E-MAIL ENCRYPTION FRAMEWORK FOR MALAYSIAN PUBLIC SECTOR

NUR ATIQAH BT MUHAMMAD

UNIVERSITI TEKNOLOGI MALAYSIA

E-MAIL ENCRYPTION FRAMEWORK FOR MALAYSIAN PUBLIC SECTOR

NUR ATIQAH BT MUHAMMAD

A project report submitted in fulfillment of the
requirements for the award of the degree of
Master of Science (Information Assurance)

Advance Informatics School
Universiti Teknologi Malaysia

JUNE 2016

DEDICATION

To my beloved mother, Asmah bt Itam, to my pillar of strength; my husband and sons, Izlan, Zaqhwan and Zaheen.
Whose gives constant source of inspiration and courage.
Thank you

ACKNOWLEDGEMENT

In preparing this thesis, I was in contact with many people, academicians and practitioners. They have contributed towards my understanding and thought. In particular, I wish to express my sincere appreciation to my main thesis supervisor, Dr. Ganthan Narayana Samy, for encouragement, guidance, critics, advices and motivation. Without his continued support and interest, this thesis would not have been the same as presented here. My friends should also be recognized for their support. My sincere appreciation also extends to all my colleagues and others who have provided assistance at various occasions. Their views and tips are useful indeed. Unfortunately, it is not possible to list all of them in this limited space. I am grateful to all my family members.

ABSTRAK

Memelihara dan manjaga keselamatan data sulit ynag dikongsi melalui mel elektronk adalah bergantung kepada kaedah penyulitan (enkripsi) yang digunakan oleh pembekal perkhidmatan e-mel serta tertakluk kepada prosedur dan peraturan organisasi yang sedang berkuatkuasa. Oleh itu, rangka kerja enkripsi e-mel menjadi faktor asas dalam mereka bentuk sistem perkhidmatan e-mail yang selamat bagi Perkhidmatan Sektor Awam di Malaysia. Dengan itu, kajian ini bertujuan untuk membangunkan rangka kerja enkripsi e-mail bagi Sektor Awam di Malaysia dalam usaha untuk memelihara system e-mel. Dalam kajian ini, kajian kualitatif telah dijalankan untuk memahami kriteria yang diperlukan bagi rangka kerja enkripsi e-mel bagi Sektor Awam di Malaysia. Bagi mengkaji ciri-ciri rangka kerja enkripsi e-mel bagi Sektor Awam di Malaysia melalui pentadbir e-mel dan kakitangan yang berkaitan, kaedah kajian diskriptif telah dilaksanakan. Selaras dengan itu, temubual secara mendalam menggunakan kaedah temubual semi struktur telah diguna pakai dalam kajian ini. Rangka kerja enkripsi e-mel telah dicadangkan, dimana rangka kerja ini terdiri daripada komponen organisasi, operasi, teknologi, perundangan dan etika. Rangka kerja yang dicadangkan kemudian telah dinilai untuk mengukur keberkesanannya terhadap system e-mel sedia ada. Penemuan dapatan dari rangka kerja yang dicadangkan akan memberi manfaat kepada Sektor Awam di Malaysia dalam memberikan perkhidmatan e-mel yang selamat disamping memilih kawalan keselamatan yang bersesuaian. Akhir sekali, kajian ini secara umunya menyumbang untuk meningkatkan tahap keselamatan sistem e-mel Sektor Awam di Malaysia yang dilaksankan pada masa ini.

ABSTRACT

Securing confidential data shared through the electronic mail is depending on the current encryption method deployed by the E-mail service provider as well as the current procedures and regulation of the organization. Hence, the E-mail encryption framework is a fundamental factor in designing a secure E-mail service in the Malaysian Public Sector. Therefore, the purpose of this study is to develop the E-mail encryption framework for Malaysian Public Sector in order to secure the E-mail system. In this study, the qualitative study has been conducted in order to understand the criteria of the E-mail encryption framework for the Malaysian Public Sector. Thus, the descriptive design is conducted to discover the features E-mail encryption framework for Malaysian Public Sector from the E-mail administrator and related personnel. Therefore, in-depth interview with the semi-structured method of interview is used in this study. The E-mail encryption framework has been proposed which comprising of organizational, operational, technological, legal and ethical components. The proposed framework was evaluated to measure its effectiveness towards an existing e-mail system. Findings on the proposed e-mail encryption framework will benefit the Malaysian Public Sector in providing secure e-mail service thus deciding applicable security control. Finally, this study generally contributes to enhance the current secure e-mail system implementation in Malaysian public sector agencies.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
5.4	E-mail Encryption Deployment Constrains	90
5.5	E-mail Service Deployments	92
5.6	E-mail Service Deployments	93
5.7	Initiatives to Establish Ethical Value	95

LIST OF APPENDICES

LIST OF ABBREVIATIONS

SMTP	-	Simple Mail Transfer Protocol
POP	-	Post Office Protocol
S/MIME	-	Secure/Multipurpose Internet Mail Extension
PKI	-	Public Key Infrastructure
IBE	-	Identity Based Encryption
MUA	-	Mail User Agent
MTA	-	Mail Transfer Agent
LDA	-	Local Delivery Agent
IMAP	-	Internet Message Access Protocol
HTTP	-	Hypertext Transfer Protocol
TLS	-	Transport Layer Security
SSL	-	Secure Socket Layer
PGP	-	Pretty Good Privacy
CA	-	Certificate Authority
PKG	-	Private Key Generator
DNS	-	Domain name system
DNSSEC	-	Domain Name System Security Extensions

CHAPTER 1

INTRODUCTION

1.1 Overview

Information located on a user's computer is shared to other users through the network communication using electronic mail (E-mail) system. Figure 1.1 shows how E-mail system works where sending and receiving E-mail message is possible by using the E-mail program that also known as an E-mail client, guaranteed the communication within short time and at any place possible. A server that connects to the E-mail client is used to stores and delivers users' E-mail. E-mail server contains valuable information of user's message that most of the commercial E-mail service provider has the right to access.

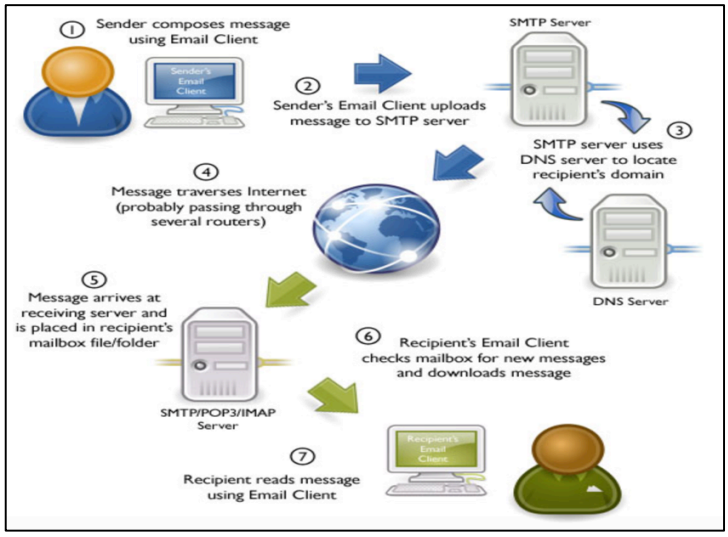

Figure 1.1 How E-mail Works (www. Onlymyemail.com)

An electronic mail that carries important and confidential information transferred over the network is accessible to many kinds of attack. Eavesdroppers who attempt to steal particular information are possible to intercept the E-mail communication intentionally copy or alter the E-mail content. Network attack can also harm the E-mail system by exploiting the network application layer component resulting the communication on E-mail system probable been compromise and content of E-mail is simply exposed to public release.

Consequently, there is a need to secure the information shared through the network to preserve its confidentiality and privacy. The Secure/Multipurpose Internet Mail Extension (S/MIME) is a broadly recognized protocol that provide secure and private communication by sending digitally signed and encrypted message. However, current E-mail encryption solution involves tedious process on public key certificates validity and trusted key management issues.

1.2 Background of the problem

1.2.1 Malaysia Public Service's Official E-mail

E-mail service is widely used nowadays as an official means or personal purpose or even social media needs. Malaysian Public Sector through the 'Guidelines on Procedure for Using Internet and Electronic Mail in Government Agencies by Prime Minister Office, 2003' specified that government officers are required to use official E-mail service to communicate within the organization or beyond to save time, resources needs and travelling cost.

Government data is particularly sensitive, which is not simply can be shared and transfer through the untrusted network. By using any free account E-mails services (e.g.; Yahoo! mail, Gmail, AIM mail, iCloud mail) the information are exposed to risk of any misused, tempered or others. According to Oppliger (2004), commercial E-mail services providers are capable to retrieve every E-mail data from their user even if the user has deleted the message from their inbox. Tariq & Arif (2014) found that 70% of users never explore their E-mail account's privacy and security setting, which is 52% of users, put trust on E-mail provider to secure

account holder information. Moreover, E-mail service that are widely offered by free account E-mails services are relying on security protocol that are commonly deploys by most of the E-mail service offered which is S/MIME and PGP (Vandenwauver & Jorissen 1998). Hence, the used of commercial E-mail in official business put risk to the organization. Official E-mail objective is to preserve the information shared within the ministries and by utilizing own server; the ministry will have the rights to control the information and access to the data.

1.2.2 Securing Confidential Data

Dealing with classified data that bring the high impact result to the nation is a huge challenge to Malaysian Public Sector. Malaysian Public Sector deals with important information including cabinet papers, project papers related to hi-impact reputation, confidential documents and others. Project papers and documents that label as classified information are certainly carried sensitive data that are strictly limited to be reviewed by authorized personnel. Leakage on confidential documents that possibly by the E-mail service will leads a massive problem on the national level where it reflect the integrity and trust on Government Agencies. Likewise, the leakage on confidential information related to the high impact project of such as in Education Sector in Malaysia through the project papers or minutes of meeting, which can provide critical information on sensitive issues that will lead to lost of trust by public towards the national education system.

Commonly, classified documents in Government agencies are documented manually, which was recorded according to the classified document's procedures and assigned responsible personnel in charged on the document's movement. In accordance with the E-mail technologies nowadays and the ease of use, confidential documents are barely transferred within the network by relying the communication network secured by E-mail services. Level of security on E-mail service of Malaysian Public Sector is critically needs to be enhanced to protect the content of classified document that are transferred through E-mail.

1.2.3 Malaysian Public Sector E-mail System

Existing e-mail system that deploys by Malaysian Public Sector is relying on communication security of the system which trusting on the network security itself. Current e-mail system for Malaysian Public Sector employs Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP). E-mail system works on SMTP to transmit message between servers over the Internet. SMTP is a basic protocol for E-mail transfer where no description of any security and privacy policy while the POP Servers act as a gate that gives E-mail users to access to the E-mail stored in the user's account on the server. Therefore, add-on protocols and procedures are deploys to make e-mail communication secure and private. The information on E-mail content should be encrypted to ensure the integrity of sensitive data is well preserved. The Secure/Multipurpose Internet Mail Extension (S/MIME) is a broadly recognized protocol that provide two security service that is sending digitally signed and encrypted message. Digital signature and message encryption is the essential function of S/MIME that provide a comprehensive solution to the security issues on SMTP.

Likewise, security protocols used by e-mail services that provide confidentiality and authentication of the E-mail system is currently facing a serious potential attack from its widely used and well-known algorithm (Schneier et al. 2015). Attack on E-mail system possibly from the poor network administration that allows an eavesdropping during the communication. Possible attack on E-mail service as discuss by Katz & Schneier (2000) prove that the security on E-mail system has to be the main consideration for the organization when dealing with the confidential documents or E-mail content. Encryption is the fundamental technique used by most of security protocol to protect E-mail content (Mohammed et al. 2013). Encryption used key to encrypt and decrypt the information to make it impossible to understand by illegitimate user during the transaction in the Internet. E-mail security protocol used by most of the E-mail service ensure the E-mail user are protected from any attack is S/MIME and PGP (Banday 2011). This protocol are used at the client side defines several cryptographic algorithm such as Tripe DES (TDES), AES, RSA, Diffe-Hellman, SHA-1 and Digital Signature. Similarly, the security of E-mail in transmission process could be enhanced using the identity password as discussed by Niu & Jiang (2014).

1.2.4 Public Key Cryptography

Digital signature and message encryption is the essential function of S/MIME that provide a comprehensive solution to the security issues on SMTP. Digital signature feasible on public key cryptography in a way to facilitate key management service. Digital signature able to identify the message sender in order to authenticate the user by public key cryptography method through handling the private and public key between user and E-mail service provider.

The S/MIME uses Public Key Infrastructure (PKI) framework to managing the keys for encryption purpose. PKI suffering with certificate management including certificate application, revocation and verification and the high cost that involved in managing the infrastructure, (Ellison & Schneier 2000).

Malaysian Public Sector currently relying on trusted third party on providing the digital certificate used on E-mail service. The high cost for public key certificate management and dependencies of the credential trust management makes these E-mail security protocols are considered less cost and trust effective for Malaysian Public Sector.

Thus, the existing frameworks of E-mail encryption need to be improving to enhance the E-mail security system. Result of the study will provide an E-mail encryption framework that serve to guide the establishment of E-mail encryption in Malaysia Government Public Sector. Subsequently, secured E-mail system with reliable encryption protocol and independent key management presented.

1.3 Problem Statement

Securing confidential data shared through the electronic mail is depending on the current encryption method deployed by the E-mail service provider as well as the current procedures and regulation of the organization/agencies. Numbers of constraint in E-mail encryption such as restriction on the add-on security protocol, credential trust on key management issues and public key certificate management essentially the factors that has to be focused by the E-mail provider.

Malaysian Public Sector e-mail services challenge with the e-mail encryption standard (S/MIME) limitation, which relying on PKI in delivering digital signature to provide authentication on encryption process. Digital signature creates difficulty on adopting the standard as both sender and receiver needs to install certificates on the E-mail client, where the certificates management including certificate application, revocation and verification found as complex process and high cost. Hence, the E-mail encryption framework is fundamental factor on designing a secure E-mail service in Malaysian Public Sector. The framework serves as the guideline to overcome the limitation of E-mail encryption system as a way to protect confidential and classified information transferred through the official E-mail service.

1.4 Research Question

To reach the research objectives, following research question are develop:

i. What are the components considered in designing the E-mail encryption framework for Malaysian Public Sector in providing secure E-mail service?
ii. How to design the proposed E-mail encryption framework that to provides encrypted and secure system?
iii. How to evaluate the proposed E-mail encryption framework to measure its effectiveness towards existing E-mail system?

1.5 Objectives of the study

The purpose of this study is to develop the E-mail encryption framework for Malaysian Public Sector to secure the E-mail system. This study is an aspiration to achieve objectives as stated below:

i. To identify the components that has to be considered in designing the proposed E-mail encryption framework for Malaysian Public Sector in providing secure E-mail service.
ii. To design the proposed E-mail encryption framework that to provides encrypted and secure system.
iii. To evaluate the proposed E-mail encryption framework to measure its effectiveness towards existing E-mail system.

1.6 Scope of the study

This study will provide safeguard on the confidentiality, integrity and authenticity of the E-mail sender, receiver and content, the E-mail security protocol will be deploys on existing E-mail system. This study will focus on determining the components of the E-mail encryption to improving the key management on existing system. The scopes of this study as below:

i. Field setting scope concentrates on the Malaysia Government Agencies that govern the Public Sector E-mail service and related private sector agencies that involves in government E-mail project.
ii. In-depth interview with the selected Malaysian Government Agencies and private sector company that manage the Malaysian Public Sector E-mail service are conducted in order to get initial view to develop proposed conceptual framework. Each interview will be documented and recorded precisely to be use in analysis phase.

1.7 Significance of the study

This study wills gives significant contribution to ensure that e-mail system for Malaysian Public Sector are encrypted and secure. Secure E-mail service will guarantee the confidentiality of classified document, preserved and difficult to

temper. This study will be focusing on the development of the e-mail encryption framework, which can be a standard on securing e-mail system in Malaysian Public Sector.

1.7.1 Theoretical Contribution

Encryption implementation on the communication medium such as e-mail service has proven to facilitate assurance on the information carried throughout the connection. Classified information used widely in most of the organization possibly contains the most important data for organization. The means to preserve classified information is to ensure data transferred in e-mail system are as its original format, resources and value. Detailed analysis on the literature will establish the theoretical framework, which furthered on investigating potential components that relevant to establish the secure e-mail system.

1.7.2 Practical Contribution

Existing e-mail encryption infrastructure elements are explored to identify the components that significantly affect the e-mail encryption method. Findings on the proposed e-mail encryption framework will benefit the Malaysian Public Sector in providing secure e-mail service thus deciding applicable security control. Finally, this study contributes to better understanding of secure e-mail system infrastructure using encryption method; therefore enhance current secure e-mail system implementation in Malaysian Public Sector agencies.

1.8 Summary

This chapter covers of the overview of the propose project which discuss the background of the problem, statement of the problem, objective of the study, research question, project hypothesis, scope of this research and significant of the research.

Background of problem mainly describes the recent situation of research study's environment, subject that will focus on and important of its usage. Statement of the problem explains current issues that are found demanding on existing environment system. Objective of the study express mechanism that is used to solve current system difficulty while research question specifies how it will be resolve.

The scope of this study describes elements that are considered towards the research process. Significant of this study justify the important components that are influenced in this research and how it is affected. Contribution of this study briefly illustrates the impact of the research towards the entire organizations and public environment. In Chapter 2, the literature review and in Chapter 3 the research methodology has been discussed and finally in chapter 4, the initial finding has been explained.

REFERENCES

Abdalla, M. et al., 2010. Wildcarded Identity-Based Encryption. *Journal of Cryptology*, 24(1), pp.42–82.

Amin, R., Ryan, J. & Dorp, J. van, 2012. Detecting Targeted Malicious Email. *IEEE Security Privacy*, 10(3), pp.64–71.

Babrahem, A.S. et al., 2015. Study of the Security Enhancements in Various E-mail Systems. *Journal of Information Security*, 06(01), pp.1–11.

Balakrishnan, S.K. & Jagathy, R.V.P., 2015. Practical implementation of secure email system based on IBE, DNS and proxy service. In Proceedings of 2014 IEEE International Conference on Advanced Communication, Control and Computing Technologies, ICACCCT 2014. pp. 1801–1806.

Banday, M.T., 2011. Effectiveness and Limitations of E-mail Security Protocols. *International Journal of Distributed and Parallel Systems (IJDPS), Academy & Industry Research Collaboration Centre, AIRCC, ISSN*, pp.0976–9757.

Banday, M.T. & Sheikh, S.A., 2014. S/MIME with multiple e-mail address certificates: A usability study. *Proceedings of 2014 International Conference on Contemporary Computing and Informatics, IC3I 2014*, p.p 707–712.

Baninajarian, N., Abdullah, Z. & Bolong, J., 2011. The Role Of Email In Improving Task Performance Among The Executives In Malaysia.

Boneh, D. & Franklin, M., 2001. Identity-Based Encryption from the Weil Pairing. In J. Kilian, ed. *Advances in Cryptology — CRYPTO 2001*. Lecture Notes in Computer Science. Springer Berlin Heidelberg, pp. 213–229.

Bostan, A. & Akman, I., 2013. ICT user and usage characteristics and e-mail security awareness. In *2013 10th International Conference on Electronics, Computer and Computation, ICECCO 2013, November 7, 2013 - November 8, 2013*. 2013 International Conference on Electronics, Computer and Computation, ICECCO 2013. IEEE Computer Society, pp. 277–280.

C.Barker, W., 2016. Domain Name System-Based Security for Electronic Mail - White Paper.

Charles Parker, 1999. E-mail use and abuse. *Work Study*, 48(7), pp.257–260.

Choukse, D. et al., 2012. Designing secure email infrastructure. In *9th IEEE and IFIP International Conference on Wireless and Optical Communications*

Networks, WOCN 2012, September 20, 2012 - September 22, 2012. IFIP International Conference on Wireless and Optical Communications Networks, WOCN. IEEE Computer Society.

Craigen, D., 2014. Assessing Scientific Contributions: A Proposed Framework and Its Application to Cybersecurity. *Technology Innovation Management Review*, 4(11), pp.5–13.

Cristian Thiago Moecke & Melanie Volkamer, 2013. Usable secure email communications: criteria and evaluation of existing approaches. *Information Management & Computer Security*, 21(1), pp.41–52.

Crouch, M. & McKenzie, H., 2006. The logic of small samples in interview-based qualitative research. *Social Science Information*, 45(4), pp.483–499.

Dumka, A. et al., 2014. Taxonomy of E-mail Security Protocol. *International Journal of Innovative Research in Computer and Communication Engineering*.

Ellison, C. & Schneier, B., 2000. Ten risks of PKI: What you're not being told about public key infrastructure. *Comput Secur J*, 16(1), pp.1–7.

Forsythe Focus, 2015. 7 Key Elements of a Successful Encryption Strategy. *Forsythe Focus*.

Fortinet, 2011. Fortimail Identity Mail Encryption - White Paper.

Garfinkel, S.L., 2003. Email-based identification and authentication: an alternative to PKI? *IEEE Security Privacy*, 1(6), pp.20–26.

Ghafoor, A., Muftic, S. & Schmolzer, G., 2010. CryptoNET: Design and implementation of the secure email system. In *2009 1st International Workshop on Security and Communication Networks, IWSCN 2009, May 20, 2009 - May 22, 2009*. 2009 Proceedings of the 1st International Workshop on Security and Communication Networks, IWSCN 2009. IEEE Computer Society.

Guest, G., Bunce, A. & Johnson, L., 2006. How Many Interviews Are Enough? An Experiment with Data Saturation and Variability. *Field Methods*, 18(1), pp.59–82.

Hélène O'Connora, Nancy Gibson, (2013), *Step-by-Step Guide to Qualitative Data Analysis*

Hsieh, H.-F. & Shannon, S.E., 2005. Three Approaches to Qualitative Content Analysis. *Qualitative Health Research*, 15(9), pp.1277–1288.

Internet Engineering Task Force-RFC2440, 1998. OpenPGP Message Format. A

Internet Engineering Task Force-RTF5751, 2010. Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification.

Jin, L., Takabi, H. & Joshi, J.B.D., 2010. Security and privacy risks of using e-mail address as an identity. In *2nd IEEE International Conference on Social Computing, SocialCom 2010, 2nd IEEE International Conference on Privacy, Security, Risk and Trust, PASSAT 2010, August 20, 2010 - August 22, 2010*. IEEE Computer Society, pp. 906–913.

Katz, J. & Schneier, B., 2000a. A Chosen Ciphertext Attack Against Several E-mail Encryption Protocols. In *USENIX Security Symposium*.

Katz, J. & Schneier, B., 2000b. A Chosen Ciphertext Attack Against Several E-mail Encryption Protocols. In *USENIX Security Symposium*.

Kihidis, A., Chalkias, K. & Stephanides, G., 2010. Practical implementation of identity based encryption for secure e-mail communication. In *14th Panhellenic Conference on Informatics, PCI 2010, September 10, 2010 - September 12, 2010*. Proceedings - 14th Panhellenic Conference on Informatics, PCI 2010. IEEE Computer Society, pp. 101–106.

Kościelny, C., Kurkowski, M. & Srebrny, M., 2013. PGP Systems and TrueCrypt. In *Modern Cryptography Primer*. Springer Berlin Heidelberg, pp. 147–173.

Kounelis, I., Muftic, S. & Loschner, J., 2014. Secure and privacy-enhanced e-mail system based on the concept of proxies. In *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2014, May 26, 2014 - May 30, 2014*. 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2014 - Proceedings. IEEE Computer Society, pp. 1405–1410.

Kumar, S., 2012. A Secure Email System Based on Identity Based Encryption. *International Journal*, 1(1).

Kuzhalvaimozhi, S. & Raghavendra Rao, G., 2012. Identity based cryptosystem: A new paradigm in public key infrastructure. *Communications in Computer and Information Science*, v 269 CCIS, n PART I, p.p 336–341.

MacDougall, C. & Fudge, E., 2001. Planning and Recruiting the Sample for Focus Groups and In-Depth Interviews. *Qualitative Health Research*, 11(1), pp.117–126.

Mason, M., 2010. Sample Size and Saturation in PhD Studies Using Qualitative Interviews. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, 11(3).

Mohammed, M.T. et al., 2013. Chaotic Encryption Based PGP Protocol. *International Journal of Computer Science and Telecommunications*. Available at: http://www.ijcst.org/Volume4/Issue2/p1_4_2.pdf

M.W. Al-Saadoon, G., 2011. Authentication and Virus Detection Enhancement for Client and Server Applications. *ISSN 2079-8407*, Volume 2 No.8, AUGUST 2011.

Niu, P. & Jiang, Z.T., 2014. Analysis of E-mail Security Events and its Solutions. In *Applied Mechanics and Materials*. Trans Tech Publ, pp. 712–716.

Oppliger, R., 2004. Certified mail: the next challenge for secure messaging. *Communications of the ACM*, 47(8), pp.75–79.

Park, E.G. & Zwarich, N., 2008. Canadian government agencies develop e-mail management policies. *International Journal of Information Management*, 28(6), pp.468–473.

Roschke, S. et al., 2010. Secure Communication Using Identity Based Encryption. In B. D. Decker & I. Schaumüller-Bichl, eds. *Communications and Multimedia Security*. Lecture Notes in Computer Science. Springer Berlin Heidelberg, pp. 256–267.

Schneier, B. et al., 2015. *Surreptitiously Weakening Cryptographic Systems*, IACR Cryptology ePrint Archive, 2015: 97.

Schreier, M., 2014. Qualitative content analysis. *The sage handbook of qualitative data analysis*, pp.170–183.

Shamir, A., 1985. Identity-based cryptosystems and signature schemes. In *Advances in cryptology*. Springer, pp. 47–53.

Sheng, Y., Rong, J. & Xiang, W., 2015. Simulation of the Users' Email Behavior Based on BP-BDI Model. In *2015 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*. 2015 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). pp. 16–22.

Shirley Daniels, 1997. Making e-mail secure. *Work Study*, 46(6), pp.207–214.

Shon Harris, (2013), *All In One CISSP Exam Guide, Sixth Edition*, McGraw Hill

Shukla, R. et al., 2014. Pehchanmail: IBE Based E-Token Authenticated Secure Email.

S. Kvale, (1996). *Interviews: An Introduction To Qualitative Research Interviewing.* Sage Publications.

Tariq, Z. & Arif, R., 2014. Usability analysis on security of E-mail accounts: Differences between fantasy and reality. *International Journal of Security and its Applications*, 8(5), pp.85–96.

Tracy, M. et al., 2007. NIST SP 800-45 Version 2, Guidelines on Electronic Mail Security.

Ula, M., Ismail, Z. & Sidek, Z.M., 2011. A Framework for the governance of information security in banking system. *Journal of Information Assurance & Cyber Security*, pp.1–12.

Vandenwauver, M. & Jorissen, F., 1998. Securing Internet Electronic Mail. In *State of the Art in Applied Cryptography*. Lecture Notes in Computer Science. Springer Berlin Heidelberg, pp. 209–223. A

Wen, S. et al., 2014. Modeling and Analysis on the Propagation Dynamics of Modern Email Malware. *IEEE Transactions on Dependable and Secure Computing*, 11(4), pp.361–374.

Yang, Y., 2014. Efficient identity-based key encapsulation scheme with wildcards for email systems. *International Journal of Communication Systems*, v 27, n 1, p.p 171–183.