	3	4	5	6	7
Very easy						Very difficult

- 12). How did you found the structure of the system, was it so clear and easy

I think of the Electronic Voting structure was so clear:

1	2	3	4	5	6	7
Not at all						very much so

- 13). In traditional election, citizen were asked to registered before election, in electronic voting participant were pre-registered by default?

I found pre-registration useful:

1	2	3	4	5	6	7
Not at all						very much

- 14). During your experience, did you think that information about candidate were useful to make your mind in choosing candidate?

During the experience I often thought that information about candidate was useful:

1	2	3	4	5	6	7
Not very useful						Very useful

- 15). What else would you like us to know about your reaction to the electronic voting design? All feedback, whether negative or positive, is welcome?

C7.2 Questionnaire final version**I-voting Experiment Evaluation**

Authentication Phase	Yes	No
Did you find problems at the authentication stage?		
Did you find authentication process secure because it asks for two factors?		
Did the system identify you without problems?		
Was the e-token easy to install?		
Were you concerned about your e-token, what would happen if e-token is lost?		
Was the process fast?		
Vote casting phase		
Was the quality of ballot design maintained?		
Was the system fast?		
Did you have any problems at voting stage? If yes, please write it down.		
Did you find confirmation of vote received useful?		
Did you feel same experience with paper based voting?		
Other questions		
Was the presentation given on how system works useful to build trust and confidence?		
Did the presentation change your mind towards trusting system?		
Please comment on system transparency		

C7.2 Sample of completed Questionnaire

I-voting Experiment Evaluation		
Authentication Phase	Yes	No
Did you find problems at the authentication stage?	✓	
Did you find authentication process secure because it asks for two factors?		✓
Did the system identify you without problems?		✓
Was the e-token easy to install?	✓	
Were you concerned about your e-token, what would happen if e-token is lost?	✓	
Was the process fast?		✓
Vote casting phase		
Was the quality of ballot design maintained?		✓
Was the system fast?	✓	
Did you have any problems at voting stage? If yes, please write it down.		✓
Did you find confirmation of vote received useful?	✓	
Did you feel same experience with paper based voting?	✓	
Other questions		
Was the presentation given on how system works useful to build trust and confidence?	✓	
Did the presentation change your mind towards trusting system?	✓	
Please comment on system transparency It is better to make source code available for public inspection.		

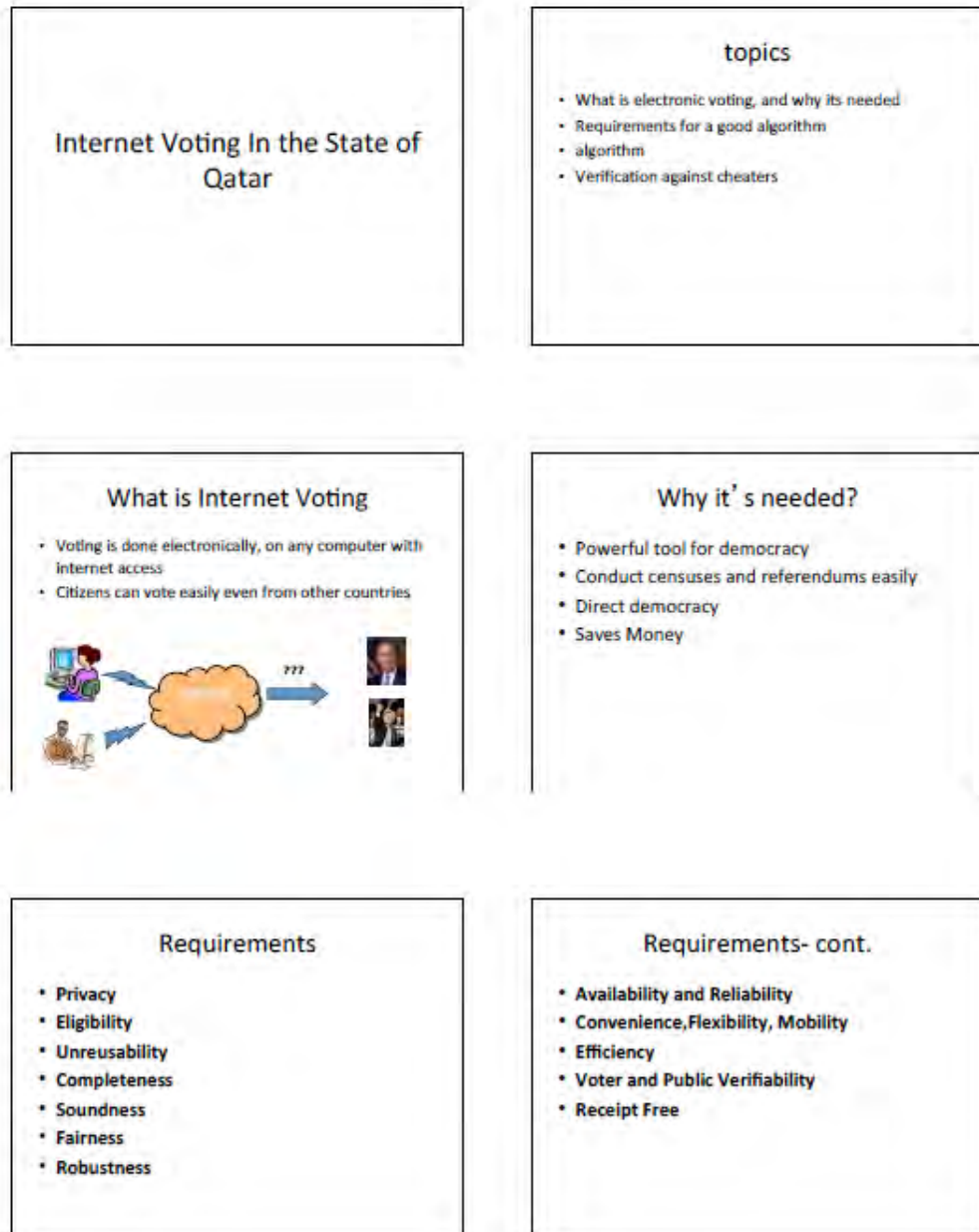
I-voting Experiment Evaluation

Authentication Phase	Yes	No
Did you find problems at the authentication stage?	—	
Did you find authentication process secure because it asks for two factors?	—	
Did the system identify you without problems?	—	
Was the e-token easy to install?		—
Were you concerned about your e-token, what would happen if e-token is lost?	—	
Was the process fast?	—	
Vote casting phase		
Was the quality of ballot design maintained?	—	
Was the system fast?	—	
Did you have any problems at voting stage? If yes, please write it down.		—
Did you find confirmation of vote received useful?		—
Did you feel same experience with paper based voting?	—	
Other questions		
Was the presentation given on how system works useful to build trust and confidence?	—	
Did the presentation change your mind towards trusting system?	—	
Please comment on system transparency allow head of Family tribe to monitor the Process		

I-voting Experiment Evaluation

Authentication Phase	Yes	No
Did you find problems at the authentication stage?		✓
Did you find authentication process secure because it asks for two factors?	✓	
Did the system identify you without problems?	✓	
Was the e-token easy to install?	✓	
Were you concerned about your e-token, what would happen if e-token is lost?		✓
Was the process fast?	✓	
Vote casting phase		
Was the quality of ballot design maintained?	✓	
Was the system fast?	✓	
Did you have any problems at voting stage? If yes, please write it down.		✓
Did you find confirmation of vote received useful?	✓	
Did you feel same experience with paper based voting?	✓	
Other questions		
Was the presentation given on how system works useful to build trust and confidence?	✓	
Did the presentation change your mind towards trusting system?	✓	
Please comment on system transparency Provide a receipt of vote.		

C7.3 Presentation of I-voting prototype



Current Solutions

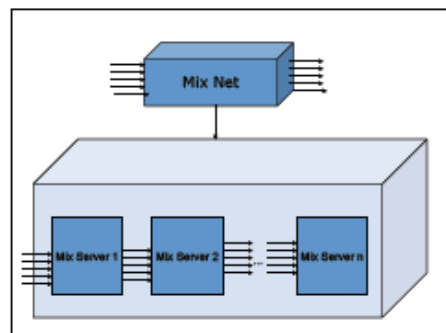
- Requirements contradict
 - Receipt freeness and Voter Verifiability
- Very hard to satisfy all the requirements
- No existing algorithm as of today do so, without assumptions
- There are three groups of algorithms:
 - Blind Signature
 - Homomorphic property
 - Mix Net

Algorithm

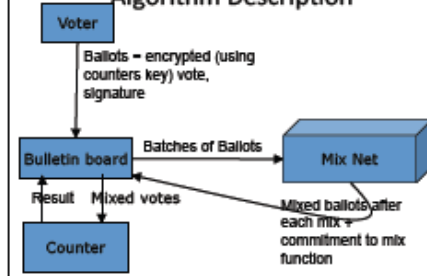
- Described in article:
 - *"Making Mix Nets Robust For Electronic Voting By Randomized Partial Checking"* by Jakobsson Juels and Rivest
- Provides all the requirements except receipt freeness
- Our implementation is limited due to time constrains.

Algorithm Description

- Entities:
 - Voter
 - Mix Net Servers
 - Counter
 - Bulletin Board
- We cannot trust any entity on its own



Algorithm Description



Bulletin Board Functionality

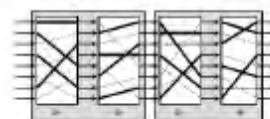
- Stores ballots received from Voters
- Initializes mixing phase
- Stores batches of ballots after each mix and servers commitments
- Distributes batches to mix servers
- Initializes counting phase, stores the result and the counters key
- All stored data is publicly available

Verification

- Mix Server submits mix function commitment to BB
- BB asks server to open $\frac{1}{2}$ of each server's mix function connections
 - Connections are determined by data stored in BB
- Corrupt mix servers are identified with good probability
- Voter can verify his vote

Verification (cont)

- For Each ballot, at least one mix should be secret
- Solution - Partial randomized checking
 - Divide mix servers in pairs
 - For each pair check half the entries in first and the supplemental entries in other



Appendix D: Proposed Model

D1 Requirements of the Voting Process

Accuracy

An essential property of any equipment used by the voting process is that it must accurately record and tally votes. Unless such an assurance can be given, the voters' confidence in the election, as well as the integrity and legitimacy of the election's outcome are at risk.

Even though voting equipment can be designed to count votes as recorded with 100% accuracy, the frequency with which the equipment counts votes in the way intended by voters is a function not just of the equipment's design but also of the interaction of people and processes. These latter factors include:

- Technicians have followed the proper procedures in testing and maintaining the system;
- Voters have followed the proper procedures when using the system;
- Election officials have provided voters with procedures that they can understand and follow;
- Poll workers have properly instructed and guided voters.

Security

In conducting elections, officials must be in a position to assure the public that the confidentiality of the ballot is always maintained and that fraud is prevented. The people, processes and technology involved in the election system all play a part in providing this assurance. This depends on and consists of the security procedures and practises implemented by the election authority, as well as the security awareness and training of the election workers executing them and the security features of the systems employed.

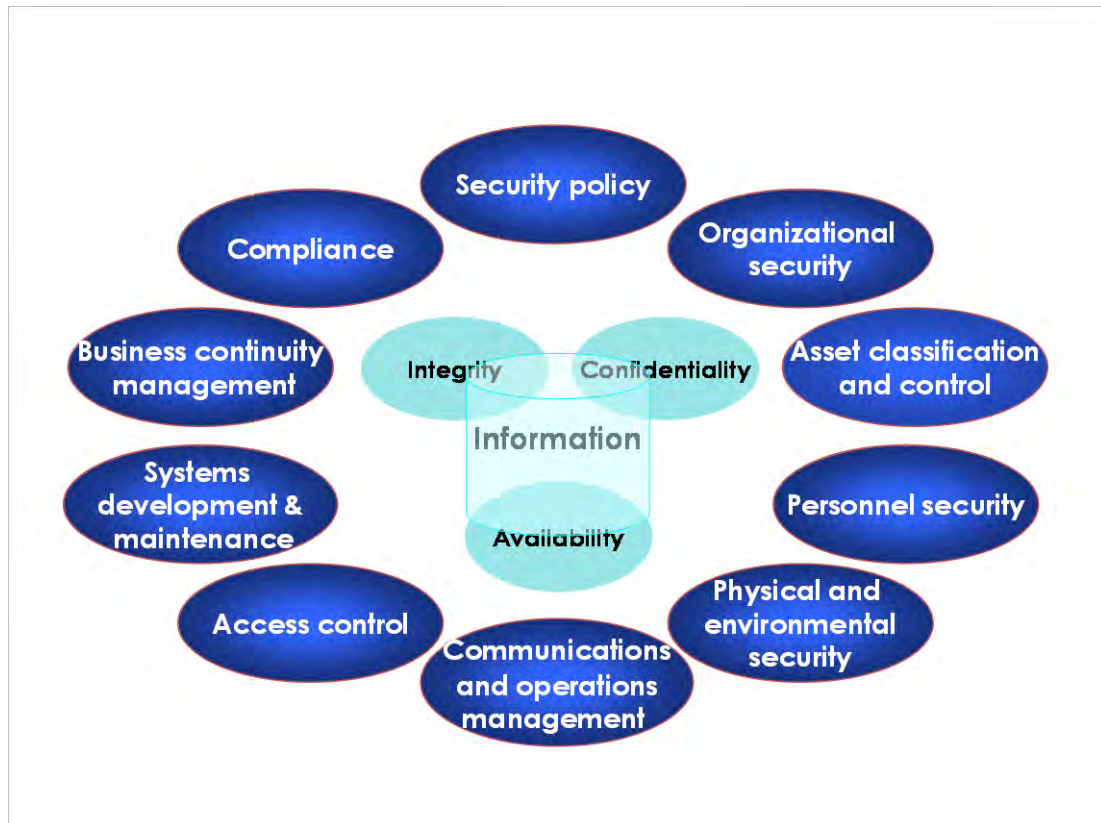
Election officials are responsible for establishing and maintaining privacy and security procedures that protect against threats to the integrity of elections. These security threats include the potential modification or loss of electronic voting data (specifically votes),

the loss, theft or modification of physical ballots, as well as unauthorised access to software and electronic equipment. Physical access controls must be implemented to secure voting equipment, vote tabulation equipment and ballots. Software access controls (such as passwords and firewalls) are required to limit the number of people who can access and operate voting devices, election management software and vote-tabulation software. In addition, election processes must be designed to ensure privacy by protecting the confidentiality of the vote: physical screens are deployed around voting booths and poll workers are present to prevent voters from being observed or coerced while voting.

In order to provide security assurance for an I-voting system, the implementation of an ISO 27001 approach can provide an appropriate response to the security challenges posed by an I-voting system. ISO 27001 is an international standard that covers every aspect of information security:

- Equipment;
- Management policies;
- Legal aspects, and
- Human resources.

The standard provides a set of controls based on the best practises in information security grouped into 10 domains. The domains are shown in Figure 9.2.



Identity Assurance

The cornerstone of trust in the results of an election is the ability to assure the identity of voters against identity and over-voting. Taking each separately, this means that trust that their identity will be respected and preserved; nothing will change or remove their identity in the voting process. The second aspect is that electors trust that the election process will prevent individuals from voting more than once using the same or different names or identities.

In the same way that an electronic election brings the advantages of the I-world to the election process, it also brings with it threats. A successful I-voting system must efficiently address the threats to personal identity that the digital world introduces.

Confidentiality and Integrity of Votes

Votes must be confidential when cast and nothing should affect their confidentiality. This is essential for avoiding vote selling and voter coercion. The integrity of a vote (in the sense of an election, referendum, etc.) is the assurance that the results cannot be contested or votes repudiated. A trusted I-voting system must implement mechanisms for confidentiality and integrity, examples of which are the use of Public-Key Infrastructure (PKI) technologies for the encryption of voting information (i.e., for the maintenance of confidentiality) and for digital signatures (used to maintain integrity). Access to voting information must be handled by a well-defined process which exists in parallel with the PKI technical infrastructure.

D2 Software requirement

Access controls

Multi election workers have to enter their user names and passwords so that they can access voting systems and software. This is intended to ensure that only authorised users make modifications.

Physical controls

Hardware locks and software seals can be used to protect against the unauthorised access to voting equipment and software once it has been prepared for an election.

Audit trails

Audit trails are used to provide documentary evidence to be used in the recreation of election-day activity. Audit-trail information includes the number of ballots cast (by each ballot configuration or type) and the totals of votes for each candidate in each context. Audit trails can also be used for verification purposes, particularly when a recount is performed.

Accuracy

As noted above, by accuracy is intended the accuracy of recording and tallying of votes by voting equipment. The approach recommended here for security I-voting systems against identity threats is to implement an efficient security-management system for voters. Such a system would employ authentication using at least two of the following three factors:

1. What I know (passwords, PINs, etc.);
2. What I can bring or what I have (identity document, election card, dongle, etc.),
and
3. What I am (biometrics such as fingerprints, iris recognition, voice recognition,
and so on).

Ease of Use

In a fashion similar to accuracy, ease of use, or user friendliness, largely depends upon how voters interact with the voting system, both physically and intellectually. This interaction, commonly referred to as the human/machine interface, is a function of the system design, the processes established for its use and user education and training.

Among other things, the quality of ballot design and how well voters are educated in the use of e-government portal affect how easy voters find the system to use.

A further aspect of ease of use is the ease with which diverse groups of voters, including those with disabilities.

Efficiency

Efficiency relates to the speed of tallying votes. It is an important consideration for jurisdictions because it influences the time voters have to wait to cast their votes, which can be a factor in voter turnout. In addition, it affects the number of voting systems that a jurisdiction needs to acquire and maintain, and thus affects the cost of engaging in a ballot.

Efficiency can be measures in terms of the number of people that the I-voting can accommodate within a given time, how quickly the system can count votes and the length of time that voters are required to wait.

For the proposed model application refer to Appendix F (CD).

D3 Presentation of the model

Context and Objectives

- Electronic voting (e-voting) is a term used for different types of voting by electronic means of casting and counting votes.
- Two primary categories
 - Optical Scan Systems using electronic technology to tabulate paper ballots
 - Direct Recording Electronic Systems (DRE)

Challenges

- Security
 - Identity assurance (what I know, what I have and what I am)
 - Vote confidentiality and Integrity
 - Auditability (able to be audited)
- Accuracy
- Ease of Use
- Efficiency

Directing Principles

- In order to address the challenges stated above we propose to implement an e-voting system based on the following directing principles
 - Internet Voting (i-voting) is a specific case of remote electronic voting, whereby the vote takes place over the Internet such as via a web site or voting applet
 - Usage of the Qatari National ID card as credential support to provide the voters identity assurance
 - Usage of the PKI credentials within the smart card in order to ensure the vote confidentiality and integrity

Proposed Solution

Step 1



Qatari citizens need Qatar smart ID card



Step 2



Smart card and finger print reader issued for authentication



Step 3



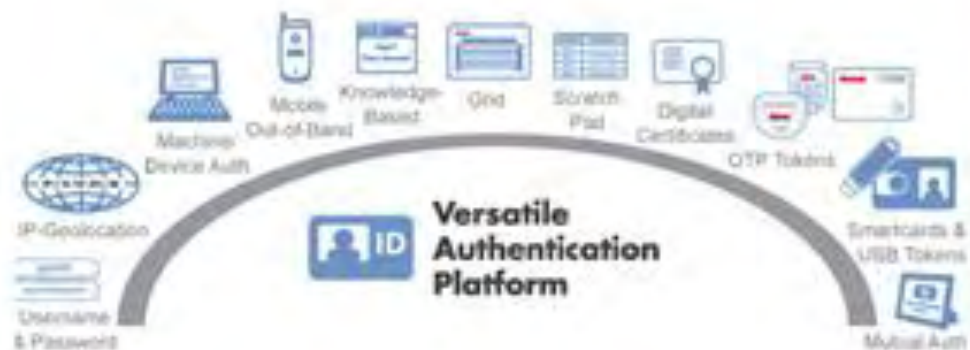
MOI provides Qatari citizens with voting application on protected CD (no copying or modifying).



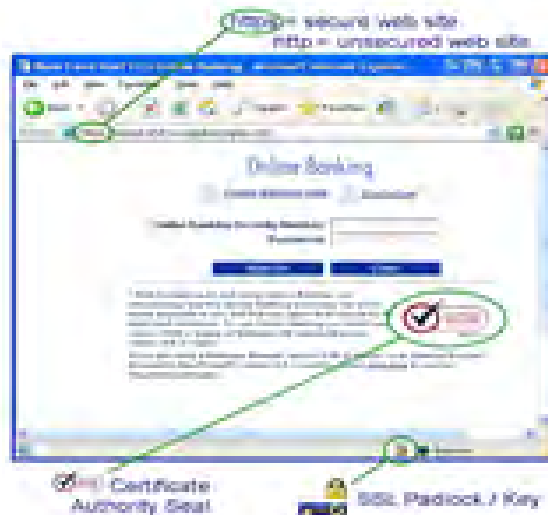
Step 4



"To cast your vote, insert CD in any computer (PC). Then insert smart ID card, scan fingerprint and enter PIN"



Step 5



After user authentication, CD creates secure connection to server using secure web browser that can not accept any URL input.

Step 6



To guarantee vote secrecy, every vote is extended with an arbitrary text before encoding to make the encoding inviolable



Yes-abcdefg-xyz

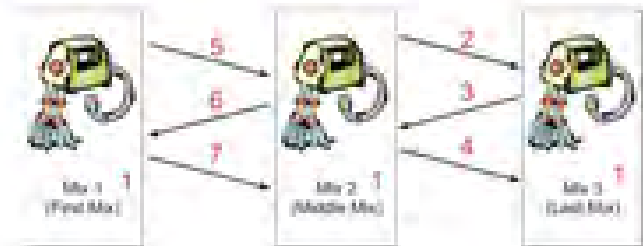
Xcfg-zYax-e-sbe

Internet - Step 1



A combination of three algorithms are used to make the voting process anonymous

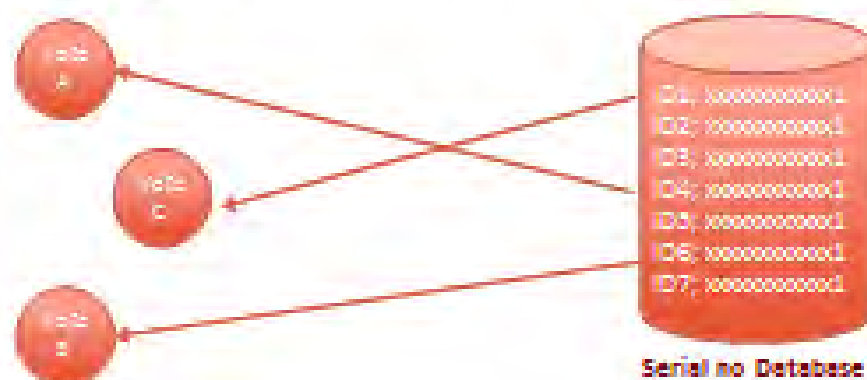
- 1) Blind Signature;
- 2) Mix-net.
- 3) Threshold Encryption



Internet - Step 2



You will be given a unique serial number to track your vote. The serial number has no link with your identity, therefore no trace back is possible



Internet - Step 3



Vote casting - All data transmitted over the Internet are encrypted and digitally signed



Internet - Step 4

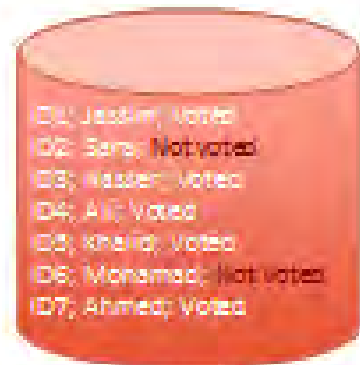


You will be asked to add signatures to your vote. Signature are used in case there is an appeal.



Internet - Step 5

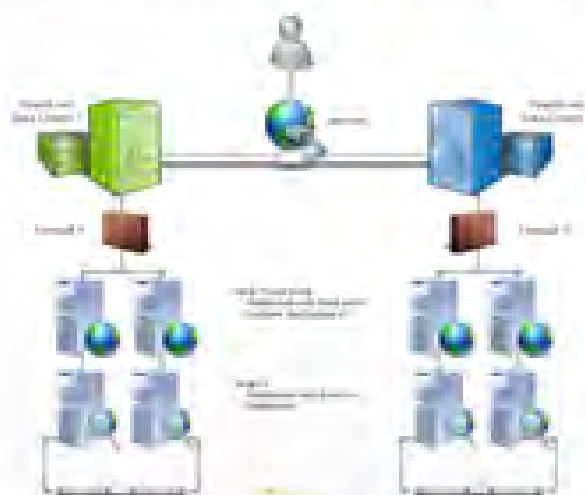
After the voting process is completed, you will be flagged on the database as "Already voted"



Voter Database

Server - Step 1

High availability solution using duplicate servers

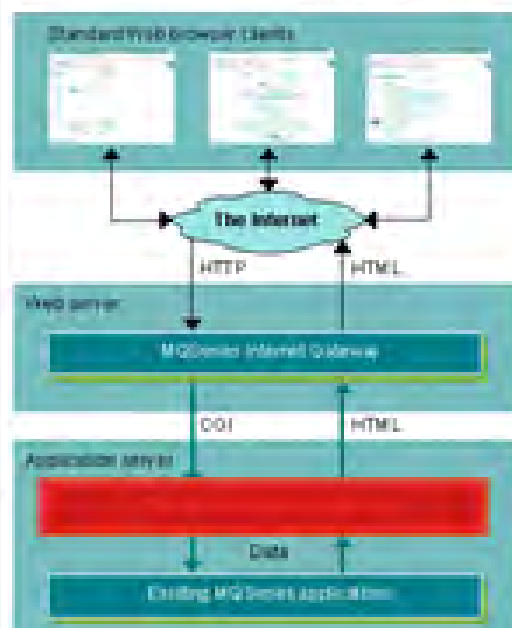


ALL server has been
hardened and
optimized

Server - Step 2

- Physically secure: The servers are installed in the safest computer room in the MOI headquarters.
- Access to this room is regulated by the police rules.
- Only a small number of officers are authorized for access the server, and never alone.
- Network access is limited to a single entry via a dedicated optical fibre which is the only link to the web. This is only activated during the election.

Server - Step 3



IBM Message Queuing (MQ) is used to ensure that no vote is lost.

Even if you loose the connection to the website, MQ will hold your session for 30 min to allow you to reconnect

Server - Step 3



Solving the problem of a fake website

The domain names server (DNS) update is carried out at an increased frequency, refreshing every few minutes instead of every few days. Any attempt to divert your connection to a fake website will be immediately discovered and countered.

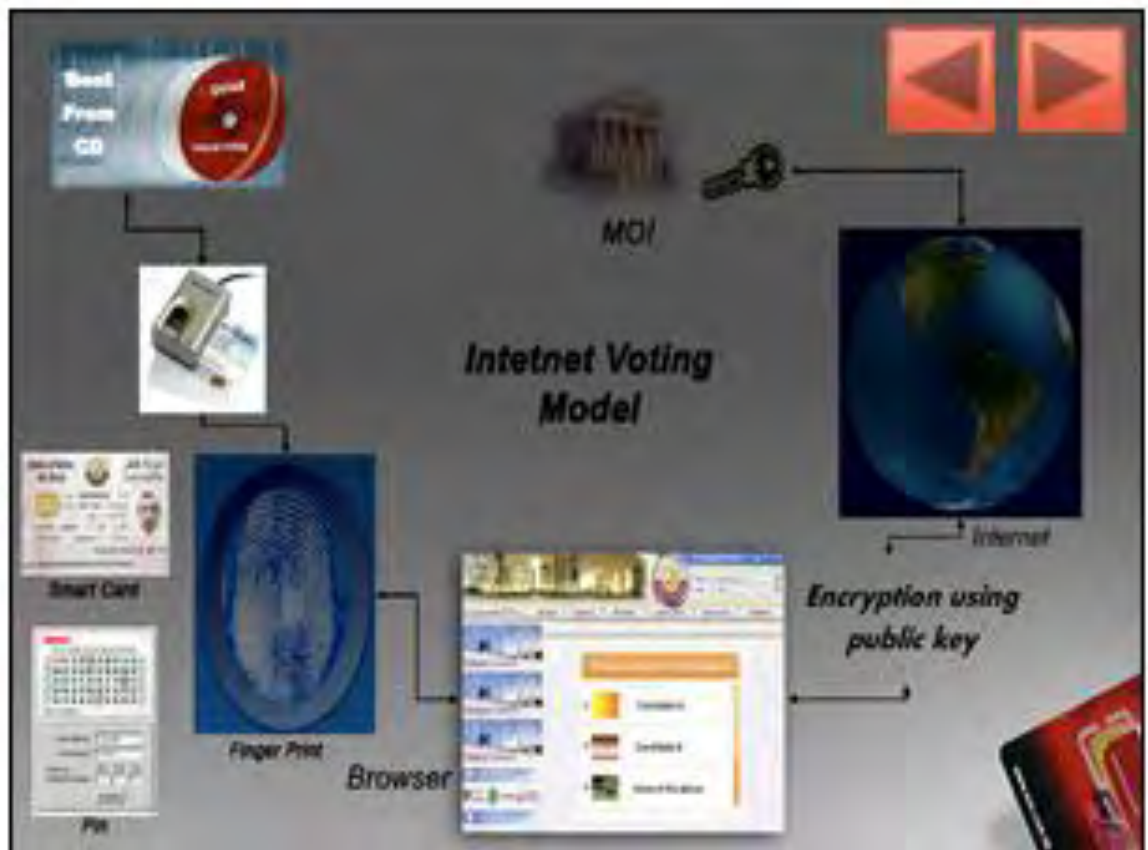
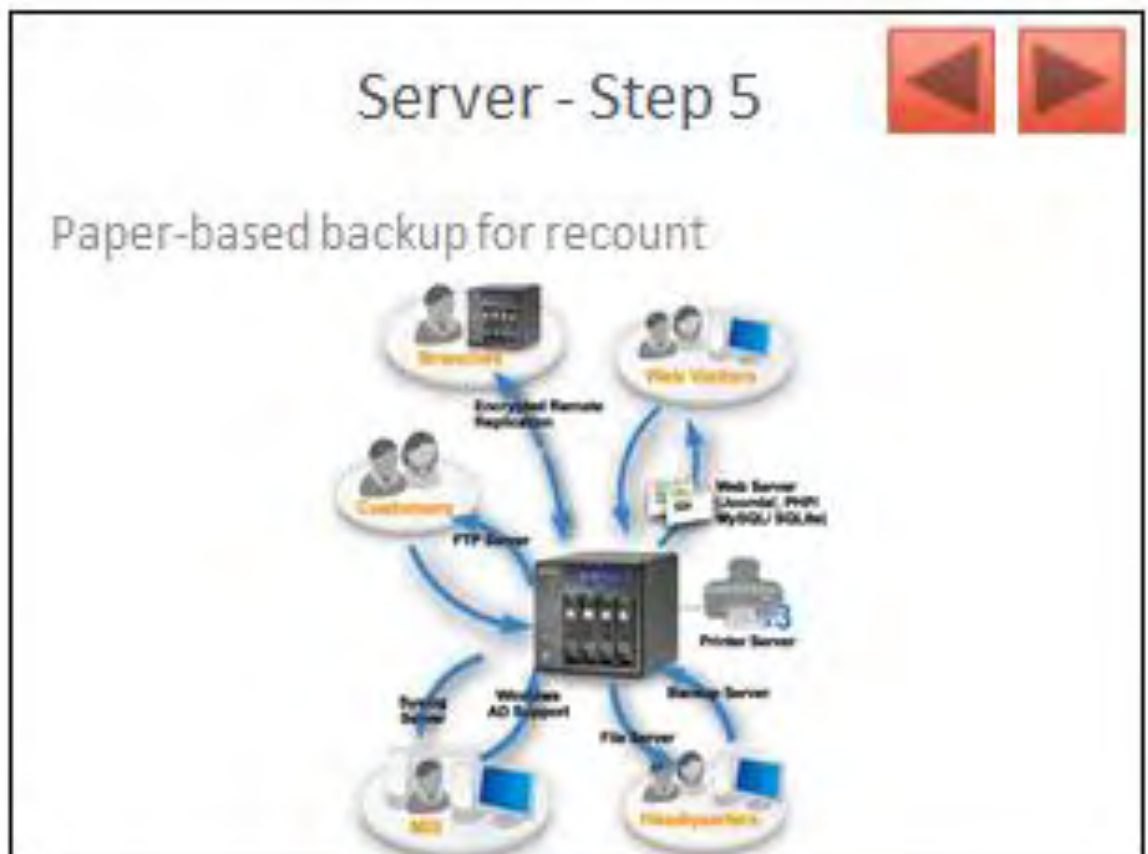


Server - Step 4



24h Network monitoring team to prevent any attack

- ☑ The same IP address requests the same page too often;
- ☑ Systematic attempts at identification are noticed;
- ☑ Abnormal and unexpected requests on certain pages are made;
- ☑ Equipment breaks down (servers, disc system, firewall, network);
- ☑ The software stops working (database);
- ☑ Abnormal modification of a file system is noticed;



D4 Evaluation of the Model

D4.1 Questionnaire sheet

Proposed I-voting model

Section 1 – Demographics

Q1: What is your age?

18 – 24

25 – 29

30 – 39

50 – 59

60 – 64

65+

Q2: What is your gender?

Male

Female

Q3: Please state how long you have been using the Internet:

Never

Less than one year

1 – 2 years

Over 2 years

Q4: How strongly do you agree or disagree with the following statements about Internet safeguard?

	Strongly agree	Agree	neutral	Disagree
The internet has sufficient safeguards and robustness to make me feel comfortable using it to transact personal business				
I feel concerned about the legal aspects of I-voting				
I feel confident that encryption and other technological advances on the Internet make it safe for me to do Internet voting				

Q5: How strongly do you agree or disagree with the following

	Strongly agree	Agree	neutral	Disagree
I am very comfortable using Internet voting facilities				
I believe government are providing adequate security for their online services				
I am comfortable using password protected internet voting				
Overall, I believe that Internet voting is a good idea				

Q6: How strongly do you agree or disagree with the following

	Strongly agree	Agree	neutral	Disagree
I could use the internet voting system if I had only the system manuals for reference				
I could use the internet voting system if I had seen someone else using it before trying it myself				
I could use the internet voting system if I could call someone for help when I got stuck				

Q7: How strongly do you agree or disagree with the following statements about general security practice?

	Strongly agree	Agree	natural	Disagree
I am aware of the dangers of phishing				
I support the use of national ID cards to participate in I-voting				
I would vote over the internet even if it required to install software or use CD				

Q8: How strongly do you agree or disagree with the following statements about general awareness of I-voting security issues?

	Strongly agree	Agree	natural	Disagree
I would feel more confident and secure about Internet Voting security if I owned my own fingerprint checking and ID card reader device				
Overall, I have no concerns about the security of Internet Voting				
I would not feel comfortable using I-voting unless fingerprint checking or other biometrics were used to check my identity				
I fear that my biometric information might be stolen if used for Internet Voting				

Q9: How strongly do you agree or disagree with the following statements about usefulness?

	Strongly agree	Agree	natural	Disagree
I understand how the proposed voting system works				
Using I-voting will improve the overall quality of voting service				
I find I-voting to be more convenient				
I would be willing to use the proposed system for Internet voting				

Q10: How strongly do you agree or disagree with the following statements about Comparison of the system to the process it replace?

	Strongly agree	Agree	natural	Disagree
The proposed I-voting system would be easier to use compared to the existing Voting systems with which I am familiar				
The proposed I-voting system would be faster compared to the existing voting systems with which I am familiar				
The proposed system would be more secure compared to the existing voting systems with which I am familiar				

Q11: How strongly do you agree or disagree with the following statements about overall views to the system?

	Strongly agree	Agree	natural	Disagree
I think Internet voting would be of benefit to me				
I think Internet voting would be of benefit to some other people				

Overall, my attitude towards Internet voting is favourable				
--	--	--	--	--

D4.2 Sample of completed questionnaire

Proposed I-voting model

Q1: What is your age?				
18 – 24	25 – 29	30 – 39	50 – 59	60 – 64
	2			
Q2: What is your gender?				
Male		Female		
Q3: Please state how long you have been using the Internet:				
Never	Less than one year	1 – 2 years	Over 2 years	
Q4: How strongly do you agree or disagree with the following statements about Internet safeguard?				
	Strongly agree	Agree	natural	Disagree
The internet has sufficient safeguards and robustness to make me feel comfortable using it to transact personal business	✓			
I feel concerned about the legal aspects of I-voting		✓		
I feel confident that encryption and other technological advances on the Internet make it safe for me to do Internet voting	✓			
Q5: How strongly do you agree or disagree with the following				
	Strongly agree	Agree	natural	Disagree
I am very comfortable using Internet voting facilities				
I believe government are providing adequate security for their online services	✓			
I am comfortable using password protected internet voting		✓		
Overall, I believe that Internet voting is a good idea	✓			
Q6: How strongly do you agree or disagree with the following				
	Strongly agree	Agree	natural	Disagree
I could use the internet voting system if I had only the system manuals for reference		✓		
I could use the internet voting system if I had seen someone else using it before trying it myself		✓		
I could use the internet voting system if I could call someone for help when I got stuck	✓			
Q7: How strongly do you agree or disagree with the following statements about general security practice?				
	Strongly agree	Agree	natural	Disagree
I am aware of the dangers of phishing				
I support the use of national ID cards to participate in I-voting			✓	

I would vote over the internet even if it required to install software or use CD			✓	
--	--	--	---	--

Q8: How strongly do you agree or disagree with the following statements about general awareness of I-voting security issues?

	Strongly agree	Agree	natural	Disagree
I would feel more confident and secure about Internet Voting security if I owned my own fingerprint checking and ID card reader device	✓			
Overall, I have no concerns about the security of Internet Voting		✓		
I would not feel comfortable using I-voting unless fingerprint checking or other biometrics were used to check my identity	✓			
I fear that my biometric information might be stolen if used for Internet Voting	✓			

Q9: How strongly do you agree or disagree with the following statements about usefulness?

	Strongly agree	Agree	natural	Disagree
I understand how the proposed voting system works				
Using I-voting will improve the overall quality of voting service	✓			
I find I-voting to be more convenient		✓		
I would be willing to use the proposed system for Internet voting			✓	

Q10: How strongly do you agree or disagree with the following statements about Comparison of the system to the process it replace?

	Strongly agree	Agree	natural	Disagree
The proposed I-voting system would be easier to use compared to the existing Voting systems with which I am familiar		✓		
The proposed I-voting system would be faster compared to the existing voting systems with which I am familiar		✓		
The proposed system would be more secure compared to the existing voting systems with which I am familiar		✓		

Q11: How strongly do you agree or disagree with the following statements about overall views to the system?

	Strongly agree	Agree	natural	Disagree
I think Internet voting would be of benefit to me		✓		
I think Internet voting would be of benefit to some other people			✓	
Overall, my attitude towards Internet voting is favourable			✓	

Proposed I-voting model

Q1: What is your age?

18 – 24

25 – 29

30 – 39

50 – 59

60 – 64

65+

Q2: What is your gender?

Male

Female

Q3: Please state how long you have been using the Internet:

Never

Less than one year

1 – 2 years

Over 2 years

Q4: How strongly do you agree or disagree with the following statements about Internet safeguard?

	Strongly agree	Agree	natural	Disagree
The internet has sufficient safeguards and robustness to make me feel comfortable using it to transact personal business		—		
I feel concerned about the legal aspects of I-voting		—		
I feel confident that encryption and other technological advances on the Internet make it safe for me to do Internet voting	—			

Q5: How strongly do you agree or disagree with the following

	Strongly agree	Agree	natural	Disagree
I am very comfortable using Internet voting facilities				
I believe government are providing adequate security for their online services	—			
I am comfortable using password protected internet voting		—		
Overall, I believe that Internet voting is a good idea			—	

Q6: How strongly do you agree or disagree with the following

	Strongly agree	Agree	natural	Disagree
I could use the internet voting system if I had only the system manuals for reference			—	
I could use the internet voting system if I had seen someone else using it before trying it myself		—		
I could use the internet voting system if I could call someone for help when I got stuck		—		

Q7: How strongly do you agree or disagree with the following statements about general security practice?

	Strongly agree	Agree	natural	Disagree
I am aware of the dangers of phishing				
I support the use of national ID cards to participate in I-voting	—			

I would vote over the internet even if it required to install software or use CD			—	
--	--	--	---	--

Q8: How strongly do you agree or disagree with the following statements about general awareness of I-voting security issues?

	Strongly agree	Agree	natural	Disagree
I would feel more confident and secure about Internet Voting security if I owned my own fingerprint checking and ID card reader device			—	
Overall, I have no concerns about the security of Internet Voting			—	
I would not feel comfortable using I-voting unless fingerprint checking or other biometrics were used to check my identity		—		
I fear that my biometric information might be stolen if used for Internet Voting		—		

Q9: How strongly do you agree or disagree with the following statements about usefulness?

	Strongly agree	Agree	natural	Disagree
I understand how the proposed voting system works				
Using I-voting will improve the overall quality of voting service			—	
I find I-voting to be more convenient	—			
I would be willing to use the proposed system for Internet voting	—			

Q10: How strongly do you agree or disagree with the following statements about Comparison of the system to the process it replace?

	Strongly agree	Agree	natural	Disagree
The proposed I-voting system would be easier to use compared to the existing Voting systems with which I am familiar	—			
The proposed I-voting system would be faster compared to the existing voting systems with which I am familiar	—			
The proposed system would be more secure compared to the existing voting systems with which I am familiar	—			

Q11: How strongly do you agree or disagree with the following statements about overall views to the system?

	Strongly agree	Agree	natural	Disagree
I think Internet voting would be of benefit to me			—	
I think Internet voting would be of benefit to some other people		—		
Overall, my attitude towards Internet voting is favourable		—		

D4.3 Questionnaire results

Q1: Gender

Male	70
female	30

Q2: Age

18-29	40
30-39	29
40-49	27
Above 50	4
	100

Q3: how long you have been using the Internet:

Never	15
Less than one year	0
1-2 years	5
Over 2 years	80
	100

Q4: How strongly do you agree or disagree with the following statements about Internet safeguard?

	Strongly agree	Agree	natural	Disagree
The internet has sufficient safeguards and robustness to make me feel comfortable using it to transact personal business	11	16	13	60
I feel concerned about the legal aspects of I-voting	4	11	15	70
I feel confident that encryption and other technological advances on the Internet make it safe for me to do Internet voting	2	8	27	63

Q5: How strongly do you agree or disagree with the following

	Strongly agree	Agree	natural	Disagree
I am very comfortable using Internet voting facilities	9	8	11	72
I believe government are providing adequate security for their online services	2	7	15	76
I am comfortable using password protected internet voting	40	23	18	19
Overall, I believe that Internet voting is a good idea	8	7	9	76

Q6: How strongly do you agree or disagree with the following

	Strongly agree	Agree	natural	Disagree
I could use the internet voting system if I had only the system manuals for reference	37	28	20	15
I could use the internet voting system if I had seen someone else using it before trying it myself	6	14	20	60
I could use the internet voting system if I could call someone for help when I got stuck	6	12	21	61

Q7: How strongly do you agree or disagree with the following statements about general security practice?

	Strongly agree	Agree	neutral	Disagree
I am aware of the dangers of phishing	7	6	7	80
I support the use of national ID cards to participate in I-voting	3	13	16	68
I would vote over the internet even if it required to install software or use CD	7	13	20	60

Q8: How strongly do you agree or disagree with the following statements about general awareness of I-voting security issues?

	Strongly agree	Agree	neutral	Disagree
I would feel more confident and secure about Internet Voting security if I owned my own fingerprint checking and ID card reader device	2	8	17	73
Overall, I have no concerns about the security of Internet Voting	4	10	11	75
I would not feel comfortable using I-voting unless fingerprint checking or other biometrics were used to check my identity	7	9	14	70
I fear that my biometric information might be stolen if used for Internet Voting	17	26	32	25

Q9: How strongly do you agree or disagree with the following statements about usefulness?

	Strongly agree	Agree	neutral	Disagree
I understand how the proposed voting system works	3	5	9	83
Using I-voting will improve the overall quality of voting service	3	12	10	75
I find I-voting to be more convenient	5	8	18	69
I would be willing to use the proposed system for Internet voting	6	11	23	60

Q10: How strongly do you agree or disagree with the following statements about Comparison of the system to the process it replace?

	Strongly agree	Agree	neutral	Disagree
The proposed I-voting system would be easier to use compared to the existing Voting systems with which I am familiar	7	16	17	60
The proposed I-voting system would be faster compared to the existing voting systems with which I am familiar	8	16	19	57
The proposed system would be more secure compared to the existing voting systems with which I am familiar	14	11	16	59

Q11: How strongly do you agree or disagree with the following statements about

overall views to the system?

	Strongly agree	Agree	neutral	Disagree
I think Internet voting would be of benefit to me	7	9	15	69
I think Internet voting would be of benefit to some other people	9	9	12	70
Overall, my attitude towards Internet voting is favourable	3	5	11	81

Correlation test

Chi-squared test were applied to measure the significance between survey variables, there were potential relationships between the following variables:

Variable	Related with
Internet experience	All variables
The internet has sufficient safeguards and robustness	<ul style="list-style-type: none"> I feel confident that encryption and other technological advances on the Internet make it safe for me to do Internet voting I believe government are providing adequate security for their online services I am comfortable using password protected Internet voting I could use the Internet voting system if I had only the system manuals for reference I am aware of the dangers of phishing I would feel more confident and secure about Internet Voting security if I owned my own fingerprint checking and ID card reader device I fear that my biometric information might be stolen if used for Internet Voting I understand how the proposed voting system works Overall, my attitude towards Internet voting is favourable
I feel concerned	<ul style="list-style-type: none"> I am comfortable using password protected Internet voting I could use the Internet voting system if I had only the system

about the legal aspects of I-voting	<p>manuals for reference</p> <ul style="list-style-type: none"> • I fear that my biometric information might be stolen if used for Internet Voting
I feel confident that encryption and other technological advances on the Internet make it safe for me to do Internet voting	<ul style="list-style-type: none"> • The Internet has sufficient safeguards and robustness to make me feel comfortable using it to transact personal business • I could use the Internet voting system if I had only the system manuals for reference • I am aware of the dangers of phishing • Overall, I have no concerns about the security of Internet Voting • I fear that my biometric information might be stolen if used for Internet Voting • I understand how the proposed voting system works • Using I-voting will improve the overall quality of voting service • The proposed system would be more secure compared to the existing voting systems with which I am familiar • I think Internet voting would be of benefit to some other people • Overall, my attitude towards Internet voting is favourable
I am very comfortable using Internet voting facilities	<ul style="list-style-type: none"> • I feel confident that encryption and other technological advances on the Internet make it safe for me to do Internet voting • I am comfortable using password protected Internet voting • I could use the Internet voting system if I had only the system manuals for reference • I fear that my biometric information might be stolen if used for Internet Voting
I believe government are providing adequate security for	<ul style="list-style-type: none"> • The Internet has sufficient safeguards and robustness to make me feel comfortable using it to transact personal business • I am comfortable using password protected Internet voting • I could use the Internet voting system if I had only the system

their online services	<p>manuals for reference</p> <ul style="list-style-type: none"> • I fear that my biometric information might be stolen if used for Internet Voting • The proposed I-voting system would be easier to use compared to the existing Voting systems with which I am familiar • The proposed I-voting system would be faster compared to the existing voting systems with which I am familiar • The proposed system would be more secure compared to the existing voting systems with which I am familiar
I am comfortable using password protected Internet voting	All variables except I could use the Internet voting system if I had only the system manuals for reference
Overall, I believe that Internet voting is a good idea	<ul style="list-style-type: none"> • I feel confident that encryption and other technological advances on the Internet make it safe for me to do Internet voting • I am comfortable using password protected Internet voting • I could use the Internet voting system if I had only the system manuals for reference • I could use the Internet voting system if I had seen someone else using it before trying it myself • I could use the Internet voting system if I could call someone for help when I got stuck • I fear that my biometric information might be stolen if used for Internet Voting • I would be willing to use the proposed system for Internet voting • The proposed I-voting system would be faster compared to the existing voting systems with which I am familiar

I could use the Internet voting system if I had only the system manuals for reference	All variable except I am comfortable using password protected Internet voting
I could use the Internet voting system if I had seen someone else using it before trying it myself	<ul style="list-style-type: none"> • I am comfortable using password protected Internet voting • Overall, I believe that Internet voting is a good idea • I could use the Internet voting system if I had only the system manuals for reference • I am aware of the dangers of phishing • I fear that my biometric information might be stolen if used for Internet Voting • I understand how the proposed voting system works • Overall, my attitude towards Internet voting is favourable
I could use the Internet voting system if I could call someone for help when I got stuck	<ul style="list-style-type: none"> • I am comfortable using password protected Internet voting • Overall, I believe that Internet voting is a good idea • I could use the Internet voting system if I had only the system manuals for reference • I am aware of the dangers of phishing • I fear that my biometric information might be stolen if used for Internet Voting • I understand how the proposed voting system works • Overall, my attitude towards Internet voting is favorable
I am aware of the dangers of phishing	<ul style="list-style-type: none"> • The Internet has sufficient safeguards and robustness to make me feel comfortable using it to transact personal business • I feel confident that encryption and other technological advances on the Internet make it safe for me to do Internet voting

	<ul style="list-style-type: none"> • I am comfortable using password protected Internet voting • I could use the Internet voting system if I had only the system manuals for reference • I could use the Internet voting system if I had seen someone else using it before trying it myself • I could use the Internet voting system if I could call someone for help when I got stuck • I support the use of national ID cards to participate in I-voting • I would vote over the Internet even if it required to install software or use CD • I fear that my biometric information might be stolen if used for Internet Voting • I would be willing to use the proposed system for Internet voting • The proposed I-voting system would be easier to use compared to the existing Voting systems with which I am familiar • The proposed I-voting system would be faster compared to the existing voting systems with which I am familiar • The proposed system would be more secure compared to the existing voting systems with which I am familiar
I support the use of national ID cards to participate in I-voting	<ul style="list-style-type: none"> • I am comfortable using password protected Internet voting • I could use the Internet voting system if I had only the system manuals for reference • I am aware of the dangers of phishing • I fear that my biometric information might be stolen if used for Internet Voting
I would vote over the Internet even if it required to install	<ul style="list-style-type: none"> • I am comfortable using password protected Internet voting • I could use the Internet voting system if I had only the system manuals for reference

software or use CD	<ul style="list-style-type: none"> • I am aware of the dangers of phishing • I fear that my biometric information might be stolen if used for Internet Voting • I understand how the proposed voting system works • Overall, my attitude towards Internet voting is favourable
I would feel more confident and secure about Internet Voting security if I owned my own fingerprint checking and ID card reader device	<ul style="list-style-type: none"> • The Internet has sufficient safeguards and robustness to make me feel comfortable using it to transact personal business • I am comfortable using password protected Internet voting • I could use the Internet voting system if I had only the system manuals for reference • I fear that my biometric information might be stolen if used for Internet Voting • The proposed I-voting system would be faster compared to the existing voting systems with which I am familiar • The proposed system would be more secure compared to the existing voting systems with which I am familiar
Overall, I have no concerns about the security of Internet Voting	<ul style="list-style-type: none"> • I feel confident that encryption and other technological advances on the Internet make it safe for me to do Internet voting • I am comfortable using password protected Internet voting • I could use the Internet voting system if I had only the system manuals for reference • I fear that my biometric information might be stolen if used for Internet Voting • The proposed system would be more secure compared to the existing voting systems with which I am familiar
I would not feel comfortable using I-voting unless	<ul style="list-style-type: none"> • I am comfortable using password protected Internet voting • I could use the Internet voting system if I had only the system manuals for reference • I fear that my biometric information might be stolen if used for

fingerprint checking or other biometrics were used to check my identity	Internet Voting
I fear that my biometric information might be stolen if used for Internet Voting	All variables
I understand how the proposed voting system works	<ul style="list-style-type: none"> • The Internet has sufficient safeguards and robustness to make me feel comfortable using it to transact personal business • I feel confident that encryption and other technological advances on the Internet make it safe for me to do Internet voting • I am comfortable using password protected Internet voting • I could use the Internet voting system if I had only the system manuals for reference • I could use the Internet voting system if I had seen someone else using it before trying it myself • I could use the Internet voting system if I could call someone for help when I got stuck • I would vote over the Internet even if it required to install software or use CD • I fear that my biometric information might be stolen if used for Internet Voting • I would be willing to use the proposed system for Internet voting • The proposed I-voting system would be easier to use compared to

	<p>the existing Voting systems with which I am familiar</p> <ul style="list-style-type: none"> • The proposed I-voting system would be faster compared to the existing voting systems with which I am familiar • The proposed system would be more secure compared to the existing voting systems with which I am familiar
Using I-voting will improve the overall quality of voting service	<ul style="list-style-type: none"> • I feel confident that encryption and other technological advances on the Internet make it safe for me to do Internet voting • I am comfortable using password protected Internet voting • I could use the Internet voting system if I had only the system manuals for reference • I fear that my biometric information might be stolen if used for Internet Voting • The proposed I-voting system would be faster compared to the existing voting systems with which I am familiar • The proposed system would be more secure compared to the existing voting systems with which I am familiar
I find I-voting to be more convenient	<ul style="list-style-type: none"> • I am comfortable using password protected Internet voting • I could use the Internet voting system if I had only the system manuals for reference • I fear that my biometric information might be stolen if used for Internet Voting
I would be willing to use the proposed system for Internet voting	<ul style="list-style-type: none"> • I am comfortable using password protected Internet voting • Overall, I believe that Internet voting is a good idea • I could use the Internet voting system if I had only the system manuals for reference • I am aware of the dangers of phishing • I fear that my biometric information might be stolen if used for Internet Voting

	<ul style="list-style-type: none"> • I understand how the proposed voting system works • Overall, my attitude towards Internet voting is favourable
The proposed I-voting system would be easier to use compared to the existing Voting systems with which I am familiar	<ul style="list-style-type: none"> • I believe government are providing adequate security for their online services • I am comfortable using password protected Internet voting • I could use the Internet voting system if I had only the system manuals for reference • I am aware of the dangers of phishing • I fear that my biometric information might be stolen if used for Internet Voting • I understand how the proposed voting system works • Overall, my attitude towards Internet voting is favourable
The proposed I-voting system would be faster compared to the existing voting systems with which I am familiar	<ul style="list-style-type: none"> • I believe government are providing adequate security for their online services • I am comfortable using password protected Internet voting • Overall, I believe that Internet voting is a good idea • I could use the Internet voting system if I had only the system manuals for reference • I am aware of the dangers of phishing • I would feel more confident and secure about Internet Voting security if I owned my own fingerprint checking and ID card reader device • I fear that my biometric information might be stolen if used for Internet Voting • I understand how the proposed voting system works • Using I-voting will improve the overall quality of voting service • Overall, my attitude towards Internet voting is favourable
The proposed system would	<ul style="list-style-type: none"> • I feel confident that encryption and other technological advances on the Internet make it safe for me to do Internet voting

be more secure compared to the existing voting systems with which I am familiar	<ul style="list-style-type: none"> • I believe government are providing adequate security for their online services • I am comfortable using password protected Internet voting • I could use the Internet voting system if I had only the system manuals for reference • I am aware of the dangers of phishing • I would feel more confident and secure about Internet Voting security if I owned my own fingerprint checking and ID card reader device • Overall, I have no concerns about the security of Internet Voting • I fear that my biometric information might be stolen if used for Internet Voting • I understand how the proposed voting system works • Using I-voting will improve the overall quality of voting service • Overall, my attitude towards Internet voting is favourable
I think Internet voting would be of benefit to me	<ul style="list-style-type: none"> • I am comfortable using password protected Internet voting • I could use the Internet voting system if I had only the system manuals for reference • I fear that my biometric information might be stolen if used for Internet Voting
I think Internet voting would be of benefit to some other people	<ul style="list-style-type: none"> • I feel confident that encryption and other technological advances on the Internet make it safe for me to do Internet voting • I am comfortable using password protected Internet voting • I could use the Internet voting system if I had only the system manuals for reference • I fear that my biometric information might be stolen if used for Internet Voting
Overall, my attitude towards	<ul style="list-style-type: none"> • The Internet has sufficient safeguards and robustness to make me feel comfortable using it to transact personal business

Internet voting is favourable	<ul style="list-style-type: none"> • I feel confident that encryption and other technological advances on the Internet make it safe for me to do Internet voting • I am comfortable using password protected Internet voting • I could use the Internet voting system if I had only the system manuals for reference • I could use the Internet voting system if I had seen someone else using it before trying it myself • I could use the Internet voting system if I could call someone for help when I got stuck • I would vote over the Internet even if it required to install software or use CD • I fear that my biometric information might be stolen if used for Internet Voting • I would be willing to use the proposed system for Internet voting • The proposed I-voting system would be easier to use compared to the existing Voting systems with which I am familiar • The proposed I-voting system would be faster compared to the existing voting systems with which I am familiar • The proposed system would be more secure compared to the existing voting systems with which I am familiar
-------------------------------	--

Appendix E: Recommendations

E1 Consent Form

CERTIFICATION BY PARTICIPANT

I, certify that I am voluntarily giving my consent to provide information for the above described project entitled: **Introduce I-voting in the State of Qatar**, being conducted at Loughborough University, UK by: Mr. Jassim AL-Hamar.

I certify that I have agreed to be interviewed in the subject of as previously explained by Mr. Jassim AL-Hamar and that that I freely consent to participate in this project. I have had the opportunity to have any questions answered, I have been fully explained the procedures of interview and that information gathered will be only used for the benefit of the entitled research and will be confidential and kept strictly private.

Signed:

Date:

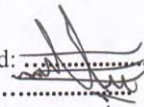
For any queries about the research topic please don't hesitate to contact the researcher (Name: Mr. Jassim AL-Hamar, ph. +97455558105, E-mail: j.alhamar@hotmail.com).

E2 Example of signed Consent Form

CERTIFICATION BY PARTICIPANT

I, certify that I am voluntarily giving my consent to provide information for the above described project entitled: **Introduce I-voting in the State of Qatar**, being conducted at Loughborough University, UK by: Mr. Jassim AL-Hamar.

I certify that I have agreed to be interviewed in the subject of as previously explained by Mr. Jassim AL-Hamar and that that I freely consent to participate in this project. I have had the opportunity to have any questions answered, I have been fully explained the procedures of interview and that information gathered will be only used for the benefit of the entitled research and will be confidential and kept strictly private.

Signed: 

Date:

For any queries about the research topic please don't hesitate to contact the researcher (Name: Mr. Jassim AL-Hamar, ph. +97455558105, E-mail: j.alhamar@hotmail.com).

CERTIFICATION BY PARTICIPANT

I, certify that I am voluntarily giving my consent to provide information for the above described project entitled: **Introduce I-voting in the State of Qatar**, being conducted at Loughborough University, UK by: Mr. Jassim AL-Hamar.

I certify that I have agreed to be interviewed in the subject of as previously explained by Mr. Jassim AL-Hamar and that that I freely consent to participate in this project. I have had the opportunity to have any questions answered, I have been fully explained the procedures of interview and that information gathered will be only used for the benefit of the entitled research and will be confidential and kept strictly private.

Signed: 


Date:

For any queries about the research topic please don't hesitate to contact the researcher (Name: Mr. Jassim AL-Hamar, ph. +97455558105, E-mail: j.alhamar@hotmail.com).

CERTIFICATION BY PARTICIPANT

I, certify that I am voluntarily giving my consent to provide information for the above described project entitled: **Introduce I-voting in the State of Qatar**, being conducted at Loughborough University, UK by: Mr. Jassim AL-Hamar.

I certify that I have agreed to be interviewed in the subject of as previously explained by Mr. Jassim AL-Hamar and that that I freely consent to participate in this project. I have had the opportunity to have any questions answered, I have been fully explained the procedures of interview and that information gathered will be only used for the benefit of the entitled research and will be confidential and kept strictly private.

Signed: 
Date:

For any queries about the research topic please don't hesitate to contact the researcher
(Name: Mr. Jassim AL-Hamar, ph. +97455558105, E-mail: j.alhamar@hotmail.com).

E3 Recommendation evaluation

Five evaluators were gathered from different organisations in Qatar from the Ministry of Interior (MOI), ictQATAR, election committee, Qtel and the Supreme Judiciary Council. The interviewees were as follows:

1. Hassan Al-Sayed, Gov. IT Platform Manager, ictQATAR
2. Abdul Rahman Al-Sulaiti, Assistant Director of Elections Department, MOI
3. Mohanad alabad, Internet security consultant, MOI
4. Jassim Alswadi, Head of ISP, Qtel
5. Mohamad Alobaidli, Judge participating in election monitoring, Supreme Judiciary Council (SJC)

Each evaluator were asked the following Interview questions:

- Q1. Do you believe the researcher's recommendations will be effective for introducing I-voting in Qatar?
- Q2. After reading the recommendations, would you encourage Qatar to introduce I-voting?
- Q3. Do you find that the recommendations satisfy voting principles (security, privacy, transparency, etc.)?
- Q4. Do you think the recommendations could help to increase voting turnout?
- Q5. Do you think the recommendations on the legal aspects are valuable?
- Q6. Is Qatar ready to introduce I-voting in terms of its infrastructure? And, are the recommendations proposed to enhance infrastructure development significant?

E4 Details of evaluator's interview

Interview 1

Date of interview: 20-Jan- 2011

Duration: Approximately 30 minutes

Interviewee: Hassan Al-Sayed, Gov. IT Platform Manager, ictQATAR

Q1. Do you believe the researcher's recommendations will be effective for introducing I-voting in Qatar?

Yes, of course it is very effective. It is based on in-depth research carried out with experiments, surveys and interviews. It help to introduce I-voting technology in Qatar by providing recommendations to help the uptake of it based on cultural and country-specific factors.

Q2. After reading the recommendations, would you encourage Qatar to introduce I-voting?

Yes, I do encourage to have I-voting technology in Qatar since it will provide flexibility to voters and will facilitate the election process were everything is done electronically and vote count is automatically calculated. However, I still think there is a need for more trials and experiments on I-voting to ensure that it fulfil voting principles. It must be considered that I-voting is highly dependent on political, social and economic situation of a state.

Q3. Do you find that the recommendations satisfy voting principles (security, privacy, transparency, etc.)?

Yes, it will help to satisfy voting principles it is was applied effectively. However, there ius a need to consider the possible threats and attacks that might encounter I-voting and therefore provide a team of expert to handle possible threats. I still think it is imposible to achieve 100% of security with nowadays improving computer power.

Q4. Do you think the recommendations could help to increase voting turnout?

I could help voting turnout, this is hard to know. We only can know whether there is an increase in participation once I-voting is applied in practice. People acceptance is a critical factor which

could increase participation, therefore the government should work on how to enhance people acceptance and encourage them to use such new technology.

Q5. Do you think the recommendations on the legal aspects are valuable?

Yes, they are. I agree on the need to review the current election law and modify it to adapt I-voting by adding sections for appeal process to recount votes, effective actions to prevent vote selling and process for vote verification. Also the current E-law should help the uptake of I-voting.

Q6. Is Qatar ready to introduce I-voting in terms of its infrastructure? And, are the recommendations proposed to enhance infrastructure development significant?

Yes, it is ready for I-voting. The e-government project have assisted in improving the telecommunication infrastructure. Therefore, introducing I-voting could use the same infrastructure, with taking account to provide telecommunications in under-served areas to ensure all voters could vote through the system. Furthermore, there is a critical need for a clear plan to ensure an effective infrastructure for I-voting, this plan should be developed by the government and companies responsible to ensure information security.

Interview 2

Date of interview: 26-Jan- 2011

Duration: Approximately 40 minutes

Interviewees: Abdul Rahman Al-Sulaiti, Assistant Director of Elections Department, MOI and Mohanad alabad, Internet security consultant, MOI

Q1. Do you believe the researcher's recommendations will be effective for introducing I-voting in Qatar?

I like the drive of your recommendations, it seems to be well-structured and valuable. Those recommendations are effective to uptake I-voting in Qatar.

Q2. After reading the recommendations, would you encourage Qatar to introduce I-voting?

Yes, I-voting can exist in Qatar. I believe I-voting will enhance the political agenda. Many countries do introduce I-voting and it was effective, however I must mention as well that other

counties were have a negative experience with I-voting, where it encounter many issues with regard to ensuring security, privacy and transparency of votes. Therefore, to avoid that happening in Qatar, more experiments should be held to test the reliability of I-voting in practice since each country has its own factors that has to be addressed in their voting system.

Q3. Do you find that the recommendations satisfy voting principles (security, privacy, transparency, etc.)?

Yes, it satisfies voting principles including security, privacy and transparency. However, it need to put into practice to ensure that those recommendations would work effectively and efficiently in the real world and that it would get people acceptance and therefore increase voter participation.

Q4. Do you think the recommendations could help to increase voting turnout?

Yes it could if it was implemented successfully taking into account country specific factors and cultural considerations. If I-voting has satisfied voters and get their acceptance voting turnout could increase.

Q5. Do you think the recommendations on the legal aspects are valuable?

Yes, there are effective. However, I think a team of experts in law and information technology should work together to update the current election law to help the uptake of I-voting. Also there are some terms should be considered such as vote selling, verification and appeal process in I-voting.

Q6. Is Qatar ready to introduce I-voting in terms of its infrastructure? And, are the recommendations proposed to enhance infrastructure development significant?

Yes, it is ready enough. The initiative of E-government, smart card and ipark with a great development in telecommunication sector could assist the introduction of I-voting in Qatar. However, I suggest introducing a supervised I-voting in polling stations, so that Qataris would be familiar with using such new technology. This would act as a test for the effectiveness of such system in Qatar and the possible barriers that might be encountered in real life.

Interview 3

Date of interview: 23-Jan- 2011

Duration: Approximately 20 minutes

Interviewee: Jassim Alswadi, Head of ISP, Qtel

Q1. Do you believe the researcher's recommendations will be effective for introducing I-voting in Qatar?

Yes, the recommendations were very valuable, I like the way it is driven and showing from where it was established based on earlier chapter of the research. It well defined and very clear. I think if it was applied effectively, it would help the introduction of I-voting in Qatar. It must be noted that there is a need to ensure that the I-voting system is connected to the election server for defining a secure and trusted system.

Q2. After reading the recommendations, would you encourage Qatar to introduce I-voting?

I encourage the uptake of I-voting in Qatar especially that many counties have already adapt it in their election process. But it must be considered that there are possible technical and non-technical issues might arise from I-voting system. Those issues has led some countries such as USA and UK to stop going further in developing I-voting.

Q3. Do you find that the recommendations satisfy voting principles (security, privacy, transparency, etc.)?

Yes. Those recommendation could simplify the voting process for both voters and election committees and ensure that voting principles are achieved sine it is based on best practices and solutions that are tested in literature such as mix netting and blind signature. However, there are some political concerns on security, anonymity and privacy of I-voting. Therefore, those recommendation should be put into practice in real world to ensure their fulfilment to voting principles and gain trust of government.

Q4. Do you think the recommendations could help to increase voting turnout?

Yes, it could if it was applied successfully based on a solid infrastructure. But this is a testable factor that which only can be approved in reality.

Q5. Do you think the recommendations on the legal aspects are valuable?

Yes, I think they are valuable. There is a need for efforts on establishing a law that support I-voting and help the uptake of it. This would be a long process which need approvals and involvement of experts in law and IT.

Q6. Is Qatar ready to introduce I-voting in terms of its infrastructure? And, are the recommendations proposed to enhance infrastructure development significant?

Yes, the infrastructure is there, only few enhancements might be required to ensure that it is capable to introduce an effective and reliable I-voting system. Furthermore, I-voting should come with proper hardware to facilitate a reliable connection between the user and the election server.

Interview 4

Date of interview: 21-Jan- 2011

Duration: Approximately 30 minutes

Interviewee: Mohamad Alobaidli, Judge participating in election monitoring, Supreme Judiciary Council (SJC)

Q1. Do you believe the researcher's recommendations will be effective for introducing I-voting in Qatar?

Yes, they are effective if applied efficiently and if there were effective cooperation between responsible parties to take up those recommendations. I think I-voting will boost the political agenda but also I do not encourage it since it hard to gain political approval for using such system in Qatar with a risk of affecting citizens' confidence in the government due to many impact associated to such system.

Q2. After reading the recommendations, would you encourage Qatar to introduce I-voting?

I do not encourage the introduction of I-voting in Qatar since it will miss voting experience, and most people would find difficulties in using it. Also worldwide experience of I-voting shows that there are many issues associated to I-voting such as security, privacy and transparency. I suggest the government have to be careful before making their decision on introducing I-voting. A procedures and experiment should be held to ensure the effective of such voting system for Qatar elections in the future, taking into considerations its possible impacts.

Q3. Do you find that the recommendations satisfy voting principles (security, privacy, transparency, etc.)?

Yes, I think. but I can not provide a fair judgment on those recommendations as it is not my expertise. But it shows clearly that it was well defined based on a depth research in the field.

Q4. Do you think the recommendations could help to increase voting turnout?

Yes, if the digital and social divide were encountered effectively voting turnout could be increased. The government could enhance the turnout by taking into account to educate people on I-voting and how to use it efficiently.

Q5. Do you think the recommendations on the legal aspects are valuable?

Yes, I have read them carefully. Although there are very general but they provide some valuable procedures for experts in law to take up and investigate further. I do think the current election law could be support the introduction of I-voting. I think developing a separate section for I-voting which would handle all of the regulation and laws related to I-voting such as verification and appealing process making sure that possible issues are addressed alongside with the current E-law. This need an approval from the government and an involvement of a team of experts in law and IT filed to establish a legal approval for I-voting.

Q6. Is Qatar ready to introduce I-voting in terms of its infrastructure? And, are the recommendations proposed to enhance infrastructure development significant?

I can't judge in terms of infrastructure, but I believe Qatar is experiencing a huge development in ICT and telecommunication sector that perform a good foundation for initiating I-voting. However, there is need to prove the effectiveness of the proposed I-voting model in ensuring its fulfilment of voting principles in practice and getting acceptance and confidence of Qatari citizens. This is very important to ensure trust of such system.

References

- A Report on the Feasibility of Internet Voting (2000). *California Internet Voting Task Force*. [Online]. Available: <http://www.ss.ca.gov/executive/ivote> [19 July 2009]
- A. Aeby and M. Wiget. (2007) *On-Line Meinungsumfragen*. Diploma thesis. Switzerland University of Applied Sciences
- A. D. Rubin, (2002) Security Considerations for Remote Electronic Voting. *Communication of the ACM*, Vol.45, No.12, pp.39-44
- A. Fujioka, T. Okamoto, and K. Ohta. (1992) A practical secret voting scheme for large scale elections. In J. Seberry and Y. Zheng, editors, *ASIACRYPT'92, Workshop on the Theory and Application of Cryptographic Techniques*, LNCS 718, pp.244-251. Australia: Gold Coast
- A. Fujioka, T. Okamoto, and K. Ohta. (1993) *Advances in Cryptology - AUSCRYPT 1992, practical Secret Voting Scheme for Large Scale Elections*, No.A pp.244-251
- A. Marconi, (2005) *Are we ready for Internet Voting? Technical Report*. Department of Information and Communication Technology (DIT): University of Trento
- Ackermann T. and Soder L. (2002) An overview of wind energy-status 2002, *Renew Sustain Energy Rev*, Vol.6, pp.67-128
- Alexander H. Trechsel. (2007) Internet voting in the March 2007 Parliamentary Elections in Estonia. *Report for the Council of Europe*
- Alvarez, R.M., Hall, T., and Roberts, B. (2007) Military Voting and the Law: Procedural and Technological Solutions to the Ballot Transit Problem. *Fordham Urban Law Journal*. Vol.34, No.3
- Amy, D. (2000) *Behind the Ballot Box: A Citizen's Guide to Voting Systems*. Praeger:

Westport, CT

- Ansolabehere, S., Stewart, C. (2002) *Voting technology and uncounted votes in the United States*. [Online]. Available: www.vote.caltech.edu/reports/residual-vote.pdf [19 July 2009]
- Arab A.H., Driss B.A., Amimeur R. and Lorenzo E, (2001) *Photovoltaic systems sizing for Algeria*. *Solar Energy*, Vol.54, No.2, pp.99-104
- B. Fairweather, S. Rogerson, (2005) Interfaces for electronic voting: focus group evidence, *Electronic Government, an International Journal (EG)*, 2 (4).
- Bahry, L. (1999) Elections in Qatar: a Window of Democracy Opens in the Gulf. *Middle East Policy*. Vol.6, No.4
- Becerra, M., Gupta, A.K. (1999) "Trust within the organization: integrating the trust literature with agency theory and transaction costs economics", *Public Administration Quarterly*, Vol.23, No.2, pp.177-203
- Benaloh J, Tuinstra D. (2004) *Receipt-free secret-ballot elections*. In: *Proceedings of the 26th Annual ACM Symposium on the Theory of Computing, Montréal*. Quebec: Canada
- Bergman, M. (2004) *Record numbers registered and voted in 2002 election*, *Census Bureau Reports*. [Online]. Available: www.census.gov/Press-Release/www/releases/archives/voting [19 July 2009]
- Bhandari, A. (2004) *Is the future in line or online?* [Online]. Available: www.thestar.com/NASApp/cs/ContentServer [19 July 2009]
- Bimber, B (2003) *Campaigning Online: The Internet in U.S. Elections*. New York: Oxford University Press
- Bonetti P., Ravaioli S. and S. Piergallini (2000). The Italian academic community's electronic voting system. *Computer Networks*, Vol.34, pp.851-860
- Bonsor, K. (2004) *"How e-voting will work"*. [Online]. Available: <http://computer.howstuffworks.com/e-voting.htm/> [19 July 2009]

- Bouras, J., Katris, N., & Triantafillou, V. (2003) An Electronic Voting Service to Support Decision-Making in Local Government. *Telematics and Informatics*, Vol 20, pp. 255–274.
- Boutin, P. (2004) *Is e-voting safe? PC World*. [Online]. Available: www.pcworld.com/resource/printable/article/0,aid,115608,00.asp [19 July 2009]
- Brace, K.W. (2004) *Overview of voting equipment usage in the United States: Direct Recording Electronic (DRE) voting*. [Online]. Available: www.electiondataservices.com [19 July 2009]
- Burke, Lynn. (2000) “*The Tangled Web of E-Voting*.” WIRED Magazine. [Online]. Available: <http://www.wired.com/news/politics/0,1283,37050,00.html> [19 June 2008]
- Burkhard Ewert, Nermin Fazlic, and Johannes Kollbeck. (2006) *E-Demokratie- Stand, Chancen und Risiken*. [Online]. Available: <http://www.bpb.de/files/5XSXDC.pdf> [19 July 2009]
- Burn, J., Robins, G. (2003), "Moving towards e-government: a case study of organizational change processes", *Logistics Information Management*, Vol.16, No.1, pp.25-35.
- C. R. Nielsen, E. H. Andersen, and H. R. Nielson. (2005) Static validation of a voting protocol. *Electronic Notes in Theoretical Computer Science*, Vol.135, No.1, pp.115-134
- California Institute of Technology — MIT, (2001) Voting: What is, what could be, *Voting Technology Project*, pp.289-311
- California Secretary of State. (2000) *California Internet Voting Task Force: Final Report*. [Online]. Available: <http://www.ss.ca.gov/executive/ivote> [19 July 2009]
- California Secretary of State. (2007) *Top-To-Bottom-Review*. [Online]. Available: http://www.sos.ca.gov/elections/elections_vsr.htm [19 July 2009]

- Caltech/MIT Voting Technology Project. (2001) *Voting---what is, what could be*.
[Online]. California Institute of Technology, Pasadena, CA. Available:
<http://www.vote.caltech.edu/Reports/2001report.html> [19 July 2009]
- Camenisch, I. J.; Piveteau, J. and Stadler, M. (2004) Blind signatures based on discrete logarithm problem. In: *Advances in Cryptology, EUROCRYPT'94 Lecture Notes in Computer Science*, Vol.950, pp.428-432
- Carter, L., Belanger, F. (2004) "The influence of perceived characteristics of innovating on e-government adoption", *Electronic Journal of E-government*, Vol.2, No.1
- Carter, L., Belanger, F. (2005) "The utilization of e-government services: citizen trust innovation and acceptance factors", *Information Systems Journal*, Vol. 15, No.1, pp.5-25
- Chaum, D. (2001) Untraceable electronic mail, return addresses, and digital pseudonyms. *Communication of the ACM*, Vol.24, pp. 84–88
- Chaum, D. (2002) Blind signatures for untraceable payments. *Advances in Cryptology, CRYPTO'82*, pp.199-203
- Chaum, D. (2008b) Elections with unconditionally secret ballots and disruption equivalent to breaking RSA. *Advances in Cryptology, EUROCRYPT'88*, pp.177-182
- Chaum, D., (1999) Elections with unconditionally-secret ballots and disruption equivalent to breaking RSA. In: *Advances in Cryptology EUROCRYPT'88 Proceedings, Springer-Verlag*, pp.177-182
- Chaum, D., (2001) Untraceable electronic mail, return address and digital pseudonyms. *Communication of the ACM*, Vol.24, No.2, pp.84–88
- Chaum, D. (2003) Blind signatures system. *Advances in Cryptology, CRYPTO'83*, pp.153-156
- Chaum, D., (2008) The dining cryptographers problem: unconditional sender and recipient untraceability. *Journal of Cryptography*, Vol.1, pp.65–75

- Chen YY. (2008) *The study of employing the cryptography in the network society*. pp.56. Ph.D. thesis, Taiwan: National Chung Hsing University
- CIO (1999) “*Technology execs and consumers voice support for e-voting, indifference to internet taxes: CIO magazine study – industry trend or event*”. [Online]. EDP Weekly's IT Monitor. Available: www.findarticles.com/p/articles/mi_m0GZQ/is_50_40/ai_58447395 [27 December 2009]
- Clarke, R. (1999) *A primer in diffusion of innovations theory*. [Online]. Available at: www.anu.edu.au/people/Roger.Clarke/SOS/InnDiff.html [19 July 2009]
- Collins, N., Butler, P. (2002) "The marketplace, e-government and e-democracy", *Iris Marketing Review*, Vol.15, No.2, pp.86-93
- Council of Europe. (2004) *Legal, Operational and Technical Standards for E-Voting*. CoE Publishing. [Online]. Available: http://www.coe.int/t/e/integrated_projects/democracy/02_activities/02_e-voting/01_recommendation [19 July 2009]
- Cramer R. Franklin M. Schoenmakers B. Yung M. (2006) “Multi-authority secret ballot elections with linear work”, *Lecture Notes in Computer Science*, Vol.1070, pp. 72-83
- Cramer R. Gennaro R. and Borrell J. (2007) A secure and optimally efficient multi-authority election scheme. *In: Advances in Cryptology, EUROCRYPT'97 Lecture Notes in Computer Science*, pp.103-117
- Cramer, R. Franklin M. Schoenmakers B. and Yung M. (2006) Multi-authority secret ballot elections with linear work. *In: Advances in Cryptology, EUROCRYPT'96, Lecture Notes in Computer Science*, pp.72-83
- Cranor L. and Cytron R. (2007) Sensus: a security-conscious electronic polling system for the Internet. *In: Proceedings of the Thirtieth Hawaii International Conference on System Sciences*, Vol.3, pp.561-570

- Cranor, L.F. and Crtron, R.K. (2007) Sensus: a security-conscious electronic polling system for the Internet, system sciences. *In: Proceedings of the 30th Hawaii International Conference on System Science*, Vol.3, pp.561-570
- Cranor, Lorrie Faith, and Ron K. Cytron. (1996) *Sensus: A Security-Conscious Electronic Polling System for the Internet*. [Online]. Available: <http://ccrc.wustl.edu/~lorracks/sensus> [19 July 2009]
- Cronbach, L. (1970) *Essentials of Psychology Testing*. New York: Harper and Row
- CyberVote (IST-1999-20338 project), (1999) Report on electronic democracy projects, legal issues of Internet voting and users requirements analysis, *European Commission, IST Programme*, pp.12
- D. Ata,c, B. Kayapinar, and W. Riedel.(2004) *e-Voting mit Open Source*. Gutachten
- D. Chaum. (1981) Untraceable electronic mail, return addresses and digital pseudonyms. *Communications of the ACM*, Vol.24, No.2, pp.84-88
- D. Chaum. (1983) *Blind signatures for untraceable payments*. *In Crypto '82*, pp.199-203. New York: Plenum Press
- D. Chaum. (1988) The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, Vol. 1, No.1, pp.65-75
- Dan Boneh, Xavier Boyen, and Shai Halevi. (2005) *Chosen ciphertext secure public key threshold encryption without random oracles*. [Online]. Available: <http://crypto.stanford.edu/~dabo/abstracts/threshold.html> [19 July 2009]
- Daniel Rubin, (2001) *The Security of Remote On-Line Voting*. [Online]. University of Virginia. Available: <http://www.cs.virginia.edu/~evans/theses/rubin.pdf> [19 July 2009]
- David Chaum. (1981) Chapter Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, *Communications of the ACM*, Vol.24, No.2, pp.84-90
- David Chaum.(2001) SureVote: Technical Overview. *In Proceedings of the workshop on trustworthy elections (WOTE'01)*

- David Corcoran, David Sims and Bob Hillhouse, (1999) *Smart Cards and Biometrics: Your Key to PKI*, *Linux journal*. [Online]. Available:
<http://www.linuxjournal.com/article/3013> [19 July 2009]
- David Wagner. CS 276: Cryptography - Lecture 24. Retrieved 19 July 2009 from:
<http://www.cs.berkeley.edu/~daw/teaching/cs276-s06/l24.ps>
- Davis, F. (1989) "Perceived usefulness, perceived ease of use and user acceptance of information technology", *MIS Quarterly*, Vol.13, No.3, pp.319-40
- Dictson, D. and D. Ray (2000) *The Modern Democratic Revolution: An Objective Survey of Internet-Based Elections*. SecurePoll.com, White Paper
- Dieter Nohlen. (2007) *Wahlrecht und Parteiensystem*, Vol.5. Verlag Barbara: Budrich
- Dini G. (2001) Electronic voting in a large-scale distributed system. *Networks*, Vol.38, pp.22-32
- Dini, G. (2003) A secure and available electronic voting service for a large-scale distributed system. *Future Generation Computer System*, Vol.19, pp.69-85
- Done, R.S. (2002) "Internet voting: bringing elections to the desktop", *The PricewaterhouseCoopers Endowment for the Business of Government*. E-government Series
- Eckhard Jesse. (2003) *Reform proposals to amend the electoral law, Bonn*. [Online]. Available:
http://www.bpb.de/publikationen/3OXR5G,0,0,Wahlssystem_und_Wahlrecht.html [19 July 2009]
- Eggers, W.D. (2005) *Government 2.0 Using Technology to Improve Education, Cut Red Tape, Reduce Gridlock, and Enhance Democracy*, Rowman & Littlefield Publishers, Inc., Lanham,
- Election Process Advisory Commission.(2007) *Voting with confidence - Summary, Conclusions and Recommendations*. [Online]. Available:
http://www.minbzk.nl/bzk2006uk/subjects/constitution-and/press_releases?ActItmIdt=109259 [19 July 2009]

- Electoral Commission. (2007) *Electoral Commission calls for end to 'piece-meal' election pilots*. [Online]. Available: www.electoralcommission.org.uk/media-centre/newsreleasereviews.cfm/news/657 [19 July 2009]
- ElGamal T. (2005) A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory IT*, Vol.31, pp.469-472
- Engelbert Hubbers, Bart Jacobs, and Wolter Pieters. (2005) *RIES - Internet Voting in Action*
- Enguehard, C. (2008) *Transparency in electronic voting : the great challenge, in 'IPSA - International Political Science Association RC 10 on Electronic Democracy'*. South Africa: Stellenbosch University
- Erika Wayne. (2001) *Election 2000 Chronology*. [Online]. Available: http://www.law.stanford.edu/publications/stanford_lawyer/issues/60/election2000_chronology.html [19 July 2009]
- EU Cybervote Project. (2003) Final Report. [Online]. Available: <http://www.eucybervote.org/MSI-WP6-D21-v1.0.pdf> [19 July 2009]
- EU Cybervote Project.(2003) *Report on Review of Cryptographic Protocols and Security Techniques for Internet Voting*. [Online]. Available: <http://www.eucybervote.org/TUE-WP2-D6V1v1.0.pdf> [19 July 2009]
- European Commission, (2000). IST 2000 Programme, The Information Society for all. Brussels, *Final Report*, pp.56
- e-VOTE, (2002) (IST-2000-29518 project), Legal and regulatory issues on e-voting and data protection in Europe, Deliverable D3.4, *European Commission, IST Programme*, pp.395. [Online]. Available: e-voto.di.fc.ul.pt/docs/The%20Modern%20Democratic%20Revolution.pdf [03 July 2009]
- Fabian Breuer and Alexander H. Trechsel. (2006) *E-Voting in the 2005 local elections in Estonia*. [Online]. European University Institute. Available:

- http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/EVoting_Documentation/PDF-FinalReportCOE_EvotingEstonia2005.pdf [19 July 2009]
- Federal Ministry of Germany. (2007) *Wahlger, Encyclopedia of Domestic Policy*. [Online]. Available: <http://www.en.bmi.bund.de> [19 July 2009]
- Fischer, E.A. (2001) "*Voting technologies in the United States: overview and issues for Congress*", The Wilson Quarterly, available at: <http://usinfo.state.gov/usa/infousa/politics/voting/rl30773.pdf> Vol. 25 No.3, pp.103.
- Freeman, C. (1993) Technical change and future trends in the world economy. *Futures*, Vol.25, No.6, pp.621-635
- Fujioka A., Okamoto T. and Ohta K. (2003) A practical secret voting scheme for large-scale elections. In: Advances in Cryptology, *AUSCRYPT'92 Lecture Notes in Computer Science*, Vol.718, pp.244–251
- G. Danezis and C. Diaz. (2008) A survey of anonymous communication channels. *Journal of Privacy Technology*
- G. Schryen. (2004) How security problems can compromise remote internet voting systems. In A. Prosser and R. Krimmer, editors, 1nd International Workshop on Electronic Voting, number P-47 in Lecture Notes in Informatics, pp.121-131. Bregenz: Austria
- Ganesan, S., Hess, R. (1997) "Dimensions and levels of trust: implications for commitment to a relationship", *Marketing Letters*, Vol.8, No.4, pp.439-48
- GAO, General Accounting Office (2004) "*Electronic voting offers opportunities and presents challenges*". [Online]. Available: www.gao.gov/new.items/d04975t.pdf [1 September 2010]
- Gefen, D. (2000) "E-commerce: the role of familiarity and trust", *Omega: The International Journal of Management Science*, Vol.28, No.6, pp.725-37

- Gefen, D., Karahanna, E., Straub, D. (2003) "Trust and TAM in online shopping: an integrated model", *MIS Quarterly*, Vol.27, No.1, pp.51-90
- Gefen, D., Rose, G.M., Warkentin, M., Pavlou, P.A. (2005), "Cultural diversity and trust in IT adoption: a comparison of potential e-voters in the USA and South Africa", *Journal of Global Information Management*, Vol.13, No.1, pp.54-78
- Gefen, D., Straub, D. (2000) "The relative importance of perceived ease of use in IS adoption: a study of e-commerce adoption", *Journal of the Association for Information Systems*, Vol.1, No.8, pp.1-28
- Gerck, E. (2000) "From voting to internet voting", *The Bell*, Vol.1, No.1, pp.1-9
- Gerck, E., Neff, C. A., Rivest, R. L., Rubin, A. D. and Yung, M. (2001), "The Business of Electronic Voting", FC'01, *5th International Conference on Financial Cryptography*, LNCS 2339, pp.243-268
- Gibson, M. Nixon, P., Ward, S. (2003) *Political Parties and the Internet: Net Gain?* New York: Routledge
- Gibson, R. (2001) "Elections online: assessing internet voting in light of the Arizona Democratic Primary", *Political Science Quarterly*, Vol.116, No.4, pp.561-83
- Gimpel, J.G., Schuknecht, J.E. (2003) "Political participation and the accessibility of the ballot box", *Political Geography*, Vol.22, pp.471-88
- Grant, G., Chau, D. (2005) "Developing a generic framework for e-government", *Journal of Global Information Management*, Vol.13, No.1, pp.1-29
- Green, T. (2000) Voting in a Virtual World. *New Statesman*, Vol.129, No.4517
- Gritzalis, D.A. (2002) Principles and Requirements for a Secure E-Voting System. *Computers & Security*, Vol.21, No.6, pp.539-556
- Gritzalis, Dimitris A. (2002) Principles and requirements for a secure e-voting system. *Computer Security*, Vol.21, No.6, pp.539–556
- Haas R. (2002) Building PV markets: customers and prices. *Renewable Energy World*, Vol.5, No.3, pp.98-111

- Hall, T., Alvarez, M. (2004) *American Attitudes about Electronic Voting Results of a National Survey*. Center for Public Policy & Administration: University of Utah
- Hans-Urs Wili.(2008) *Amendment to federal legislation on the Political Rights entered into force effective*. [Online]. Available:
<http://www.bk.admin.ch/themen/pore/evoting/00773/index.html?lang=de>,
 2007 [19 July 2009]
- Harn L, Kiesler T. (2001) How to hold an election over computer network. *Workshop on Information Security & Modern Cryptography*. Taiwan: R.O.C
- Heise online (2006) *Italy will stop voting computer projects*. [Online]. Available:
<http://www.heise.de/newsticker/Italien-stoppt-Wahlcomputer-Projekte--meldung/81832> [09 May 2009]
- Hirt M, Sako K. (2000) Efficient receipt-free voting based on homomorphic encryption. *Advances in Cryptology - EUROCRYPT'00. Lecture notes in computer science*, Vol.1087, p.539-56. Berlin
- Hoeing, C. (2001) "Beyond e-government", *Government Executive*, pp.49-52
- Hoffman L. Cranor L. (2001) "Internet voting for public officials", *Communications of the ACM*, Vol.44, No.1, pp. 69-71
- Hulme, G.V. (2004) *"E-voting systems face security questions"*, Information Week, 9 February
- Hunter, G.E. (2001) "The role of technology in the exercise of voting rights", *Law Technology*, Vol.34, No.4, pp.1-14
- Ikonomopoulos S. Gritzalis D. Lambrinoudakis C. Kokolakis S. Vassiliou C.(2002) "Functional requirements for a secure electronic voting system", in Proc. of the 17th IFIP International Information Security Conference, M. Hadidi, et al. (Eds.), pp.507-520

- International Working Group for Data Protection in Telecommunications, (2001) *Common Position on the Use of the Internet in the Conduct of Elections*, pp.96. Berlin
- Internet Policy Institute, (2001) *Report of the National Workshop on Internet Voting: Issues and Research Agenda*, pp.45
- ITAA (2000) "*Keeping the faith: government information security in the internet age*". [Online]. Available: www.ita.org/infosec/faith.pdf [01 June 2009]
- J. Benaloh. (1987) *Verifiable Secret-Ballot Elections*. PhD thesis. New Haven-USA: Yale University
- J. Helbach and J. Schwenk. (2007) Secure internet voting with code sheets. In A. Alkassar and M. Volkamer, editors, VOTE-ID'07, 1st International Conference on E-Voting and Identity, LNCS 4896, pp.166-177. Bochum: Germany
- J. Jillbert and M. Musaruddin, (2003) *Online voting for e-democracy in developing countries: is it possible?* Indonesia
- J. Kitcat. (2004) Source availability and e-voting: an advocate recants. *Communications of the ACM*, Vol.47, No.10, pp.65-6
- Jörg Helbach. (2007) *Secure Internet Voting with Code Sheets*. In Pre-Proceedings Vote-ID
- Jacobson I. (2003) *Object-oriented software engineering - a use case driven approach*, Addison-Wesley, pp.63
- Jacobson I., Booch G., Rumbaugh J. (1999) *The Unified Software Development Process*, Addison-Wesley, pp.174
- Jaeger, P.T. (2003) "The endless wire: e-government as global phenomenon", *Government Information Quarterly*, No.20, pp.323-31

- Jaeger, P.T., Thompson, I.M. (2003) "E-government around the world: lessons, challenges, and future directions", *Government Information Quarterly*, No.20, pp.389-94
- Jan JK, Chen YY, Chen CL. (2003) A realistic secure anonymous e-voting protocol based on the ElGamal scheme. *Proceedings of the International Conference on Communications & Broadband Networking*, pp.1-9. India: Bangalore
- Jan JK, Chen YY, Lin Y. (2001) The design of protocol for e-voting on the Internet. *Proceedings of the IEEE International Carnahan Conference on Security Technology*. England: London
- Jan JK, Lin RH. (2005) A secure anonymous voting by employing Diffie–Hellman PKD concept. *IEEE International Carnahan Conference on Security Technology*. England
- Jan, J.K. and Tai, C.C. (2007) A secure electronic voting protocol with IC cards, *Journal of the System Software*, Vol.39, pp.93-101. USA
- Jarvenpaa, S.L., Knoll, K., Leidner, D.E. (1998) "Is anybody out there? Antecedents of trust in global virtual teams", *Journal of Management Information Systems*, Vol.14, No.4, pp.29-64
- Jefferson, D., Rubin, A., Simons, B., Wagner, D. (2004) "A security analysis of the secure electronic registration and voting experiment". [Online]. Available: <http://servesecurityreport.org> [05 July 2010]
- Jinn-Ke Jan, Yu-Yi Chen, Yi Lin. (2001) "The Design of Protocol for e-Voting on the Internet". *Annual Computer Security Applications Conference IEEE*
- Joaquim, R. and Ribeiro, C. (2007) 'Codevoting protection against automatic vote manipulation in an uncontrolled environment', *Lecture Notes in Computer Science* 4896/2007
- Jones B. (2000) A report on the feasibility of Internet voting, *Internet Voting Task Force*, State of California

- Joshua Sunshine, Serge Egelman, Hazim Almuhiemedi, Neha Atri, and Lorrie Faith Cranor ,(2009) *Crying Wolf: An Empirical Study of SSL Warning Effectiveness*, *18th USENIX Security Symposium*. [Online]. Carnegie Mellon University. Available: http://www.usenix.org/events/sec09/tech/full_papers/sunshine.pdf [19 July 2009]
- Juang, W.S. and Lei, C.L. (2006) A collision-free secret ballot protocol for computerized general elections, *Computer Security*, Vol.15, No.4, pp.339-348
- Jun Chen. (2007) *Verifiable Mixnets Techniques and Prototype Implementation*. Master's thesis: Darmstadt University of Technology
- K. Sako and J. Kilian. (1994) Secure voting using partially compatible homomorphisms. In Y. Desmedt, editor, *CRYPTO'94, 14th Annual International Cryptology Conference on Advances in Cryptology*, LNCS 839, pp.411-424. USA: Santa Barbara
- Kaldellis J.K. and Sotiraki K. (1999) In: Proceedings of the Sixth National Congress on Soft Energy Applications, Volos, Greece, Autonomous photovoltaic plants for remote islands. *Design proposals and operational study*, Vol.A, pp.301-308
- Kaldellis J.K., Doumouliakas J. and Michalis K. (2000) *Optimum stand-alone PV solution, including financial aspects*, pp.1966-1969
- Kaldellis J.K., Kavadias K.A. and Kondili E. (2004) Renewable energy desalination plants for the Greek islands, technical and economic considerations, *Journal of the Desalination*, Vol.170, No.2, pp.187-203
- Kaldellis J.K. (2002) Optimum autonomous wind power system sizing for remote consumers, using long-wind speed data, *Journal of the Apple Energy*, Vol.71, No.2, pp.215-233
- Karro J. and Wang J. (1999) Towards a practical, secure, and very large scale online election. In: *Proceedings of 15th Annual Computer Security Applications Conference (ACSAC'99)*, pp.161-169

- Kavadias K, Komnimglou A, Kaldellis JK. (2001) *Wind energy surplus management for remote consumers using a water pumping storage system*, p.972-975.
Copenhagen: European Wind Energy Conference, Conference Proceedings-
Bella Centre
- Kawachiya K. Ogata K. Silva D. Onodera T. Komatsu H. Nakatani T.
(2007). "*Cloneable JVM: a new approach to start isolated java applications faster*"
- Kawalek, P., Wastall, D. (2005) "Pursuing radical transformation in information age government: case studies using the SPRINT methodology", *Journal of Global Information Management*, Vol.13, No.1, pp.79-91
- Kent, M., Harrison, T. and Taylor, M. (2006) A Critique of Internet Polls as Symbolic Representation and Pseudo-Events, *Communication Studies*, Vol.57, No.3
- Kim A. (2001) "Ten things I want people to know about voting technology", *Democracy Online Project's National Task Force*, California Voter Foundation, pp 63-84
- Kofler R, Krimmer R, Prosser A. (2003) Electronic voting: algorithmic and implementation issues. *Proceedings of the 36th Hawaii International Conference on System Science (HICSS'03)*, pp.56
- Krishna Sampigethaya and Radha Poovendran. (2006) A framework and taxonomy for comparison of electronic voting schemes. *Computers Security*, Vol.25, pp.137-153
- L. F. Cranor and R. K. Cytron. (1996) Design and implementation of a practical security-conscious electronic polling system. *Technical Report WUCS-96-02*. Washington: Uni-versity
- L. Loeber. (2008) E-voting in the Netherlands: from general acceptance to general doubt in two years. In R. Krimmer and R. Grimm, editors, *3rd International Workshop on Electronic Voting*. Austria: Bregenz
- Larman G., (2008) *Applying UML and patterns*, Prentice-Hall, pp.45-187

- Lazou A. and Papatsoris A. (2000) The economics of photovoltaic stand-alone residential households: a case study for various European and Mediterranean locations, *Solar Energy Mater Solar Cells Journal*, Vol.62, No.4, pp.411-427
- Lee, M.K.O., Turban, E. (2001) "A trust model for internet shopping", *International Journal of Electronic Commerce*, Vol.6, No.1, pp.75-91
- Lei C.L. and Fan C.I. (2008) A universal single-authority election system. *IEICE Transactions on Fundamentals*, Vol.E81, No.A10, pp.2186-2193
- Lemos, R. (2004) "E-voting 'risks fraud'". [Online]. Available: <http://news.zdnet.co.uk/business/0,39020645,39119276,00.htm> [29 January 2010]
- Lin, I.C., Hwang, M.S. and Chang, C.C. (2003) Security enhancement for anonymous secure e-voting over a network. *Computer Stand Interface*, Vol.25, pp.131-139
- M. Jakobsson, A. Juels, and R. Rivest. (2002) Making mix nets robust for electronic voting by randomized partial checking. *In Proceedings of the 11th USENIX Security Symposium*
- M. Volkamer and M. McGaley. (2007) Requirements and evaluation procedures for evoting. *In ARES'07, 2nd International Conference on Availability, Reliability and Security*, pp.895-902. Austria: Vienna
- M. Volkamer and R. Grimm. (2006) Multiple Casts in Online Voting: Analyzing Chances. *In Electronic Voting 2006*, pp.97-106. Bonn
- Macintosh, A., Whyte, A. (2000) *Electronic Democracy and Educating Young People*, International Teledemocracy Centre. Edinburgh: Napier University
- Manna, D.R., Smith, A.D. (2003) "Measuring the theoretical paradigm shift from marketing mix to relational marketing", *International Business and Economics Research Journal*, Vol.2, No.11, pp.1-8
- Marche, S., McNiven, J.D. (2003) "E-government and e-governance: the future isn't what it used to be", *Canadian Journal of Administrative Sciences*, Vol.20, No.1, pp.74-86

- Marie-Fleur Auf der Maur and Samuel Vontobel. (2007) *Case Studies on E-voting*. Master's thesis. Switzerland: University of Freiburg
- Matrix (2000) *Internet Voting a Threat to Democracy*, Vol.1, No.3. Matrix: The Magazine for Leaders in Higher Education
- Mayer, R. Davis, J. Schoorman, D. (1995) "An integrative model of organization trust", *Academy of Management Review*, Vol.20, No.3, pp.709-34
- Mayor, T. (2004) "Unlocking our future". [Online]. Available: www.keepmedia.com/jsp/article [01 June 2009]
- McGraw, Gary and Greg Morrisett. (2000) "Attacking Malicious Code: A Report to the Infosec Research Council" *IEEE Software*
- McKnight, H. Choudhury, V. Kacma, C. (2000) "Trust in e-commerce vendors: a two-stage model", *Proceedings of the 21st International Conference on Information Systems*, Brisbane, pp.532-6.
- McKnight, H. Choudhury, V. Kacmar, C. (2002) "Developing and validating trust measures for e-commerce: an integrative typology", *Information Systems Research*, Vol.13, No.3
- McKnight, H. Cummings, L. (1998) "Initial trust formation in new organizational relationships", *Academy of Management Review*, Vol.23, No.3, pp.473-90
- McMillen, D. (2004) "Privacy, confidentiality, and data sharing: issues and distinctions", *Government Information Quarterly*, Vol.21, No.3, pp.359-82
- Melanie Volkamer and Robert Krimmer. (2006) *The online poll on the way to break through*, No.29, pp.98-113
- Mercuri R. (2000) "Voting automation?", *Communications of the ACM*, Vol.43, No.2, pp.176
- Mitrou L. Gritzalis D. Katsikas S. (2002) "Revisiting legal and regulatory requirements for secure e-voting", in *Proc. of the 17th IFIP International Information Security Conference*, pp.469-480

- Mohen, Joe and Julia Glidden, (2001) "The Case for Internet Voting", *Communications of the ACM*. Vol.44, No.1
- Moon, J-M., Kim, Y-G. (2001) "Extending the TAM for a world-wide-web context", *Information and Management*, No.28, pp.217-30
- Moore, G.C., Benbasat, I. (1991) "Development of an instrument to measure the perceptions of adopting an information technology innovation", *Information Systems Research*, Vol.2, No.3, pp.173-91
- Morse, R. (2002) "Electronic voting: progress over setbacks", *Law Technology*, Vol. 35, No.4, pp.1-6
- Mote, C.D. (2001) E-voting Report: Report of the National Workshop on Internet Voting: Issues and Research Agenda, *Internet Policy Institute*
- Mu Y. and Mu V. (2008) Anonymous secure e-voting over a network. In: *Proceedings of the 14th Annual Computer Security Applications Conference, ACSAC'98*, pp.293-299
- Mu Yi, Varadharajan V. (1998) Anonymous secure e-voting over a network. *Computer Security Applications Conference. Proceedings. 14th Annual*
- Muselli M. Notton G. and Louche A. (1999) Design of hybrid-photovoltaic power generator, with optimization of energy management, *Solar Energy Journal*, Vol.65, No.3, pp.143-157
- Nair, A. (2009) *Legislative body polls 'by June 2010'*. [Online]. Available: http://www.gulf-times.com/site/topics/article.asp?cu_no=2&item_no=266087&version=1&template_id=57&parent_id=56 [01 June 2009]
- National Democratic Institute (2009) *Qatar*. [Online]. Available: <http://www.ndi.org/qatar> [19 July 2010]
- Nohlen, D., Grotz, F. and Hartman, C. (2001) *Elections in Asia and the Pacific: A Data Handbook*. England: Oxford

- Norbert Kersting. (2004) *Online Voting: an international comparison*. In *Modern Governance / e-government*, No.18, pp.16-23. [Online]. Available: http://www.bpb.de/publikationen/5T5OEL,0,OnlineWahlen_im_internationale_n_Vergleich.html [19 July 2009]
- Notton G, Muselli M, Poggi P, Louche A. (1999) Stand alone wind energy systems sizing procedure with cost optimization, *presented at 1999 European Wind Energy Conference and Exhibition*. France: Nice
- Notton G., Muselli M., Poggi P. and Louche A., (2008) Sizing reduction induced by the choice of electrical appliances options in a stand-alone photovoltaic production. *Renewable Energy*, Vol.15, pp.581-584
- Nurmi, H., Salomaa, A. and Santeau, L. (2001) Secret ballot elections in computer networks. *Computer Security*, Vol.10, No.6, pp.553-560
- Okamoto T. (2007) Receipt-free electronic voting schemes for large-scale elections. *In: Proceedings of the Fifth Workshop on Security Protocols. Lecture notes in computer science*, p.25-35. France: Paris
- Oostveen, A. and P.van den Besselaar (2004) Security as Belief. User's Perceptions on the Security of Electronic Voting Systems. In: *Electronic Voting in Europe: Technology, Law, Politics and Society*.
- OSCE/ODIHR. (2007) *Parliamentary Elections*. Republic of Estonia
- P. G. Neumann. (1993) Security criteria for electronic voting. *In NCSC'93, 16th National Computer Security Conference*, pp.478-482. USA: Baltimore
- P. Y. A. Ryan and S. A. Schneider. (2006) Pret a Voter with Re-encryption Mixes. *In European Symposium on Research in Computer Security, number 4189 in Lecture Notes in Computer Science*. Springer-Verlag
- Paul Krugman. (2007) *When votes disappear*. [Online]. Available: http://www.truthout.org/docs_2006/112406C.shtml [19 July 2009]

- Pavlou, P.A. (2003) "Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model", *International Journal of Electronic Commerce*, Vol.7, No.3, pp.69-103
- Permanent Election Committee (2008). *A Training Course Organized By Permanent Elections Committee, SCFA*. [Online]. Available: http://www.pecq.org.qa/news_21feb08_en.php [19 July 2009]
- Pfitzmann A., (2004) A switched/broadcast ISDN to decrease user operability. *In: Proceedings of International Zurich Seminar on Digital Communications*, pp.183-190. Zurich
- Philippe Beaucamps, Daniel Reynaud-Plantey, Jean-Yves Marion (2009) *On the use of Internet Voting on Compromised Computers, Army Signals Academy Virology and Cryptology Laboratory*. [Online]. France: Rennes. Available: http://lhs.loria.fr/images/stories/Doc/beaucamps-reynaud-marion-filiol-internet_voting-iciw09_paper.pdf [19 July 2009]
- Phillips D., von Spakovsky H. (2001) "Gauging the risks of Internet elections", *Communications of the ACM*, Vol.44, No.1, pp.73-85
- Phillips D.M. & Jefferson, D. (2000) *Is The Internet Safe?* [Online]. Available: <http://www.voting-integrity.org/text/2000/internetsafe.shtml> [19 July 2009]
- Prof. Dr. Johannes Buchmann. (2004) *Introduction to cryptography*. Springer, Berlin Heidelberg, third edition.
- R. Anane, R. Freeland, and G. Theodoropoulos. (2007) e-voting requirements and implementation. *In CEC'07, 9th IEEE Conference on E-Commerce Technology*, pp. 382-392. Tokyo: Japan
- R. Cramer, R. Gennaro, and B. Schoenmakers. (1997) A Secure and Optimally Efficient Multi-Authority Election Scheme. *European Transactions on Telecommunications*, Vol.8, No.5, pp.481-490
- R. Krimmer, editor, *1st International Workshop on Electronic Voting, number P-47 in Lecture Notes in Informatics*, pp.31-42. Austria: Bregenz:

- R. Krimmer, S. Triessnig, and M. Volkamer. (2007) *The development of remote e-voting around the world: A review of roads and directions*. In A. Alkassar and M. Volkamer, editors, *VOTE-ID'07, 1st International Conference on E-Voting and Identity*, pages 1-15, Germany: Bochum
- R. Oppliger, (2002) *Addressing the Secure Platform Problem for Remote Internet Voting in Geneva*. [Online]. Available:
http://www.geneve.ch/evoting/english/doc/rapports/rapport_oppliger_en.pdf
 [19 July 2009]
- R. Oppliger. (2002) How to address the secure platform problem for remote internet voting. In *SIS'02, 5th Conference on "Sicherheit in Informations systemen"*, pp.153-173. Austria: Vienna
- Ray I, Ray I, Narasimhamurthi N. (2001) An anonymous electronic voting protocol for voting over the Internet. Advanced issues of e-commerce and web-based information systems, WECWIS. *Third International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems*, pp.188-90
- Regenscheid, A. and Hastings, N. (2008) *A Threat Analysis on UOCAVA Voting Systems*. [Online]. National Institute of Standards and Technology. Available:
<http://vote.nist.gov/uocava-threatanalysis-final.pdf> [19 July 2009]
- Internet Policy Institute (2001) *Report of the National Workshop on Internet Voting*
- Report on the electronic voting Opportunities (2002) *risks and feasibility of electronic Exercise of political rights .Technical report*. [Online]. Available:
<http://www.admin.ch/ch/d/ff/2002/645.pdf> [19 July 2009]
- Report on the pilot projects for electronic voting (2006) *Swiss Federal Council, Bern. Technical report*. [Online]. Available:
<http://www.bk.admin.ch/themen/pore/evoting/00776/02793/index.html?lang=de&unterseite=yes> [19 July 2009]
- Riera A, Borrel J, Rifà J. (2008) An uncoercible verifiable electronic voting protocol. *Proceedings of the 14th International Security Conference (IFIP/SEC'98)*, pp.206-215

- Rivest R.L., Shamir A. and Adleman L. (2005) A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, Vol.21, pp. 120-126
- Rivest, R., Shamir, A. and Adleman, L. (2008) A method for obtaining digital signatures and public-key cryptosystems. *Communications ACM*, Vol.21, No.2, pp. 120-126
- Rogers, E.M. (1986) *Communication: The New Media in Society*. New York: The Free Press
- Rogers, E.M. (1995) *Diffusion of Innovations*. New York: The Free Press
- Rolf Oppliger (2002) *Addressing the Secure Platform Problem for Remote Internet Voting in Geneve*
- Ronald L. Rivest. (2002) Electronic Voting. *Financial Cryptography '01*, SpringerVerlag
- Rubin, A. (2002) "Security considerations for remote electronic voting over the internet", *Communications of the ACM*, Vol.45, No.12, pp.39-43
- Rubin, Avi. (2000) *Security Considerations for Remote Electronic Voting over the Internet*. [Online]. Available: <http://avirubin.com/e-voting.security.html> [19 July 2009]
- Saco, D. (2002) *Cybering Democracy: Public Space and the Internet*. Minneapolis: University of Minnesota Press
- Sako K, Kilian J. (2005) Receipt-free mix-type voting scheme a practical implementation of a voting booth. *Advances in Cryptology CRYPTO'95. Lecture notes in computer science*, Vol.921, p.393-403. Berlin
- Saltman, R. (2008) Accuracy, integrity and security in computerized vote-tallying. *Communication of the ACM*, Vol.31, No.10, pp.1181-1191

- Schoenmakers B. (1999) "A simple publicly verifiable secret sharing scheme and its application to electronic voting", in *Lecture Notes in Computer Science*, Vol.1666, pp. 148-164
- Schweizerischer Bundesrat. (2006) *Report on the pilot projects for electronic voting. Technical report*
- Shamir, A. (1999) How to share a secret. *Communication of the ACM*, Vol.22, pp.612-613
- Shane, P. (2004) *Democracy Online: The Prospects for Political Renewal through the Internet*. New York: Routledge
- Shannon, C.E., (2003) In: *Sloane, N.J.A. and Wyner, A.D., Editors, 1993. Collected papers: Claude Elmwood Shannon*, pp.25. New York: IEEE Press
- Siegfried Thielbeer. (2007) *Choose Living*. FAZ, No.232
- Simons A., Graham I. (2008) *37 things that don't work in object-oriented modelling with UML, Technical Report TUM-I9813*, pp.967. Technical University of Munich
- Slessenger, P.H. (2001) Socially secure cryptographic election scheme. *Electron Lett*, Vol.27, No.11, pp. 955–957
- Smith, A.D. (2002) "Loyalty and e-marketing issues: customer retention on the Web", *Quarterly Journal of E-commerce*, Vol.3, No.2, pp.149-161
- Smith, A.D. (2004) "Online privacy policies and diffusion theory perspectives: security or chaos?", *Services Marketing Quarterly*, Vol.25, No.1, pp.47-74
- Smith, A.D., Manna, D.R. (2005), "Exploring why people love their jobs", *Journal of Business & Economics Research*, Vol.3, No.3, pp.21-26
- Smith, A.D., Rota, D.R., Turchek, J.C. (2003) "Combining automatic data capture systems: smart cards and biometrics", *Journal of Contemporary Business*, Vol.11, No.2, pp.26-36

- Smith, A.D., Rupp, W.T. (2002b) "Issues in cyber-security: understanding the potential risks associated with hackers/crackers", *Information Management & Computer Security*, Vol.10, No.4, pp.178-83
- Smith, A.D., Rupp, W.T. (2003) "Information management leveraging in the case of e-folios: mass customization approaches in an e-commerce environment", *Services Marketing Quarterly*, Vol.25, No.1, pp.47-74
- State of Geneva. (2007) *E-Voting*. [Online]. Available:
<http://www.geneve.ch/evoting/english/welcome.asp> [19 July 2009]
- Statements about Internet Voting from Experts, (2005). [Online]. Available:
www.votersunite.org/info/WACommentsFromExperts.pdf [20 July 2010]
- Storer, T., Duncan, I. (2004) "Polsterless remote electronic voting", *Journal of E-Government*, Vol.1, No.1, pp.75-103
- Strassman, M. (2000) "Reply to Deborah Phillips." *E-Mail List Serve Posting*. In Dictson D. & Ray D. *The Modern Democratic Revolution: An Objective Survey of Internet-Based Elections*. [Online]. Available: <http://e-voto.di.fc.ul.pt/docs/The%20Modern%20Democratic%20Revolution.pdf> [13 August 2009]
- T. Kohono, A. Stubblefield, A. D. Rubin, and D. S. Wallach, (2004) *Analysis of an Electronic Voting System*. In *Proc. of IEEE Symposium on Security and Privacy 2004*. IEEE: Computer Society Press
- Tan, C.W., Pan, S.L., Lim, E.T.K. (2005) "Managing stakeholder interests in e-government implementation: lessons learned from a Singapore e-government project", *Journal of Global Information Management*, Vol.13, No.1, pp.31-53
- The Electoral Commission. (2009) *Summary of Electronic Voting - May 2007 electoral pilot schemes*. [Online]. Available:
http://www.electoralcommission.org.uk/files/dms/Electronicvotingsummarypaper_27194-20114__E__N__S__W__.pdf [19 July 2009]

- The Electoral Commission. (2003) *Technical Report on the May 2003 pilots*. [Online]. Available:
http://www.electoralcommission.org.uk/files/dms/Copyofcoverandreport-final_11369-8944__E__N__S__W__.pdf [19 July 2009]
- The State News. (2004). [Online]. Available:
www.statenews.com/op_article.phtml?pk=21398 [19 July 2009]
- Thomas, J.C., Streib, G. (2003) "The new face of government: citizen-initiated contacts in the era of e-government", *Journal of Public Administration Research and Theory*, Vol.13, No.1, pp.83-102
- Tom Espiner, (2009) *Web users ignoring security certificate warnings*. [Online]. Available: http://news.cnet.com/8301-1009_3-10297264-83.html [19 July 2009]
- Tom Sperlich. (2007) *Zurich E-Voting Project Wins UN Award, Heise online*. [Online]. Available:
http://www.bk.admin.ch/themen/pore/evoting/00773/02380/index.html?download=M3wBPgDB_8ull6Du36WenojQ1NTTjaXZnqWfVpzLhmfnapmmmc7Zi6rZnqCkkIR9g3d_bKbXrZ6lhuDZz8mMps2gpKfo&lang=de [19 July 2009]
- Toregas, C. (2001) "The politics of e-gov: the upcoming struggle for redefining civic engagement", *National Civic Review*, Vol.90, No.3, pp.235-40
- Touch plc. (2002) *"Survey shows electorate eager to vote online"*. [Online]. Available: www.touchplc.com/dyncat.cfm?catid=251 [04 February 2009]
- Trechsel, A. and Mendez, F. (2004) *The European Union and E-Voting: Addressing the European Parliament's Internet Voting Challenge*. New York: Routledge
- U.S. Department of Commerce, National Telecommunications and Information Administration. (2000) *Falling Through the Net: Toward Digital Inclusion*.
- Ulle Madise and Tarvi Martens (2006) E-Voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world. In *Electronic Voting 2006*, pp.15-26. GI Lecture Notes in Informatics, Robert Krimmer,

- United States Government Accounting Office (2004) *Elections: Electronic Voting Offers Opportunities and Presents Challenges*. [Online]. Available: <http://www.gao.gov/new.items/d04766t.pdf> [19 July 2009]
- United States Government Accounting Office (2004) *Elections: Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way But Key Activities Need to be Completed*. [Online]. Available: <http://www.gao.gov/new.items/d05956.pdf> [19 July 2009]
- USA Votenet (2002). [Online]. Available: www.usavotenet.com [19 July 2009]
- Van Slyke, C. Bélanger, F. Comunale, C. (2004) "*Adopting business-to-consumer electronic commerce: the effects of trust and perceived innovation characteristics*", accepted 19 February 2003 for the Data Base for Advances in Information Systems,
- Warkentin, M., Gefen, D., Pavlou, P., Rose, G. (2002) "Encouraging citizen adoption of e-government by building trust", *Electronic Markets*, Vol.12, No.3, pp.157-62
- Weinstein, L. (2000) Inside risks: Risks of Internet voting. *Communications of the ACM June 2000*, Vol.43, No.6
- West, D.M. (2004) "E-government and the transformation of service delivery and citizen attitudes", *Public Administration Review*, Vol.64, No.1, pp.15-27
- Wolter Pieters and Robert van Haren. (2007) *E-Voting Discourses in the UK and the Netherlands*
- Yang, E and Gaines, K. (2004) Voting Technology and the Law: From Chads to Fads and Somewhere in Between. *Social Education*. Vol.68, No.6
- Ziegler, Peter-Michael. (2006) *Italien stoppt Wahlcomputer-Projekte*. [Online]. Available: <http://www.heise.de/newsticker/meldung/81832> [19 July 2009]

- Buchsbaum, T. M. (2004) *E-Voting: International Developments and Lessons Learnt*, Proceedings ESF TED Workshop on Electronic Voting in Europe, SchlossHofen: Bregenz, pp. 31-42.
- ACE (Administration and Cost of Elections) Electoral Knowledge Network (2010). *Focus on E-Voting*. ACE is a collaborative effort between nine organisations.. [Online] Available. <http://aceproject.org/ace-en/focus/e-voting/countries?toc> [23 May 2009].
- Chaum, D. and Jakobsson, M. and Rivest, R.L. and Ryan, P.Y.A. and Benaloh, J. and Kutykowski, M. and Adida, B (2010). *Towards Trustworthy Elections: New Directions in Electronic Voting*. Berlin : New York : Springer. 403
- Kohno, T., Stubblefield, A., Rubin, A., and Wallach, D. (2004). Analysis of an Electronic Voting System. In *Proceedings IEEE Symposium on Security and Privacy*, pages 27--42.
- TGC: Trusted Computing Group (2007) [Online] Available. <https://www.trustedcomputinggroup.org/home> [12 June 2009]
- BBC News. (2008). Severed cables disrupt internet. [Online]. Available from: <http://news.bbc.co.uk/2/hi/technology/7218008.stm>. [19th May 2009]
- Crossan, F. (2003). "Research Philosophy: Towards an Understanding". *Nurse Researcher*, 11, (1), pp. 46-55.
- Galliers, R. D. (ed.) (1992). "Information Systems Research: Issues, Methods and Practical Guidelines". Oxford, Blackwell Scientific Publications.
- Miles, M.B. and Huberman, A.M. (1994). "Qualitative data analysis", 2nd edition. Newbury Park, CA, Sage.
- Walsham G. (1995). "The emergence of interpretivism in IS research." *Information Systems Research*, Vol. 6, No. 4, pp. 376-394.

- Yin, R.K. (1994). "Case Study Research: Design and Methods", 2nd edition, Newbury Park, Sage.
- Themistocleous, M. (2002). "Enterprise Application Integration", Brunel University.
- Orlikowski, W.J. and Baroudi, J.J. (1991). "Studying Information Technology in Organizations: Research Approaches and Assumptions." *Information Systems Research* ,Vol. 2, No.1, pp. 1-28
- Jackson, S. and Scott, S. (2001). "Gender", London: Routledge.
- Walsham, G. (1993). "Interpreting information systems in organizations". Chichester, Wiley.
- Myers, M.D. (1997). "Qualitative research in information systems." *MIS Quarterly*, Vol. 21, No.2, pp.241-242.
- Galliers, R. D. (ed.) (1992). "Information Systems Research: Issues, Methods and Practical Guidelines". Oxford, Blackwell Scientific Publications.
- Miles, M.B. and Huberman, A.M. (1994). "Qualitative data analysis", 2nd edition. Newbury Park, CA, Sage.
- Kaplan, B. and Duchon, D. (1988). "Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study" *Management Information Systems Quarterly*, Vol.12, No. 4, pp.571-586
- Benbasat, I. (1984) "An Analysis of Research Methodologies," in F. Warren McFarlan (Ed.), "The Information Systems Research Challenge ", Boston , HBS Press , pp.47-85.
- Cornford, T. and Smithson, S. (1996) *Project Research in Information Systems, A Student's Guide*. Basingstoke, Macmillan.
- Myers, M.D. (1997). "Qualitative research in information systems." *MIS Quarterly*, Vol. 21, No.2, pp.241-242.
- Miles, M.B. and Huberman, A.M. (1994). "Qualitative data analysis", 2nd edition. Newbury Park, CA, Sage.

- Alavi, M. (1994). "Computer-Mediated Collaborative Learning: An Empirical Evaluation." *MIS Quarterly*, Vol. 2, No. 18, pp. 159-174.
- Remenyi, D. and Williams, B. (1996) "The Nature of Research: Qualitative or Quantitative, Narrative or Paradigmatic?" *Information Systems Journal*, Vol. 6, pp 131-146.
- Leedy, P. and Ormrod, J.E. (2001). "Practical research: planning and design", 7th edition. New Jersey, Prentice-Hall
- Hussey, J. and Hussey, R. (1997). "Business research". Basingstoke, Palgrave
- Cavaye, A. (1996). Case study research: a multi-faceted approach for IS. "Information Systems Journal", Vol.6, No.4, pp.227-242
- Rapoport, R.N. (1970). "Three dilemmas in action research" *Human Relations*, Vol.23, No. 6, pp.499-513
- Denscombe, M. (2002) *Ground Rules for Good Research*. (Maidenhead:Open University Press).
- Benbasat, I.G., Goldstein, D.K. and Mead, M. (1987) "The case research strategy in studies of information systems", *MIS Quarterly*, Vol. 11, No. 3, pp. 369-386
- Yin, R.K. (1989) "Case Study Research: Design and Methods", 1st edition, Beverly Hills, CA, Sage.
- Bonoma, T. (1985) Case research in marketing: opportunities, problems, and a process. *Journal of Marketing Research*, Vol. 22, May, pp. 199-208.
- Kaplan, B. and Duchon, D. (1988). "Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study" *Management Information Systems Quarterly*, Vol.12, NO. 4, pp.571-586
- Creswell, J. W. (2003). "Research Design: Qualitative, Quantitative, and Mixed Methods Approaches". Thousand Oaks, Sage.
- Weisberg, Herbert F., and Bruce D. Bowen (1977) *An Introduction to Survey Research and Data Analysis*. San Francisco: W. H. Freeman and Co.

- Sekaran, U. (1992). "Research methods for business: a skill building approach", 2nd edition, New York, Chichester, Wiley.
- Habermas, Jurgen. (1989) *The Structural Transformation of the Public Sphere: An Inquiry Into a Category of Bourgeois Society*. Trans. Thomas Burger: The MIT Press
- Alvarez, R.M., Hall, T., and Roberts, B. (2007) Military Voting and the Law: Procedural and Technological Solutions to the Ballot Transit Problem. *Fordham Urban Law Journal*, Vol.34, No.3
- Amy, D. (2000) *Behind the Ballot Box: A Citizen's Guide to Voting Systems*. Praeger Westport, CT
- Bimber, B. (2003) *Campaigning Online: The Internet in U.S. Elections*. New York: University Press
- Green, T. (2000) *Voting in a Virtual World*. New Statesman. Vol.129, No.4517
- Gibson, M. Nixon, P., Ward, S. (2003) *Political Parties and the Internet: Net Gain?* New York: Routledge
- Kent, M., Harrison, T. and Taylor, M. (2006). *A Critique of Internet Polls as Symbolic Representation and Pseudo-Events*. *Communication Studies*, Vol.57, No.3
- Saco, D. (2002) *Cybering Democracy: Public Space and the Internet*. University of Minnesota Press: Minneapolis
- Shane, P. (2004) *Democracy Online: The Prospects for Political Renewal through the Internet*. New York: Routledge
- Nair, A. (2009) *Legislative body polls 'by June 2010'*. [Online]. Available: http://www.gulf-times.com/site/topics/article.asp?cu_no=2&item_no=266087&version=1&template_id=57&parent_id=56 [19 May 2009]
- National Democratic Institute (2009). *Qatar*. [Online]. Available:

- <http://www.ndi.org/qatar> [19 May 2009]
- Nohlen, D., Grotz, F. and Hartman, C. (2001) *Elections in Asia and the Pacific: A Data Handbook*. England: Oxford
- Permanent Election Committee (2008) *A Training Course Organized By Permanent Elections Committee, SCFA*. [Online]. Available: http://www.pecq.org.qa/news_21feb08_en.php [19 May 2009]
- Matrix (2000) *Internet Voting a Threat to Democracy*. Matrix: The Magazine for Leaders in Higher Education, Vol.1, No.3
- Trechsel, A. and Mendez, F. (2004) *The European Union and E-Voting: Addressing the European Parliament's Internet Voting Challenge*. New York: Routledge
- United States Government Accounting Office (2004) *Elections: Electronic Voting Offers Opportunities and Presents Challenges*. [Online]. Available: <http://www.gao.gov/new.items/d04766t.pdf> [19 May 2009]
- United States Government Accounting Office (2004) *Elections: Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way But Key Activities Need to be Completed*. [Online]. Available: <http://www.gao.gov/new.items/d05956.pdf> [23 May 2009]
- Yang, E and Gaines, K. (2004) *Voting Technology and the Law: From Chads to Fads and Somewhere in Between*. Social Education, Vol.68, No.6
- Dictionary.com. (2011) *Define voting at Dictionary.com*. [Online]. Available: <http://dictionary.reference.com/browse/vote> [23 May 2009]
- Randal L. Schwartz, Tom Phoenix. (2001) *Learning Perl, Making Easy Things Easy and Hard Things Possible, Third Edition* ISBN 10: 0-596-00132-0
- Isobel White. (2010) *Postal Voting & Electoral Fraud. Parliament and Constitution Centre*. [Online]. Available: <http://www.parliament.uk/documents/commons/lib/research/briefings/snpc-03667.pdf> [23 May 2009]

- Eckhard Jesse. (2003) Reform proposals to amend the electoral law, Bonn. [Online]. Available:
http://www.bpb.de/publikationen/3OXR5G,0,0,Wahlssystem_und_Wahlrecht.html [23 May 2009]
- Norbert Kersting. (2004) *Online Voting: an international comparison*. In Modern Governance / e-government, No.18, pp.16-23. [Online]. Available:
http://www.bpb.de/publikationen/5T5OEL,0,OnlineWahlen_im_internationalen_Vergleich.html [23 May 2009]
- RadioFan (2010) *voting machine on display at the Smithsonian National Museum of American History*. [Online]. Available:
http://en.wikipedia.org/wiki/Voting_machine [23 May 2009]
- M. Mackerras and I. McAllister (1999) *Compulsory voting, party stability and electoral advantage in Australia*. Vol.18, No.2, pp.217-233. [Online]. Available
http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6V9P-3W19G62-5&_user=10&_coverDate=06%2F30%2F1999&_rdoc=1&_fmt=high&_orig=gateway&_origin=gateway&_sort=d&_docanchor=&view=c&_searchStrId=1703568142&_rerunOrigin=scholar.google&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=5b5dc08fcc6cff9967af80cd2639b04b&searchtype=a [24 May 2009]
- Bahry, L. (1999) Election in Qatar: A Window of Democracy Opens in the Gulf. *Middle East Policy*, Vol.6, No.4. pp.118-126
- Khalaf, A. and Luciani, G. (2008) *Constitutional Reform and Political Participation in the Gulf*. Dubai: Gulf Research Center

- Greenway, P. and Robinson, G. (2000) *Lonely Planet Bahrain, Kuwait & Qatar*. 1st Edition. Australia: Lonely Planet Publications
- Tore Kjeilen (2010) *Qatar - Political situation [online]* Publisher: Looklex *Encyclopedia*. [Online]. Available: <http://i-cias.com/e.o/qatar.political.htm> [01 May 2010]
- Ahmed A. K (2009) *A Guide to Qatar's Legal System*. New York: GlobaLex. [Online]. Available: <http://www.nyulawglobal.org/globalex/Qatar.htm> [01 May 2010]
- Leigh Catherine Miles (2010) *Qatar - Political Context*. Washington: National Democratic Institute. [Online]. Available <http://www.ndi.org/qatar> [01 May 2010]
- Louay Bahry (2010) *Programme on Governance in the Arab Region: Qatar Election [online]* UNDP. [Online]. Available: <http://www.undp-pogar.org/countries/theme.aspx?cid=15&t=3> [05 May 2010]
- Nizar Hamzeh (2003) *Qatar: The Duality of the Legal System. Al Mashriq of Høgskolen i Østfold: Norway*. [Online]. Available: <http://Ddc.aub.edu.lb/projects/pspa/qatar.html> [05 May 2010]
- Zelaky, E.; Sami, S.; Ziada, D. (2006) *Implacable adversaries: Arab governments and the Internet*. Open Arab Internet: Syria. [Online]. Available: <http://www.openarab.net/en/node/359> [05 May 2010]
- Unknown (2010) *Qatar Profile. World-Map: USA*. [Online]. Available: <http://www.worldmap.org/maps/other/profiles/qatar/Qatar%20Profile.pdf> [05 May 2010]
- Unknown (2007) *Qatar: Election Results (1999 election 55%)*. Programme on Governance in the Arab Region: Beirut. [Online]. Available: <http://www.pogar.org/countries/theme.aspx?cid=15&t=3> [05 May 2010]

- Stephanie Miles (1999) *Intel's security headache spreads*. Staff Writer: CNET News. [Online]. Available: http://news.cnet.com/Intels-security-headache-spreads/2100-1001_3-222103.html [05 May 2010]
- Unknow (Unknow) *Candidate Interview Advice*. com: CNET News. [Online]. Available: <http://www.scom.com/candidates/interviewadvice.aspx> [05 May 2010]
- InfoDev (2002) *The e-Government Handbook for Developing Countries, Center of Democracy and Technology*. [Online]. Available <http://www.cdt.org/egov/handbook/> [06 May 2010]
- Davison, R.M., Wagner, C. and Ma, L.C. (2005) *From government to e-government: a transition model, Information Technology & People*, Vol.8, No.3, pp.280-299
- Reynolds, M. M. and Regio-Micro, M. Microsoft E-Government Initiatives. (2001) *Introduction: The Purpose Of Transforming Government-E-Government as a Catalyst In The Information Age*. [Online]. Available <http://www.netcaucus.org/books/egov2001/pdf/EGovIntr.pdf> [06 May 2010]
- Bonham, G., Seifert, J. and Thorson, S (2001) *The Transformational Potential of e-Government: The Role Of Political Leadership. The 4th Pan European International Relations Conference of the European Consortium for Political Research*. Canterbury-U.K.: The University of Kent
- Hazlett, Thomas W. (1990) ‘‘The Rationality of U.S. Regulation of the Broadcast Spectrum.’’ *Journal of Law and Economics*, Vol.33, pp.133-75
- Shafi Al-Shafi and Vishanth Weerakkody, (2010) *Adoption of Wireless Internet Parks: An Empirical Study in Qatar*. [Online]. Available: <http://www.iseing.org/emcis/emcis2008/Proceedings/Refereed%20Papers/Contributions/C%2070/Emcis08%20v7.00.pdf> [06 May 2010]
- IctQatar. (2007) *Free wireless internet in Qatar's public parks*. [Online]. Available: <http://www.ict.gov.qa/output/page422.asp> [07 May 2010]

- Qatar Statistic Authority (QSA) (2008) “*Population in Qatar*”. [Online]. Available http://www.qsa.gov.qa/eng/population_census/2009/population_census_July.htm [07 May 2010]
- Ministry of Foreign Affairs (2007a) “*General information*”. [Online]. Available: <http://english.mofa.gov.qa/details.cfm?id=6> [07 May 2010]
- Ministry of Foreign Affairs (2007b) “*Communications and transport*”. [Online]. Available: <http://english.mofa.gov.qa/details.cfm?id=107> [07 May 2010]
- Ministry of Foreign Affairs (2007c) “*Education*”. [Online]. Available: <http://english.mofa.gov.qa/details.cfm?id=28> [07 May 2010]
- United Nations Development Programme (2009) “*Human Development Report 2007/2008, Fighting climate change: Human solidarity in a divided world*”. [Online]. Available: <http://hdrstats.undp.org/fr/indicators/89.html> [07 May 2010]
- Central Intelligence Agency (CIA) (2008a) “*Middle East: Qatar*”. [Online]. Available: <https://cia.gov/library/publications/the-world-factbook/geos/qa.html> [08 May 2010]
- Amiri Diwan (2009) “*Economy Development*”. Qatar. [Online]. Available: http://www.diwan.gov.qa/english/qatar/Qatar_now.htm#Economy [08 May 2010]
- United States Department of State (2005) “*International Religious Freedom Report (2005)*”. Bureau of Democracy, Human Rights, and Labor. [Online]. Available: <http://www.state.gov/g/drl/rls/irf/2005/51608.htm> [08 May 2010]
- Sambidge, A. (2009a) “*Qatar's economy to see 9.6% growth in 2009 – report*”. [Online]. Available: <http://www.arabianbusiness.com/557317-qatars-economy-to-see-96-growth-in-2009---report> [08 May 2010]
- AME Info (2004) “*Literacy in the Arab world remains below the developed nations' minimum average of 95%*”. [Online]. Available at <http://www.ameinfo.com/33975.html> [08 May 2010]

- INTELSAT (2010) “*Qatar Telecom Secures Capacity on Intelsat 15 to Expand International Services*”. [Online]. Available: <http://www.intelsat.com/news-release/2010/20100303-1.asp> [08 May 2010]
- Ministry of Foreign Affairs (2007) *Qatar's Supreme Council for Communications and Information Technology (ictQatar)*. [Online]. Available: <http://english.mofa.gov.qa/details.cfm?id=115> [08 May 2010]
- ICTQatar, Decree Law No. (34) of 2006 on the promulgation of the Telecommunications Law, “This is an unofficial English translation of the Telecommunications Law of the State of Qatar which will be adopted and applied by Supreme Council for Information and Communications Technology(ictQATAR),” <http://www.ict.gov.qa/files/elaw.pdf>.
- ICT Qatar (2009b) “*Vodafone wins Qatar's second mobile license*”. [Online]. Available: <http://www.ictqatar.gov.qa/output/NewsPage.aspx?PageID=561> [09 May 2010]
- AME Info. (2008) “*Vodafone and Qatar Foundation take first steps towards launch of Vodafone Qatar*”. [Online]. Available: <http://www.ameinfo.com/154793.html> [09 May 2010]
- Internet World Stats (2009b) “*Internet Usage in the Middle East and in the World*”. [Online]. Available: <http://www.Internetworldstats.com/stats5.htm> [09 May 2010]
- Qtel (2009a) “*Qtel's Vision*”. [Online]. Available: <http://www.qtel.com.qa/IndexPage.do> [06 May 2010]
- Qtel (2009b) “*ADSL FAQ*”. [Online]. Available: <http://www.qtel.com.qa/ADSLFaq.do> [06 May 2010]
- Qtel (2009c) “*Dial Up – FAQ*”. [Online]. Available: <http://www.qtel.com.qa/DialupFaq.do> [06 May 2010]

- Qtel (2009d) “*Qatar’s Companies See Doubled Speeds with Qtel’s Ongoing Internet Broadband Business ADSL Enhancement*”. [Online]. Available:
<http://www.qtel.com.qa/SearchDetails.do?search=16741> [06 May 2010]
- U.S. Department of State Diploma in Action (2007) “*International Religious Freedom Report 2007 – Qatar*”. [Online]. Available:
<http://www.state.gov/g/drl/rls/irf/2007/90219.htm> [06 May 2010]
- Cooperation Council for the Arab States of the Gulf (GCC), Secretariat General (2001) “*The Economic Agreement between the GCC States Adopted by the GCC Supreme Council (22nd Session, 31 December 2001)*”. [Online]. Available:
<http://library.gcc-sg.org/English/Books/econagree2004.htm> [07 May 2010]
- Qatar Science and Technology Park (QSTP) (2007) “*Qatar innovator, news from the frontline of technology business in Doha*”, No.1. [Online]. Available:
<http://www.qstp.org.qa/files/other/QSTP%20Newsletter%20Apr07%20v16.html> [07 May 2010]
- Ashrafi, R., Yasin, M., Czuchry, A. and Al Hinai, Y. (2007) “*E-commerce practices in the Arabian Gulf GCC business culture: utilisation and outcomes patterns*”. Vol.2, No.4, pp.351-371. [Online]. Available:
<http://portal.acm.org/citation.cfm?id=1356448.1356449> [07 May 2010]
- ICT Qatar (2009e) “*QR 930m e-payments via e-Gov and Hukoomi*” Qatar. [Online]. Available: <http://www.ict.gov.qa/output/NewsPage.aspx?PageID=684> [07 May 2010]
- Ministry of Culture, Art and Heritage (2008) “*Our Mission*”. [Online]. Available:
http://www.nccah.com/e_mcah.htm [07 May 2010]
- Central Intelligence Agency (CIA) (2008a) “*Middle East: Qatar*”. [Online]. Available: <https://cia.gov/library/publications/the-world-factbook/geos/qa.html> [08 May 2010]
- Qatar Statistic Authority (QSA) (2008) “*Population in Qatar*”. [Online]. Available:
http://www.qsa.gov.qa/eng/population_census/2009/population_census_July.htm [08 May 2010]

- U.S. Department of State Diploma in Action (2007) *“International Religious Freedom Report 2007 – Qatar”*. [Online]. Available:
<http://www.state.gov/g/drl/rls/irf/2007/90219.htm> [08 May 2010]
- FIFA (2010) *“Russia and Qatar awarded 2018 and 2022 FIFA World Cups”*. [Online]. Available:
<http://www.fifa.com/worldcup/russia2018/news/newsid=1344698/index.html>
 [08 May 2010]
- Al-hamar. M, Dawson. R, Guan. L (2010) “A Culture of Trust Threatens Security and Privacy in Qatar” cit, pp.991-995, *10th IEEE International Conference on Computer and Information Technology*. UK: Bradford
- Central Intelligence Agency (CIA) (2008a) *“Middle East: Qatar”*. [Online]. Available: <https://cia.gov/library/publications/the-world-factbook/geos/qa.html> [08 May 2010]
- Al-Shafi, S. & Weerakkody, V. (2007) *Exploring E-government in the State of Qatar: Benefits, Challenges and Complexities*. European and Mediterranean
- Bertelsmann Stiftung, (2009) *BTI 2010 — Qatar Country, Report*. Gütersloh: Bertelsmann Stiftung
- ICTQatar, Decree Law No. (34) of 2006 on the promulgation of the Telecommunications Law, “This is an unofficial English translation of the Telecommunications Law of the State of Qatar which will be adopted and applied by Supreme Council for Information and Communications Technology(ictQATAR),” <http://www.ict.gov.qa/files/elaw.pdf>.
- BBC News, (2009) *“Country Profile: Qatar,” BBC News*. [Online]. Available:

- http://news.bbc.co.uk/2/hi/middle_east/country_profiles/791921.stm [11 March 2009]
- M.Al-Hamar, R. Dawson and J. Al-Hamar. (2011a) "*The Threat of Phishing to Systems Quality in the State of Qatar*". SQM paper
- M.Al-Hamar, R. Dawson and J. Al-Hamar. (2011b) "*The Need for Education on Phishing : A Survey Comparison of the UK and Qatar*". InSPIRE paper
- J.Al-Hamar, R. Dawson and M. Al-Hamar. (2011c) "*Internet Voting in the State of Qatar: The People's Quality Requirements*". SQM paper
- CyberVote (2008). [Online]. Available: <http://www.eucybervote.org/> [01 May 2010]
- J. Gilberg. (2003) E-VOTE: An Internet-based Electronic Voting System: Consolidated Prototype 2 Documentation, Technical Report. [Online]. Available: http://www.instore.gr/evote/evoteend/htm/3public/doc3/public/publicdeliverables/d74/Consolidated_Docu final.zip [01 May 2010]
- J. Benaloh. (1987) Verifiable Secret-Ballot Elections. *PhD thesis: Yale University*
- D. Chaum. (1981) Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of the ACM, Vol.24, No.2, pp.84-88*
- J. Benaloh. (1987) Verifiable Secret-Ballot Elections. *PhD thesis: Yale University*
- I. Damgård, J. Groth, and G. Salomonsen. (2003) *Secure Electronic Voting*, Kluwer Academic Publishers, Vol.6, pp.77-99
- A. Fujioka, T. Okamoto, and K. Ohta, (1993) *A Practical Secret Voting Scheme for Large Scale Elections*. In *Proceedings of AUSCRYPT '92*, pp.244-251

- D. Boneh and P. Golle, (2002) Almost Entirely Correct Mixing with Applications to Voting. In V. Atlury, editor, Proceedings of the 9th ACM Conference on Computer and Communication Security (CCS-02), pp.68-77. NewYork: ACM Press*
- J. Furukawa and K. Sako, (2001) An Efficient Scheme for Proving a Shuffle. In J. Kilian, editor, Advances in Cryptology – CRYPTO ' 2001, Lecture Notes in Computer Science, Vol.2139, pp.368-387. International Association for Cryptologic Research, Springer-Verlag: Berlin-Germany*
- P. Golle, S. Zhong, D. Boneh, M. Jakobsson, and A. Juels, (2002) Optimistic Mixing for Exit-Polls. In ASIACRYPT:Advances in Cryptology – ASIACRYPT: International Conference on the Theory and Application of Cryptology, Vol.2501, pp. 451-465*
- C. A. Neff, (2001) A Verifiable Secret Shuffle and Its Application to E-Voting. In P. Samarati, editor, Proceedings of the 8th ACM Conference on Computer and Communications Security, pp.116-125. Philadelphia-USA: ACM Press*
- D. Chaum, (1983) "Blind signatures for untraceable payments", Proceedings of CRYPTO82, pp.199-203. New York: Plenum Press*
- Bo Meng, (2007) "Analyzing and Improving Internet Voting Protocol," e-Business Engineering. ICEBE 2007. IEEE International Conference, pp.351-354. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4402113&isnumber=4402049> [01 May 2010]*
- Belanger, F.; Carter, L. (2010) "The Digital Divide and Internet Voting Acceptance," Digital Society, 2010. ICDS '10. Fourth International Conference, pp.307-310. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5432779&isnumber=5432399> [01 May 2010]*
- C-K. Wu, R. Sankaranarayana, (2002). Internet Voting: Concerns and Solutions. First International Symposium on Cyber Worlds (CW'02). pp. 261 – 266.*

- Schryen, G. (2004) "Security aspects of Internet voting," *System Sciences*, 2004. Proceedings of the 37th Annual Hawaii International Conference, pp.5-9. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1265298&isnumber=28293> [01 May 2010]
- Abadi, M. and A.D. Gordon, (1999) A calculus for cryptographic protocols: The spi calculation Information Computer, Vol.148, pp.1-70
- Abadi, M. and C. Fournet, (2001) Mobile values, new names and secure communication. *Proceedings of the 28th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*. London: UK. ACM New York: USA., pp.104-115
- Sako, K. and J. Kilian, (1995) *Receipt-free Mix-Type Voting Scheme*, A Practical Solution to the Implementation of a Voting Booth . In :*Advances in Cryptology- EUROCRYPT'95*, Guillou, L.C. and J.J. Quisquater (Eds.). Springer-Verlag, Berlin: Heidelberg. Pp.393-403
- Benaloh, J. and D. Tuinstra, (1994) *Receipt-free secret-ballot elections*. *Proceeding of the 26th Annual ACM Symposium on Theory of Computing*. New York: USA. pp.544-553
- Juels, A. and M. Jakobsson, (2002) Coercion-resistant electronic elections. [online]. Available: <http://www.vote-auction.net/VOTEAUCTION/165.pdf> [01 May 2010]
- Magkos ,E., M. Burmester and V. Chrissikopoulos, (2001) *Receipt-freeness in large-scale elections without untappable channels*. *Proceedings of the IFIP Conference on Towards the E-Society: E-Commerce, E-Business, E-Government*, uwer B.V., Deventer, The Netherlands, pp.683-694
- Acquisti, A. (2004) *Receipt-free homomorphic elections and write-in voter verified ballot*. CMU-ISRI-04-116, Carnegie Mellon Institute for Software Research International. [Online]. Available: http://www.heinz.cmu.edu/~acquisti/papers/acquisti-electronic_voting.pdf [01 May 2010]

- Chaum, D. (2004) *Secret-ballot receipts: True voter-verifiable elections*. IEEE Security Privacy, Vol.2, p.38-47
- Juels, A., D. Catalano and M. Jakobsson, (2005) *Coercion-resistant electronic elections*. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, Nov.07-07, Alexandria, VA, USA., pp:61-70.
- Chaum, D., P. Y.A. Ryan and S. Schneider, (2005) *A practical voter-verifiable election scheme*. *Proceedings of the ESORICS*, pp:118-139. Milan: Italy
- Rivest, R.L. (2006) *The threeBallot voting system*. [Online]. Available: <http://theory.csail.mit.edu/~rivest/Rivest-TheThreeBallotVotingSystem.pdf> [08 August 2010]
- Cichon, J., M. Kutyłowski and B. Glorz, (2008) *Short Ballot Assumption and Three ballot Voting Protocol*. In: *SOFSEM 2008: Theory and Practice of Computer Science*, Geffert, V. et al. (Eds.). Springer-Verlag, Berlin Heidelberg, pp:585-598.
- Clarkson, M.R., S. Chong and A.C. Myers, (2008) *Civitas: Toward a secure voting system*. *Proceeding of the 2008 IEEE Symposium on Security and Privacy*, May 18-21, pp.354-368. Oakland, California: USA.
- Meng, B. (2009a) *A secure internet voting protocol based on non-interactive deniable authentication protocol and proof protocol that two ciphertexts are encryption of the same plaintext*. *Networks*, Vol.4, pp.370-377
- Meng, B. and J.Q. Wang, (2010) *An efficient receiver deniable encryption scheme and its applications*, *Journal of Network*, Vol.5, pp.683-690
- Meng, B., Z.M. Li and J. Qin, (2010) *A receipt-free coercion-resistant remote internet voting protocol without physical assumptions through deniable encryption and trapdoor commitment scheme*, *Journal of the Software*, Vol.5:942-949
- Meng, B., W. Huang and J. Qun, (2010b) *Automatic verification of security properties of remote internet voting protocol in symbolic model*. *Inform, Journal of the Technology*, Vol.9, pp.1521-1556

- Meng, B., W. Huang and D.J. Wang, (2010c) Automatic verification of remote internet voting protocol in symbolic model Recent Advances in Electronic Commerce and Information Technology of ISECS
- Meng, B. (2008) *Formal analysis of key properties in the internet voting protocol using applied PI*, Journal of the calculus. Inform. Technol., Vol.7, pp.1133-1140
- Backes, M., C. Hritcu and M. Maffei, (2008a) *Automated verification of remote electronic voting protocols in the applied Pi-calculus*. Proceeding of the 21st IEEE Computer Security Foundations Symposium, IEEE Computer Society, pp.195-209. Washington: DC
- Backes, M., M. Maffei and D. Unruh, (2008b) *Zero-knowledge in the applied pi-calculus and automated verification of the direct anonymous attestation protocol*. Proceedings of the 29th IEEE Symposium on Security and Privacy, Preprint on IACR ePrint . pp: 202-215
- Meng, B. (2011) *Refinement of mechanized proof of security properties of remote internet voting protocol in applied PI calculus with proverif*. Journal of the Information Technology, Vol.10, pp.293-334. [Online]. Available: <http://docsdrive.com/pdfs/ansinet/itj/2011/293-334.pdf> (extract references) [18 May 2010]
- Bo Meng, (2008) "A Formal Analysis of Coercion-Resistance of the Internet Voting Protocol Based on DKR Formal Model," Information Processing (ISIP), 2008 International Symposiums, pp.490-494. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4554137&isnumber=4554037> [18 May 2010]
- Dini, G. (2002) "Increasing security and availability of an Internet voting system," Computers and Communications. Proceedings. ISCC 2002. Seventh International Symposium, pp. 347- 354. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1021700&isnumber=21983> [01 May 2010]

- Bruschi, D.; De Cindio, F.; Ferrazzi, D.; Poletti, G.; Rosti, E. (2002) "Internet voting: do people accept it? Do they trust it?," *Database and Expert Systems Applications, 2002. Proceedings. 13th International Workshop*, pp.437. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1045936&isnumber=22410> [01 May 2010]
- California Internet Voting Task Force (CIVTF) (2000) "A Report on the Feasibility of Internet Voting". [Online]. Available: www.sos.ca.gov/elections/ivote/ [01 May 2010]
- National Science Foundation (NSF) (2001) "Internet Policy Institute," Report of the National Workshop on Internet Voting: Issues and Research Agenda (Washington). [Online]. Available: www.news.findlaw.com/cnn/docs/voting/nsfe-voterprt.pdf [13 May 2010]
- Parakh, A.; Kak, S. (2008) "Internet Voting Protocol Based on Implicit Data Security," *Computer Communications and Networks, 2008. ICCCN '08. Proceedings of 17th International Conference*, pp.1-4. [Online]. Available: URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4674300&isnumber=4674160> [13 May 2010]
- D. Chaum, (2004) *Secret-Ballot Receipts: True Voter-Verifiable Elections*. IEEE Security & Privacy, Vol.2, No.1, pp.38-47
- A. Riera and P. Brown, (2004) *Bringing Confidence to Electronic Voting*. EJEG, Vol.2, No.1
- P. Vora, (2004) *Citizen Verified Voting: An implementation of Chaum's voter verifiable scheme*. Talk given at the DIMACS Workshop on Electronic Voting, Rutgers U., NJ
- L. Cranor and R. Cytron, (1996) *Design and Implementation of a Practical Security-Conscious Electronic Polling System. Technical Report WUCS-96-02: Washington University*

- A. Fujioka, T. Okamoto, and K. Ohta, (1993) *A Practical Secret Voting Scheme for Large Scale Elections*. In Proceedings of AUSCRYPT '92, pp.244-251
- M. A. Herschberg, (1997) *Secure Electronic Voting Over the World Wide Web*. Master's thesis: MIT
- B. W. DuRette. (1999) *Multiple Administrators for Electronic Voting*. Bachelor's thesis: MIT
- R. Joaquim, A. Zúquete, and P. Ferreira, (2003) *REVS – A Robust Electronic Voting System*. IADIS International Journal of WWW/Internet, Vol.1, No.2
- Orhan Cetinkaya, (2008) "Analysis of Security Requirements for Cryptographic Voting Protocols", 3rd IEEE International Conference on Availability, Reliability and Security, pp.1451-1456
- purushothama, B.R.; Pais, A.R. (2009) "Design and Implementation of Secure Internet Based Voting System with User Anonymity Using Identity Based Encryption System," *Services Computing, SCC '09*. IEEE International Conference, pp.474-481. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5283919&isnumber=5283890> [13 May 2010]
- Anane R, Freeland R, Theodoropoulos G. (2007) "e-Voting Requirements and Implementation", *E-Commerce Technology and the 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services*, pp.382-392
- Jinn-Ke Jan, Chih-Chang Tai, (1997) "A secure electronic voting protocol with IC cards", *Journal of Systems and Software*, IEEE publication 1995, pp.93-101
- John R. Vacca, (2004) *Public Key Infrastructure Building Trusted Applications and Web Services*. New York: Auerbach publications
- Kiayias, A.; Korman, M.; Walluck, D. (2006) "An Internet Voting System Supporting User Privacy", *IEEE 22nd Annual conference on Computer Security Applications*, pp.165-174

- Kwangjo Kim, Jinho Kim, Byoungcheon Lee, Gookwhan Ahn, (2001) "Experimental Design of Worldwide Internet Voting using PKP", SSGRR2001. L'Aquila: Italy*
- Ibrahim S, Kamat M, Salleh M, Aziz S.R.A. (2003) "Secure Evoting with blind signature", Proceedings of the 4th IEEE National Conference on Telecommunication Technology, pp.193-197*
- P. Bonetti, S. Ravaoli, and S. Piergallini, (2000) The Italian academic community's electronic voting system. Computer Networks, Vol.34, No.6, p.851-860*
- R. Cramer, M. Franklin, B. Schoenmakers, and M. Yung, (1996) Multi-authority secret bollat elections with linear work. In Advances in Cryptology, EUROCRYPT'96, Lecture Notes in Computer Science, Vol.1070, pages72-83*
- R. Cramer, R. Gennaro, and J. Borrell, (1997) A secure and optimally efficient multi-authority election scheme. In Advances in Cryptology, EUROCRYPT'97, Lecture Notes in Computer Science, Vol.1233, pp.103-117*
- J. - K. Jan, Y. - Y. Chen, and Yi - Lin, (2001) The design of protocol for e-voting on the Internet. In Proceedings of the IEEE International Carnahan Conference on Security Technology, pp.180-189. London: England*
- J. - K. Jan and C. - C. Tai, (1997) A secure electronic voting protocol with IC cards. Journal of Systems and Software, Vol.39, No.2, pp.93-101*
- W. - C. Ku and S. - D. Wang, (1999) A secure and practical electronic voting scheme. Computer Communicarions, Vol.22, No.3, pp.279-286*
- C. L. Lei and C. I. Fan, (1998) A universal single-authority election system. IEICE Transactions on Fundamentals, Vol.E81-A, No.10, pp.2186-2193*
- A. Riera, J. Rif a, and J. Borrell, (2000) Efficient construction of vote-tags to allow open objection to the tally in electronic elections. Information Processing Letters, Vol.75, No.5, pp.211-215*
- H. T. Liaw (2004) A secure electronic voting protocol for general elections. Computers & Security, Vol.23, No.2, pp.107-119*

- C. C. Chang and J. S. Lee, (2006) *An anonymous voting mechanism based on the key exchange protocol*. Computers & Security, Vol.25, No.4, pp.307-314
- Chun-Ta Li; Min-Shiang Hwang; Yan-Chi Lai; (2009) *"A Verifiable Electronic Voting Scheme over the Internet,"* Information Technology: New Generations, 2009. ITNG '09. Sixth International Conference. [Online]. pp.449-454.
Available:
<http://ieeexplore.ieee.org/Xplore/login.jsp?url=http%3A%2F%2Fieeexplore.ieee.org%2Fstamp%2Fstamp.jsp%3Ftp%3D%26arnumber%3D5070659%26isnumber%3D5070575&authDecision=-203> [13 May 2010]
- Wachowicz, J. (2010) *"Bidirectional voting and continuous voting concepts as possible use of Internet in democratic voting process,"* Computer Science and Information Technology (IMCSIT), Proceedings of the 2010 International Multiconference, pp.599-603. [Online]. Available:
<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5680038&isnumber=5679615> [03 May 2010]
- D. Chaum, (1981) *"Untraceable Electronic Mail, Return Address and Digital Pseudonyms"*, Communications of the ACM, Vol.24, No.2, pp.84-88
- C. Boyd, (1990) *"A New Multiple Key Cipher and an Improved Voting Scheme"*, Advances in Cryptology-EUROCRYPT'89 Proceedings, pp.617-625
- J. Borrell and J. Rifa, (1996) *"An Implementable Secure Voting Scheme"*, Computers & Security, Vol.15, No.4, pp.327-338
- C. I. Fan and C. L. Lei, (1997) *"A multi-Recastable Ticket Scheme for Electronic Elections"*, Advances in Cryptology - ASIACRYPT'96 Proceedings, Springer-Verlag, pp.116-124
- J. K. Jan and R. H. Lin, (1995) *"A Secure Anonymous Voting by Employing Diffie-Hellman PKD Concept"*, IEEE International Carnahan Conference on Security Technology-England, pp.252-258
- D. Chaum, C. Crepeau, and I. B. Damgrad, (1988) *"Multiparty Unconditionally Secure protocols"*, Proceedings of the 20th ACM Symposium on Theory of

Computing, pp.87-119

- J. D. Cohen, (1986) "Improving Privacy in Cryptographic Elections", Technical Report, YALEUDCSRR-454. Computer Science Department: Yale University*
- R. Cramer, M. Franklin, B. Schoenmakers, and M. Yung, (1997) "Multi-Authority Secret-Ballot Elections with Linear Work", Advances in Cryptology - EUROCRYPT'96 Proceedings, Springer-Verlag, pp.72-83*
- L. Harn and T. Kiesler, (1991) "How to Hold an Election over Computer Network", Workshop on Information Security & Modern Cryptography, Taiwan, R.O.C., pp.129-138*
- D. Chaum, (1985) "Security without Identification: Transaction Systems to Make Big Brother Obsolete", Communications of the ACM, Vol.28, No.10, pp.1030-1044*
- D. Chaum, (1988) "Blinding for Unanticipated Signatures", Advances in Cryptology - EUROCRYPT'87 Proceedings, Springer-Verlag, pp.227-233*
- A. Fujioka, T. Okamoto, and K. Ohta (1993) "A practical Secret Voting Scheme for Large Scale Elections", Advances in Cryptology - AUCRYPT'92 Proceedings, Springer-Verlag, pp.6.15-6.19*
- Yi Mu and Vijay Varadharajan, (1998) "Anonymous Secure E-Voting over a Network", Computer Security Applications Conference. Proceedings. 14* Annual, pp.293-299*
- D. Chaum, (1981) "Untraceable Electronic Mail, Return Address and Digital Pseudonyms", Communications of the ACM, Vol.24, No.2, pp.84-88*
- D. Chaum, (1989) "Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA", Advances in Cryptology - EUROCRYPT '88 Proceedings, Springer-Verlag, pp. 177-182*
- J. K. Jan and R. H. Lin, (1995) "A Secure Anonymous Voting by Employing Diffie-Hellman PKD Concept", IEEE International Carnahan Conference on Security Technology-England, pp.252-258*

- W. S. Juang and C. L. Lei, (1996) "A Collision-Free Secret Ballot Protocol for Computerized General Elections", Computers & Security, Vol.15, No.4, pp.339-348*
- J. K. Jan and C. C. Tai, (1997) "A Secure Electronic Voting Protocol with IC Cards", Journal of Systems and Software, Vol.39, PP.93-101. U.S.A.*
- H. Nurmi, A. Salomaa, and L. Santeau, (1991) "Secret Ballot Elections in Computer Networks", Computers & Security, Vol.10, No.6, pp.553-560*
- P. H. Slespenger, (1991) "Socially Secure Cryptographic Election Scheme", Electronics Letters, Vol.27, No.11, pp.955-957*
- Jinn-Ke Jan; Yu-Yi Chen; Yi Lin, (2001) "The design of protocol for e-voting on the Internet," Security Technology, 2001, IEEE 35th International Carnahan Conference pp.180-189. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=962831&isnumber=20784> [01 May 2010]*
- K. Kim. Killer Application of PKI to Internet Voting. In IWAP 2002. Springer Verlag, 2002. Lecture Notes in Computer Science No. 1233.*
- D. Jefferson, A. Rubin, B. Simmons, and D. Wagner, (2004) A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE). [Online]. Available: <http://servesecurityreport.org/> [19 May 2010]*
- J. Schwartz, (2004) Online Voting Canceled for Americans Overseas. The New York Times*
- RIES (Year) facts and features sheet. [Online]. Available: [http://www.surfnet.nl/bijeenkomsten/ries/RIES Word1.doc](http://www.surfnet.nl/bijeenkomsten/ries/RIES%20Word1.doc) [19 May 2010]*
- Andrew Myers (2003) Condorcet Internet Voting Service. [Online]. Available: <http://www.cs.cornell.edu/andru/civs.html> [19 May 2010]*
- Evm (2003) The Electronic Voting Machine Project. [Online]. Available: <http://evm2003.sourceforge.net> [19 May 2010]*

- GNU.FREE (2004) Heavy-Duty Internet Voting.[Online]. Available: <http://www.j-dom.org/users/re.html> [19 May 2010]*
- Schneier, B. (1996) Applied Cryptography, Second Edition - Protocols, Algorithm and Source Code in C. John Wiley and Sons.*
- Alkhelaiji, M, Alja'am, J. and Al-Sayrafi, M. (2009) Towards an Electronic Voting System for the State of Qatar. [Online]. Available from <http://ieeexplore.ieee.org/Xplore/login.jsp?url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F5210688%2F5227822%2F05227947.pdf%3Ftp%3D%26arnumber%3D5227947%26punumber%3D5210688&authDecision=-203> [04 December 2010]*
- Carley, J. (2008) Legislative Voting and Accountability (Cambridge Studies in Comparative Politics). London: Cambridge University Press*
- Cranor, L. (1999) Electronic Voting, ACM Crossroads. [Online]. Available: <http://www.acm.org/crossroads/xrds2-4/voting.html> [04 November 2010]*
- Friel, B. (2006) Let the Recounts Begin. National Journal, Vol.24, No.2, pp.321-322*
- Glass, R. (1999) Evolving a New Theory of Project Success. Communications of the ACM, Vol.41, No.7, pp.21-132*
- Gritzalis, D. (2006) Secure Electronic Voting. Norwell. Massachusetts: Kluwer Academic Publishers*
- Mehdi, K. (2001) Managing Information Technology in a Global Economy [e-Book]. [Online]. Available from http://books.google.com/books?id=7Cq7nDrm5cEC&pg=PA1045&lpg=PA1045&dq=legal+challenges+in+internet+voting&source=bl&ots=PjE9F_Vbfz&sig=ITmbip5mbilPyS7_wnmLxnJlrHg&hl=en&ei=Ntf4TJXBAsGF4Qb84LDEBw&sa=X&oi=book_result&ct=result&resnum=3&ved=0CCgQ6AEwAg#v=onepage&q=legal%20challenges%20in%20internet%20voting&f=false [04 December 2010]*

- Mendez, F. and Trechsel, A. (2008) The European Union and E-Voting: Addressing the European Parliaments Internet Voting Challenge. London: Routledge Publishers*
- Metz, G. (1996) Virtual Voters. School Library Journal, Vol.42, No.9, pp.138-145*
- Niemi, M. (2008) Voting Technology: The Not-So-Simple Act of Casting a Ballot. Washington, D.C: Brookings Institution Press*
- Rubin, A. (2006) Brave New Ballot: The Battle to Safeguard Democracy in the Age of Electronic Voting. New York: Broadway Publishers*
- Schaffer, C. (2008) The Hidden Costs of Clean Election Reform. New York: Cornell University Press*
- Strassman, M. (1999) Could the Internet Change Everything? Journal of State Government, Vol.72, No.2, pp.41-54*
- Thornburgh, D. and Celeste, R. (2006) Asking the Right Questions About Electronic Voting. Chicago: National Research Council*
- EPA. Gov. (2005) Energy policy act of 2005. [Online]. Available: http://www.epa.gov/oust/fedlaws/publ_109-058.pdf [18 November, 2010]*
- Google Inc (2010) 'Powering a Google search,' Official Google Blog. [Online]. Available: <http://googleblog.blogspot.com/2009/01/powering-google-search.html> [20 November 2010]*
- Green IT (2010) Annual international conference on green IT 2010. [Online]. Available: <http://www.greenitconf.org/> [20 November, 2010]*
- Green IT (2010) Eco-efficiency and Eco-innovation for IT. [Online]. Available: www.greenit.net [25 November 2010]*
- Harris, J. (2008) Green computing and green IT best practices: on regulations and industry. New York: Lulu.com*

- Hird, G. (2008) *Green IT in Practice. Cambridgeshire: IT Governance Publishing*
- Jones, E. (2006) EPA announces new computer efficiency requirements. [Online]. Available: <http://yosemite.epa.gov/opa/admpress.nsf/a8f952395381d3968525701c005e65b5/113b0c0647fee41585257210006474f1!OpenDocument> [28 November 2010]
- Kevin, M. (2003) 'Cost-Reduction Quagmire: Structured ASIC and Other Options,' FPGA and Programmable Logic Journal. [Online]. Available: http://www.fpgajournal.com/articles/20041123_quagmire.htm [28 November 2010]
- Mingay, S. (2007) Gartner: 10 Key Elements of a 'Green IT' Strategy. [Online]. Available: www.onsitelasermedic.com/pdf/10_key_elements_greenIT.pdf [28 November 2010]
- San, M. (2008) "Harnessing green IT: principles and practices", IEEE IT Professional, January-February 2008, pp.24-33
- Schuhmann, D. (2005) Strong showing: high-performance power supply units. [Online]. Available: http://www.tomshardware.com/2005/02/28/strong_showing/page38.html [01 December 2010]
- The White House (2007) Office of the Press Secretary: Executive Order: Strengthening Federal Environmental, Energy, and Transportation Management. [Online]. Available: <http://georgewbush-whitehouse.archives.gov/news/releases/2007/01/20070124-2.html> [01 December 2010]
- Abercrombie, N., Hill, S., Turner, B. S. (1984) *Dictionary of sociology*. Harmondsworth: Penguin

- Campbell, D. T., Stanley, J. C. (1966) *Experimental and quasi-experimental designs for research*. Chicago: Rand McNally
- Chaum, D. (1983) Blind signatures for untraceable payments. In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds.) *Crypto 82*, pp.199-203
- Chaum, D. (1981) *Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms*. CACM, Vol.24, No.2, pp.84-88
- Estonian National Electoral Committee (2007a) *Main Statistics of E-Voting*. [Online]. Available: [http://www.vvk.ee/english/Ivoting comparison 2005 2007.pdf](http://www.vvk.ee/english/Ivoting%20comparison%202005%202007.pdf) [05 May 2011]
- Estonian National Electoral Committee (2007b) *Parliamentary elections 2007: Statistics of e-voting*. [Online]. Available: [http://www.vvk.ee/english/Ivoting stat eng.pdf](http://www.vvk.ee/english/Ivoting%20stat%20eng.pdf) [05 May 2011]
- European Union Democracy Observatory (2007) *Report for the Council of Europe: Internet Voting in the March 2007 Parliamentary Elections in Estonia*. [Online]. Available: [http://www.vvk.ee/english/CoE and NEC Report E-Voting 2007.pdf](http://www.vvk.ee/english/CoE%20and%20NEC%20Report%20E-Voting%202007.pdf) [05 May 2011]
- Fujioka, A., Okamoto, T., Ohta, K. (1993) A Practical Secret Voting Scheme for Large Scale Elections, In: Seberry, J., Zheng, Y. (eds.) *AUSCRYPT 1992*. LNCS, Vol.718, pp.244-251. Springer-Berlin: Heidelberg
- Krimmer, R., Triessnig, S., Volkamer, M. (2008) The Development of Remote E-Voting Around the World: A Review of Roads and Directions. In: Alkassar, A., Volkamer, M. (eds.) *VOTE-ID 2007*. LNCS, Vol.4896, pp.1-15. Springer-Berlin: Heidelberg
- Mohen, J., Glidden, J. (2001) *The Case for Internet Voting*. CACM, Vol.44, No.1, pp.72-85
- OSCE: OSCE/ODIHR (2007) *Election Assessment Mission Report in the 2007 parliamentary elections in Estonia*. [Online]. Available: [http://www.vvk.ee/english/OSCE report EST 2007.pdf](http://www.vvk.ee/english/OSCE%20report%20EST%202007.pdf) [05 May 2011]

- Philips, D.M., von Spankovsky, H.A. (2001) *Gauging the Risks of Internet Elections*. CACM, Vol.44, No.1, pp.73-85
- Ragib, C. C., Becker, H. S. (1992) (eds.): *What is a case? Exploring the foundations of social inquiry*. Cambridge: Cambridge University Press
- Solvak, M., Pettai, V. (2008) The parliamentary elections in Estonia, March 2007. *Notes on Recent Elections/Electoral Studies*, Vol.27, No.3, pp.547-577
- Stake, R.E. (1995) *The art of case study research*. London: Thousand Oaks- Sage Publications
- A Yin, R.K. (2003) *Applications of case study research*, 2nd ed. Sage Publications, Thousand Oaks, London, New Delhi
- BYin, R.K. (2003) *Case study research: design and methods*, 3rd ed. Sage Publications, Thousand Oaks, London, New Delhi
- Jensen, J.L. and Rodgers, R. (2001) "Cumulating the intellectual gold of case study research". *Public Administration Review*, Vol.61, No.2, pp.236-246
- Perry, C. (2001) "Case research in marketing". *The Marketing Review* 2001. [Online]. Available: www.themarketingreview.com [05 May 2011]
- Welman, C. and Kruger, F. (1999) "*Research methodology for the business and administrative sciences*". Cape Town, Oxford University Press
- Myers, M.D. (1997) "Qualitative research in information systems." *MIS Quarterly*, Vol.21, No.2, pp.241-242
- Tellis, W. (1997) Introduction to case study. *The Qualitative Report*, Vol.3, No.2. [Online]. Available: www.nova.edu/ssss/QR/QR3-2/tellis1.html [05 May 2011]
- Cavaye, A. (1996) Case study research: a multi-faceted approach for IS. *Information Systems Journal*, Vol.6, No.4, pp.227-242
- Yin, R.K. (1989) *Case Study Research: Design and Methods*, 1st edition. Beverly Hills-CA: Sage

- Yin, R.K. (1994) *Case Study Research: Design and Methods*, 2nd edition. Newbury Park: Sage
- Stake, R.E. (1995) *The art of case study research*. London: Sage
- Alavi, M. and Carlson, P. (1992) A review of MIS research and disciplinary development. *Journal of Management Information Systems*, Vol.8, No.4, pp.45-62
- Orlikowski, W.J. and Baroudi, J.J. (1991) Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information Systems Research*, Vol. 2, No.1, pp.1-28
- DTI and PriceWaterHouseCoopers (2006), *Information Security Breaches Survey 2006 – Technical Report* [online]. Available from: <http://www.dti.gov.uk/files/file28343.pdf>, [Accessed on 3rd June 2010]
- Dowland P.S, Furnell S.M, Illingworth H.M and Reynolds P.L (1999). *Computer crime and abuse: A survey of public Attitude and awareness*, Computers & Security, vol. 18, Part 8, Pages 715-726
- Federal Trade Commission (2006a), *Financial Institutions and Customer Data: Complying with the Safeguards Rule*. Available from: <http://www.ftc.gov/bcp/online/pubs/buspubs/safeguards.htm>, [Accessed 22nd December 2009]
- Federal Trade Commission (2006b), *Information Security*. Available from: <http://www.ftc.gov/bcp/online/edcams/infosecurity>, [Accessed 22nd December 2009]
- Fox, (2002) “Cyberspace Invaders”, Consumer Reports. Available from: <http://www.consumerreports.org>, [Accessed 22nd January 2010].

- Furnell S.M, Alayed A, Barlow I, Dowland P.S (2002) *Critical awareness – The problem of monitoring security vulnerabilities*, Proceedings of European Conference on Information Warfare and Security, Brunel, UK, Pages 85-92
- Furnell S.M, Gennatou M, Dowland P.S (2002) *prototype tool for information security awareness and training*, International Journal of Logistics Information management, vol. 15, Part 5, Pages 352-357
- Kvavik, R. B., and Voloudakis, J. (2003). *Information Technology Security: Governance, Strategy, and Practice in Higher Education*. [online] Research Study Roadmap published by the EDUCAUSE Center for Applied Research. Available from:
http://www.educause.edu/ir/library/pdf/ecar_so/ers/ERS0305/ECM0305.pdf
 [Accessed 13th January 2010]
- Khalaf, A. and Luciani, G. (2008) *Constitutional Reform and Political Participation in the Gulf*. Gulf Research Center.
- Mitnick, Kevin D (2003), *The Art of Deception: Controlling the Human Element of Security*, Hungry Minds Inc: U.S.
- National Infrastructure Security Co-ordination Centre (2003), *NISCC Quarterly Review, January – March 2003*. Available from: <http://www.niscc.gov.uk>,
 [Accessed 3rd January 2010]
- Schultz E (2005), “*The human factor in security*”, Computer & Security, Vol. 24, part 6, Pages 425-426.
- Aloul, F.A. (2010). Information security awareness in UAE: A survey paper. *Internet Technology and Secured Transactions (ICITST)*. no (1), pp.1-6, 8-11.
- Talib, S.; Clarke, N.L.; Furnell, S.M. (2010). An Analysis of Information Security Awareness within Home and Work Environments. *ARES '10 International Conference*. no (1), pp196-203, 15-18.

- Boujettif, M.; Yongge Wang. (2010). Constructivist Approach to Information Security Awareness in the Middle East. *Broadband, Wireless Computing, Communication and Applications (BWCCA)*. no (1), pp.192-199, 4-6.
- Tolnai, A.; von Solms, S. (2010). Solving security issues using Information Security Awareness Portal. *Internet Technology and Secured Transactions*. no (1), pp.1-5, 9-12.
- Smith, M. (2006). The Importance of Employee Awareness to Information Security. *The Institution of Engineering and Technology Conference on Crime and Security* . no (1), pp.115-128, 13-14.
- Meister, E.; Biermann, E. (2008). Implementation of a Socially Engineered Worm to Increase Information Security Awareness. *Third International Conference on Broadband Communications, Information Technology & Biomedical Applications*. no (1), pp.343-350, 23-26.
- Hailian, K.; Zhenggang, W.. (2009). Research on E-Learning-Based Educational Technology Training Model for College Teachers. *Ninth International Conference on Hybrid Intelligent Systems*. 3 (1), pp.206-210, 12-14.
- Dede, C. (1996). "Emerging technologies and distributed learning". *American Journal of Distance Education*, Vol.10, No. 2, pp. 4-36.
- Kearsley, G. (Ed.) (2005). "Online learning: Personal reflections on the transformation of education". NJ: Educational Technology Publications.
- Willems, J. (2005). "Flexible learning: Implications of "when-ever", "where ever" and "what-ever"". *Distance Education*, Vol. 26, No.3, pp.429-435.
- Khan, B. (Ed.) (1997). "Web-based instruction". NJ, Educational Technology Publications.

- Edelson, D. C., Gordin, D. N. and Pea, R. D. (1999). "Addressing the challenges of inquiry-based learning through technology and curriculum design". *The Journal of the Learning Sciences*, Vol. 8, Nos.3&4, pp.391-450.
- Edelson, D. C. and O'Neill, D. K. (1994). "The CoVis collaboratory notebook: Supporting collaborative scientific inquiry." In: *Proceedings National Educational Computing Conference, Recreating the Revolution*, pp. 146-152.
- Hall, B. (1997). "Web-Based Training Cookbook, Everything you need to know for online training". Wiley Computer Publishing, New York, p. 10.
- Zenger, J. and Uehlein, C. (2001) "Why Blended Will Win", *Training and Development Magazine*, VOL. 55, No. 8, pp. 54-60
- Fletcher, J.D. (1991). "Multimedia Review". pp 33-42.
- Pea, R. D. (1994). "Seeing what we build together: Distributed multimedia learning environments for transformative communications." *The Journal of the Learning Sciences*, Vol.3, No.3, pp. 285-299.
- Auditmypc (2011). "free security scan, web tools and information to keep you secure!". Available at: <http://www.auditmypc.com/firewall-test.asp> [26 April 2010].
- Al-Hamar, M. K., (2010). *Reducing the Risk of E-mail Phishing in the State of Qatar through an Effective Awareness Framework*. Thesis, (PhD). University of Loughborough.
- Herzberg, A. (2008). "Why Johnny can't surf (safely)? Attacks and defenses for web users". Department of Computer Science, Bar Ilan University, Ramat Gan, Israel.

- Downs, J.S., Holbrook, M. and Cranor, L.F. (2007). "Behavioral Response to Phishing Risk". *Proceedings 2nd Annual eCrime Researchers' Summit*, October 4-5, pp. 37-44.
- Masatoshi Kawakami, Hiroshi Yasuda, Ryoichi Sasaki (2010). "Development of an E-learning Content-Making System for Information Security (ELSEC) and its Application to Anti-phishing Education." *Proceedings, 2010 International Conference on e-Education, e-Business, e-Management and e-Learning*, pp.7-11.
- Roy G. Saltman. (1988). Accuracy, Integrity, and Security in Computerized Vote-Tallying. *Institute for Computer Sciences and Technology*.
- Zúquete, A., Costa, C., Romão, M. (2007). An intrusion-tolerant E-voting client system. *1st Workshop on Recent Advances on Intrusion-Tolerant Systems*.
- Volkamer, M., Alkassar, A., Sadeghi, A.-R. and Schulz, S. (2006). 'Enabling the application of open systems like pcs for online voting. *Frontiers in Electronic Elections*.
- Sadeghi, A.R., Selhorst, M., Stübke, C., Wachsmann, C., Winandy, M. (2006). Tcg inside?: a note on tpm specification compliance. *Proceedings of the first ACM workshop on Scalable trusted computing*. no (7), pp. 47–56.
- C. Andrew Neff. (2004). *Practical high certainty intent verification for encrypted votes*. [online] Available: <http://www.votehere.net/vhti/documentation>. [20th Aug 2010].
- Chaum, D. (unknown). *Secret-Ballot Receipts and Transparent Integrity. Better and less-costly electronic voting and polling places*. [online] Available: <http://www.vreceipt.com/article.pdf>. [10th Aug 2010].
- P.Y.A. Ryan. (2004). A variant of the chaum voting scheme. *Technical Report CS-TR-864*.

- David Chaum, Aleksander Essex, Richard Carback, Jeremy Clark, Stefan Popoveniuc, Alan T. Sherman, and Poorvi Vora. (2008). : End-to-end voter verifiable optical-scan voting. *IEEE Security and Privacy*.
- Kutylowski, M., Zagórski, F. (2007). Internet voting solving secure platform problem. *International Workshop on Security - IWSEC*. no (0), pp 199-213.
- Skagestein, G., Haug, A.V., Nødtvedt, E., Rossebø, J.E.Y. (2006) How to create trust in electronic voting over an untrusted platform. *Electronic Voting*. pp. 107–116.
- Allen House holder, Art Manion, Linda pesante, George M. Weaver. (2001). Managing the Threat of Denial-of-Service Attacks. *CERT/C CCERT Coordination Centre*. [online] available: www.cert.org/archive/pdf/Managing_DoS.pdf [01st Feb 2010].
- Brickell, E., Camenisch, J., Chen, L. (2004). Direct anonymous attestation. *Proceedings of the 11th ACM conference on Computer and Communications Security*. pp 132–145.
- Xianju Geng; Whinston, A.B. (2000). Defeating distributed denial of service attacks. *IT Professional*. 2 (4). pp 36 – 42
- T. Morgan and R. D. Kriz and S. Howard and F. Das Neves and J. Kelso. (2001) Extending the Use of Collaborative Virtual Environments for Instruction to K-12 Schools
- A. Chou, J. Yang , B. Chelf , S. Hallem , D. Engler.(2001). An Empirical Study of Operating System Errors. *Proc. 18th ACM Symp. Operating System Principles*, ACM Press, pp. 73–88.
- Garfinkel, S. and Spafford, G. and Schwartz, A. (2003). *Practical UNIX and Internet security*. O'Reilly. pp. 34-56.
- Daniel J. Barrett, Richard E. Silverman, and Robert G. Byrnes. (2005). *SSH: The Secure Shell (The Definitive Guide)*, O'Reilly.

- Comer, Douglas E. (2006). *Internetworking with TCP/IP: Principles, Protocols, and Architecture*. 1 (5th ed.). Prentice Hall.
- Sabiha Hossain, Upama Kabir, Shaila Rahman and Alope Kumar Saha. (2011). JXTA & Web Services Using Secret Key Based Encryption, *International Journal of Computer and Information Technology*, IJCIT, 1, (02), pp. 71—75.
- W3Schools organisation. (2011). *Asynchronous JavaScript and XML Tutorial*. [online] Available: <http://www.w3schools.com/ajax/default.asp>. [21st July 2011].
- Avaliktos, N. (2004). *The election process revisited*. [Online] Nova Publishers, p.152
- U.S Department of State (2010) *Background Note: Qatar, 2010*. [Online]. Available at: <http://www.state.gov/r/pa/ei/bgn/5437.htm> [31 December 2010].
- Emir Sheikh Hamad bin Khalifa Al-Thani. 2009. *Qatar Country Reports on Human Rights Practices*, [Online] Available at: <http://www.historycentral.com/nationbynation/Qatar/Human.html> [31 December 2010].
- Gronlund, A., (2002). *Electronic government: design, applications and management*. [Online] Idea Group Inc (IGI), p.80 Available at: <http://books.google.co.in/books?id=heJUDmmlkRoC&pg=PA80&dq=definition+of+internet+voting&hl=en#v=onepage&q=definition%20of%20internet%20voting&f=false> [31 December 2010].
- Unknown. (2007) *Internet Law - Internet Voting becomes a Reality in Estonia; Global Experts Question Online Security and Inclusiveness*. [Online] iBLS. Available at: http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1699 [31 December 2010].
- Kim, W., (2001). The human society and the Internet: Internet-related socio-economic issues: *First International Conference Human.Society@Internet*, Seoul, Korea, pp. 289.

- Unknown. (2010). Qatar Science & Technology Park. [Online] Available at:
<http://www.qstp.org.qa/output/page7.asp> [31 December 2010].
- National Science Foundation. (2001). National Workshop on Internet Voting. [Online] *Find Law. Report*. Available at:
<http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/election2000/nsfe-voterprt.pdf> [31 December 2010].
- S Al-Shafi and V Weerakkody., 2010. *Factors Affecting E-Government Adoption in the State of Qatar*. [Online] EMCIS. Available at:
<http://www.iseing.org/emcis/EMCIS2010/Proceedings/Accepted%20Refereed%20Papers/C101.pdf> [31 December 2010].
- Sharp, J.M., (2004). *Qatar: Background and U.S. Relations*. [Online] Available at:
<http://fpc.state.gov/documents/organization/33741.pdf> [31 December 2010].
- Brian Wesolowski (2010) *Tag Archive for 'Technology', 2010*. [Online] Digital Qatar. Available at: <http://www.digitalqatar.net/tag/technology/> [31 December 2010].
- White, J.D., (2007). *Managing information in the Public Sector*. [Online]. Sharpe, pp. 120 Available at:
http://books.google.co.in/books?id=UrcCT_OrZ5gC&pg=PA119&dq=digital+divide+for+internet+voting&hl=en#v=onepage&q=digital%20divide%20for%20internet%20voting&f=false [31 December 2010].
- Dow Jones, (2007). Qatari Officials Pleased With Voter Turnout In Municipal Poll.
- Qatar Foundation. (2011). "Education City". Available at <http://www.qf.org.qa/> [25 August 2010].
- ICDL GCC Foundation (2009). "Our role" Qatar. Available at
<http://www.icdlgcc.com/aboutus.htm> [23 June 2011]