



Saurashtra University

Re – Accredited Grade 'B' by NAAC
(CGPA 2.93)

Kathiriya, Dhaval R., 2006, “*Designing & generating prototype for E-Governance based election strategy using biometric authentication and smart card device*”, thesis PhD, Saurashtra University

<http://etheses.saurashtrauniversity.edu/id/eprint/336>

Copyright and moral rights for this thesis are retained by the author

A copy can be downloaded for personal non-commercial research or study, without prior permission or charge.

This thesis cannot be reproduced or quoted extensively from without first obtaining permission in writing from the Author.

The content must not be changed in any way or sold commercially in any format or medium without the formal permission of the Author

When referring to this work, full bibliographic details including the author, title, awarding institution and date of the thesis must be given.

Saurashtra University Theses Service
<http://etheses.saurashtrauniversity.edu>
repository@sauuni.ernet.in

DESIGNING & GENERATING PROTOTYPE FOR
E-GOVERNANCE BASED ELECTION STRATEGY
USING BIOMETRIC AUTHENTICATION AND
SMART CARD DEVICE

A THESIS SUBMITTED TO
SAURASHTRA UNIVERSITY, RAJKOT
FOR THE AWARD OF
DOCTOR OF PHILOSOPHY IN COMPUTER
SCIENCE
IN THE FACULTY OF SCIENCE



SUBMITTED BY
DHAVAL R. KATHIRIYA
DEPARTMENT OF COMPUTER SCIENCE
SAURASHTRA UNIVERSITY, RAJKOT

UNDER THE GUIDANCE OF
DR. N. N. JANI
PROF. & HEAD
DEPARTMENT OF COMPUTER SCIENCE
SAURATHRA UNIVERSITY, RAJKOT

February 2006

CERTIFICATE

I hereby certify that Mr. Dhaval R. Kathiriya has completed his thesis for doctorate degree entitled "Designing & Generating Prototype for e-Governance based Election Strategy using Biometric Authentication and Smart Card Device". I further certify that the research work done by him is of his own and original and is carried out under my guidance and supervision. For the thesis that he is submitting, he has not been conferred any degree, diploma or distinction by either the Saurashtra University or any other University according to best of my knowledge.

Place: Rajkot

Date:

Dr. N.N. Jani
Prof. & Head
Department of Computer Science
Saurashtra University, Rajkot.

CERTIFICATE

I certify that the developed model for e-Governance and strategies derived by analysis and described in the thesis has been based on the literature survey, bibliographical references and through study of the web sites in respect of related areas.

Apart from these, all the analysis, hypothesis, inferences and interpretation of data and strategy have been my own and original creation. The model has been prototyped to a domain, which is my own and original creation. Moreover, I declare that the work done in the thesis, either the Saurashtra University or any other university has not conferred any degree, diploma or distinction on me before.

Place: Rajkot

Date:

Dhaval R. Kathiriya

ACKNOWLEDGEMENT

I express my profound sense of gratitude to Dr. N.N. Jani - my research guide, who provides me undeviating encouragement, indefatigable guidance and valuable suggestions throughout the research project.

I take opportunity to express my deep sense of gratitude to Dr. K. P. Joshipura, Vice-Chancellor of the Saurashtra University for his consistent encouragement to the research and development.

I express my gratitude to all those officials in Collector office of Junagadh and Rajkot district, who spared their precious time to me and thus provided me valuable information and insight into various important issues related to the study.

I also give my sincere thanks to faculty members and of Department of Computer Science, Saurashtra University, who debated few key issues and offered critical comments on several aspect of the study. I am also thankful to the administrative staff of the department, who has always been a support of inspiration during my entire work.

I am highly indebted to my parents, my wife and sister, all my relatives and friends who constantly inspired me.

Dhaval R. Kathiriya
Rajkot.

LIST OF FIGURES & TABLE

Sr. No.	Figure No.	Figure Title	Page No.
1	1.1	e-Governance Platform	5
2	1.2	Categories in e-Governance	12
3	1.3	Phases in e-Governance	13
4	1.4	ICT in e-Governance	21
5	1.5	Conceptual Positioning of the Middleware	25
6	1.6	Middleware Structure	27
7	1.7	e-Governance challenges	69
8	1.8	The Strategic Response to the e-Governance	74
9	2.1	Components of Electronic Voting Machine	101
10	2.2	Balloting Unit	102
11	2.3	Model Layout of EVM Polling Station	120
12	3.1	Smart Card	137
13	3.2	Smart Card Manufacturing	138
14	3.3	Smart Card—A Key to Information Services	142
15	3.4	Microprocessor based Smart Card Types	149
16	3.5	Contact Cards	150
17	3.6	Memory Architecture in Card	151
18	3.7	Contactless Smart Card	155
19	3.8	Prox Cards	156
20	3.9	Hybrid Cards	157
21	3.10	Combi Cards	158
22	3.11	Front Side View of Smart Citizen Card	174
23	3.12	Back Side View of Smart Citizen Card	175
24	3.13	Accessibility of information	178
25	4.1	Generic Biometric Systems	201
26	4.2	Biometric System Process	209
27	4.3	The Classes of Fingerprint Patterns	218

28	4.4	Fingerprint Pattern Classification	219
29	4.5	Fingerprint Ridges, Bifurcation and Island	220
30	4.6	Fingerprint Minutiae	221
31	4.7	Fingerprint Imaging	222
32	4.8	Enrolment of minutia points	224
33	4.9	Verification using minutia points	225
34	4.10	Enrolment with pattern-based algorithm	226
35	4.11	Verification using pattern-based algorithm	227
36	4.12	Fingerprint Verification	231
37	4.13	EER Measurement	234
38	4.14	Fingerprint Scanner with Smart card	237
39	4.15	Match on Card Technology	240
40	5.1	Network connectivity requirements for the system	245
41	5.2	The TCP/IP stack	253
42	5.3	Bio-Smart Card Device: AET63 BioTrustKey	259
43	5.4	GSWAN Network	265
44	5.5	GSWAN Network Architecture	267
45	5.6	First tier architecture of GSWAN	268
46	5.7	Second tier architecture of GSWAN	269
47	5.8	Third tier architecture of GSWAN	270
48	5.9	Virtual Private Network connection	275
59	5.10	Using a VPN connection to connect a remote client to a private intranet	277
50	5.11	Using a VPN connection to connect two remote sites	278
51	5.12	Using a VPN connection to connect to a secured or hidden network	279
52	5.13	IPSec architecture	283
53	5.14	IPSec VPN Solution for the entire system	297
54	5.15	System Architecture	303
55	5.16	Dataflow Chart of System	306

56	5.17 (a, b)	Database Architecture	308
57	5.18	Login Screen	316
58	5.19	Main Screen	317
59	5.20	Citizen Module (Add Mode)	318
60	5.21	Citizen Module (Search Mode)	319
61	5.22	Citizen Module (Report)	320
62	5.23	Election Module (General Entry)	321
63	5.24	Election Module (Candidate Entry)	322
64	5.25	RTO Module (Add Record – CIN Entry)	323
65	5.26	RTO Module (License Detail Entry)	324
66	5.27	RTO Module (Search by CIN)	325
67	5.28	RTO Module (Search Mode)	325
68	5.29	IT Module (Add Record - CIN Entry)	326
69	5.30	IT Module (PAN Entry)	327
70	5.31	IT Module (Search Record by City)	327
71	5.32	IT Module (Report)	328
72	5.33	Bank Module (CIN Entry)	329
73	5.34	Bank Module (Account Entry)	330
74	5.35	Bank Module (Search Record by CIN)	331
75	5.36	Bank Module (Display Record)	331
76	5.37	Authentication Module	332
77	5.38	Authentication Module (Display)	333
78	5.39	Election Module (Online Authentication for EVM)	335
79	5.40	Election Module (Online Voting)	336
80	5.41	Layout of EVM Polling Station	337
81	5.42	Model Layout of polling station using the focused system of Online Voting	338

TABLE

Sr. No.	Table No.	Table Title	Page No.
1	4.1	Biometrics Technologies Comparison	235

CONTENTS

ACKNOWLEDGEMENT	I
LIST OF FIGURES & TABLE	II
Purpose and Objectives of Research in e-Governance for Indian Election	01
1 Basics of e-Governance	03
1.1 e-Governance – an Overview	
1.2 1.2e-Governance – Need and Benefits	
1.3 e-Governance – Categories	
1.4 e-Governance – Information and Communication technologies	
1.5 Data warehousing for e-Governance	
1.6 e-Governance – towards the Global Village	
1.7 e-Governance – Laws	
1.8 e-Governance – Challenges for development	
2 Current Election System	81
2.1 Indian Election – an Overview	
2.2 System of Election	
2.3 Election Commission – to Conduct the Elections	

2.4	Electronic Voting Machine (EVM)	
2.5	Counting of Votes	
3	Unique Identity Smart Citizen Card	129
3.1	Unique Identity Citizen Card – Need for common people	
3.2	Smart Card Technology – an Overview	
3.3	Smart Card as a unique identity Citizen Card	
3.4	Central Database for the card	
4	Integration of Biometric Technology with Smart Card	181
4.1	Biometric Technologies – an Overview	
4.2	Biometrics in Model Identification Systems	
4.3	Fingerprint based Identification System	
4.4	Identification System with Integration of Fingerprint and Smart card	
5	Implementation of designed Identification System on the Network Architecture and Prototype generation for the entire system	244
5.1	Network Connectivity overview and requirement for the system.	

- 5.2 Network Connectivity using existing network of Government of Gujarat – GSWAN for the system.
- 5.3 Internet as shared infrastructure using IPSec VPN for the system.
- 5.4 Development and implementation of the application with bio-smart card and generate the prototype that facilitates the e-Election.

Purpose and Objectives of Research in e-Governance for Indian Election

As is true all over the world, government in the developing nations costs too much, delivers too little, and is not sufficiently responsive or accountable. Good governance reforms aim to address these shortcomings. Yet progress – after many years of effort in implementing such reforms – has been much more limited than expected. e-Governance offers a new way forward, helping improve government processes, connect citizens, and build interactions with and within civil society.

The need of multipurpose Citizen Card has been felt now instead of multiple cards, multiple databases by various government departments. The current approach of e-Governance is not integrated and does not give convenience to the citizen in getting information and services. Looking to the needs for easy access of information and services by citizen, effective and better management of e-Governance by government and integrated approach for Citizen Card serving multipurpose for e-Governance has been represented as a model.

The existing election system has been studied and the challenges of this system with regard to identification and use of EVMs in rural area where operating understanding is very

low. These challenges don't give a methodology, which is convincing to the masses residing in rural areas.

To bring convincing aspects and easy use of device for casting votes, the research is purposed to provide ease of operation and convincing to the satisfaction with regards to identity.

The intended research is to give an outcome as an elegant system of identity, which much more secure and most convincing with the use of biometric and smart card technologies. The identity is reflected to match the patterns instantly which doesn't leave any lapses in identification and on completion of the voting cast the data is securely transmitted to the server and one has not to worry about data that is lying either on the paper media and electronically on EVMs.

Chapter – 1

Basics of e-Governance

1.1 e-Governance – an Overview

1.2 e-Governance – Need and Benefits

1.3 e-Governance – Categories

1.4 e-Governance – Information and
Communication technologies

1.5 Data warehousing for e-Governance

1.6 e-Governance – towards the Global Village

1.7 e-Governance – Laws

1.8 e-Governance – Challenges for development

1. Basics of e-Governance

1.1 e-Governance – an Overview

Electronic Governance can be defined as giving Citizens the choice of when and where they access government information and services. Putting the Citizen at the center of government means taking a delivery channel view. This would mean using more and more of Electronics & Information Technology in many of the government functions.

In short e-Governance is a kind of 'Window of Opportunity' facilitating a much faster, convenient, transparent and dynamic interaction between the government and its people.

The e-Governance has consequently become an accepted methodology involving the use of IT in:

- Improving transparency
- Providing information speedily to all citizens
- Improving administration efficiency
- Improving public services such as transportation, power, health, water, security and municipal services.

Governments around the world are struggling with fundamental changes in the way they work. They are seeking ways to provide better services for citizens and improve the climate for business growth at a time of growing pressure for flat or

reduced taxation. Today nations want to reduce costs and improve efficiencies; developing nations want to deliver new services without creating huge bureaucracies or costs.

All nations are trying to create the infrastructure and business climate to succeed in today's world markets. As many countries have already discovered, a solid technology infrastructure can play a significant role in helping governments deliver a comprehensive set of services to citizens, support business growth, attract outside investment, improve education, increase operating efficiencies and reduce costs.

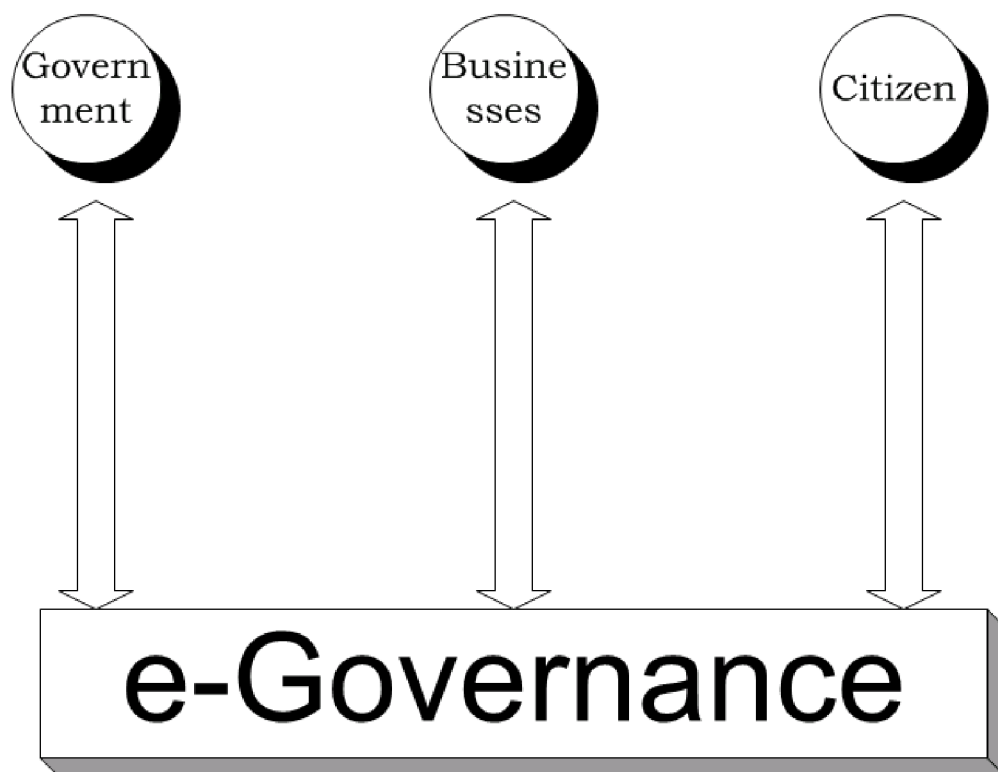


Figure: 1.1 e-Governance Platform

Above figure1.1 shows that e-Governance is not just about government web site and e-mail. It is not just about service delivery over the Internet. It is not just about digital access to government information or electronic payments. It will change how citizens relate to governments as much as it changes how citizens relate to each other. It will bring new concepts of citizenship, both in terms of needs and responsibilities. e-Governance will allow citizens to communicate with government, participate in the governments' policy-making and citizens to communicate each other. The e-Governance will truly allow citizens to participate in the government decision-making process, reflect their true needs and welfare by utilizing e-government as a tool.

Imagine a situation in which all interactions with government can be done through one counter 24 hours a day, 7 days a week, without waiting in lines. In the near future this will be possible if governments are willing to decentralize responsibilities and processes, and if they start to use electronic means such as the Internet. Each citizen can then contact the government through a website where all forms, legislation, news and other information will be available.

Today commercial banks have already adopted this approach. Most transactions can be done at an ATM, by mail or by the Internet, which has saved banks enormous costs. In other words, they do more work, with less people, in less time and with less and smaller offices.

e-Governance is not just about government web site and e-mail. It is not just about service delivery over the Internet. It is not just about digital access to government information or electronic payments. It will change how citizens relate to governments as much as it changes how citizens relate to each other. It will bring forth new concepts of citizenship, both in terms of needs and responsibilities.

e-Governance will allow citizens to communicate with government, participate in the governments' policy-making and citizens to communicate each other. The e-Governance will truly allow citizens to participate in the government decision-making process, reflect their true needs and welfare by utilizing e-government as a tool. e-Governance will allow ordinary people to constantly interface with the government in both local and central level on various matters.

1.2 e-Governance – Need and Benefits

World economies have recognized Information Technology (IT) as an effective tool in catalyzing the economic activity, in efficient governance and in developing human resource. They have, therefore, made significant investments in it and successfully integrated it with the development process, thereby reaping the benefits to their society. In India also these developments have impacted the industrial, education, service and Government sectors and their influence on various applications is increasingly being felt of late.

As the era of digital economy is evolving, the concept of governance has assumed significant importance. The questions often asked in this context are:

- How government can become more responsive and accessible?
- How can the government enhance its role as a catalyst of economic growth?
- How can one provide better Government services?
- How can the government use advanced technologies for transferring benefits, improving health care and education, re-engineering?

These questions are now adequately answered through the adoption of e-Governance.

- Benefits of e-Governance

e-Governance offers a new way forward, helping improve government processes, connect citizens, and build interactions with and within a civil society. What reform has e-Governance in store? At root it provides three basic change potentials for good governance for development:

- Automation

Replacing current human-executed processes, which involve accepting, storing, processing, outputting or transmitting information. For example, the automation of existing clerical functions.

- Informatisation

Supporting current human-executed information processes. For example, supporting current processes of decision-making, communication, and decision implementation.

- Transformation

Supporting new human-executed information processes. For example, creating new methods of public service delivery. These change potentials, in turn, can bring – singly or in combination, five main benefits to governance for development:

- Governance that is cheaper
Producing the same outputs at lower total cost.
- Governance that does more
Producing more outputs at the same total cost.
- Governance that is quicker
Producing the same outputs at the same total cost in less time.
- Governance that works better
Producing the same outputs at the same total cost in the same time, but to a higher quality standard.
- Governance that is innovative
Producing new outputs.

1.3 e-Governance – Categories

The most common three categories in e-Governance are:

- a) Government to Citizen (G2C)
- b) Government to Business (G2B)
- c) Government to Government (G2G)

a) G2C: Government to Citizen

G2C will aim at connecting citizens to government by talking to citizens and supporting accountability, by listening to citizens and supporting democracy, and by improving public services. It will involve better services to the citizens through single point delivery mechanism. The spirit behind G2C services will encompass all the services that the Government is delivering to its citizens.

b) G2B: Government to Business

This will constitute the various services a business house needs to get from the Government, which includes getting licenses etc. Standards for Electronic Transactions or E-Commerce need to be built. The standards will also include standards on content etc.

c) G2G: Government to Government

This can also be referred as e-Administration. It involves improving government processes by cutting costs, by managing performance, by making strategic connections within government, and by creating empowerment. It will involve networking all Government offices so as to produce synergy among them.

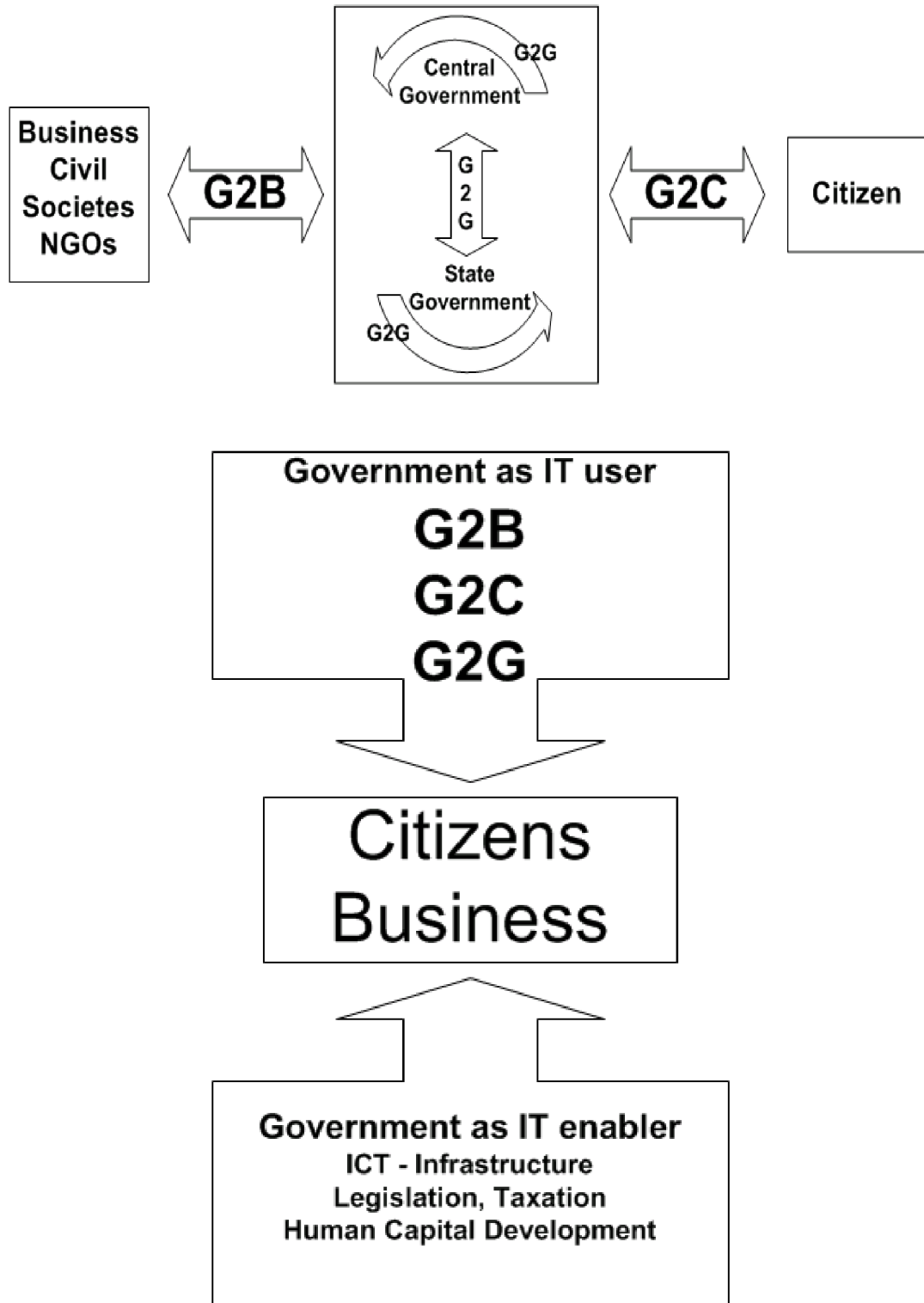


Figure: 1.2 Categories in e-Governance

1.3.1.1 Phases in e-Governance

As per e-Governance categories, there are following four phases:

- a) Information
- b) Interaction
- c) Transaction
- d) Transformation

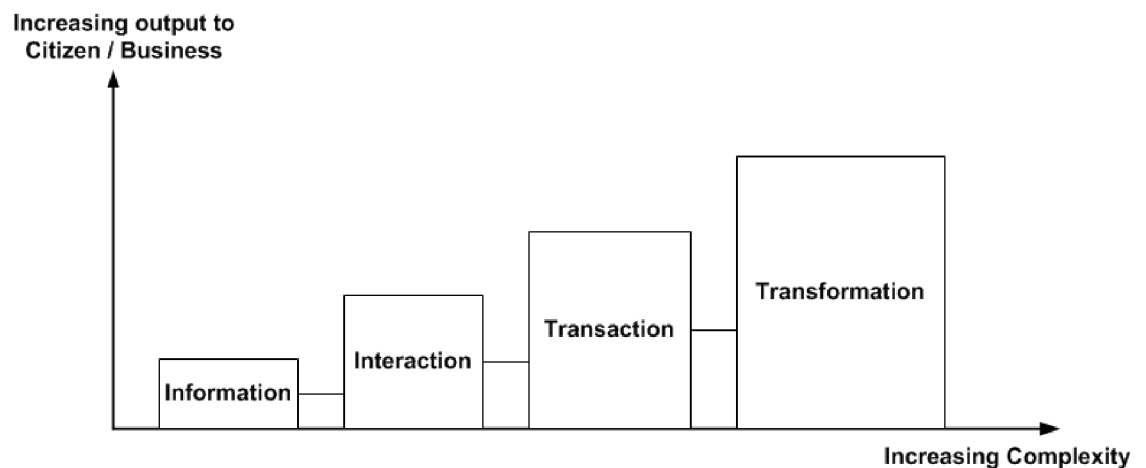


Figure: 1.3 Phases in e-Governance

a) Information

In the first phase e-Governance means being present on the web, providing the external public (G2C and G2B) with relevant information. The format of the first government websites is similar to that of a brochure or leaflet. The value to the public is that government information is publicly accessible; processes are described and thus become more transparent, which

improves democracy and service. Internally (G2G) the government can also disseminate information with static electronic means, such as the Internet. This phase it is all about information. From a website to a site with all relevant government information available to the public, in order to improve transparency in democracy.

b) Interaction

In the second phase the interaction between government and the public (G2C and G2B) is stimulated with various applications. People can ask questions via e-mail use search engines for information and are able to download all sorts of forms and documents. These functionalities save time. In fact the complete intake of (simple) applications can be done online 24/7. Normally this would have only been possible at a counter during opening hours. Internally (G2G) government organizations use Local Area Networks (LAN), intranets and e-mail to communicate and exchange data. The bottom line is that more efficiency and effectiveness is achieved because a large part of the intake process is done online. However, we still have to go to the office to finalize the transaction, by paying a fee, handing over evidence or signing papers. The use of electronic communications tools speed up the internal government processes.

c) Transaction

With phase three the complexity of the technology is increasing, but customer (G2C and G2B) value will also be higher. Complete transactions can be done without going to an

office. Examples of online services are filing income tax, filing property tax, extending/renewal of licenses, visa and passports and online voting. Phase three is mainly complex because of security and personalization issues – e.g., digital (electronic) signatures are necessary to enable legal transfer of services. On the business side the government is starting with e-procurement applications. In this phase, internal (G2G) processes have to be redesigned to provide good service. Government needs to create new laws and legislation that will enable paperless transactions with legal certification. The bottom line is that now the complete process is online, including payments, digital signatures etc. This saves time, paper and money.

d) Transformation

The fourth phase is the transformation phase in which all information systems are integrated and the public can get G2C and G2B services at one (virtual) counter. One single point of contact for all services is the ultimate goal.

The complex aspect in reaching this goal is mainly on the internal side, e.g. the necessity to drastically change culture, processes and responsibilities within the government institution (G2G). Government employees in different departments have to work together in a smooth and seamless way. In this phase cost savings, efficiency and customer satisfaction are reaching highest possible levels.

1.4 e-Governance – Information and Communication technologies

1.4.1 Information Technology's Potential

This is all the more frustrating given the undoubted potential that new technology has to offer. IT can make to the relationship between local governments and the communities they serve: in 'grass rooting' government; in building social, political and economic coalitions; in building representation upwards and outwards; and in mobilizing the bureaucracy.

1.4.1.1 The Reality of IT in Government: Barriers and Failures

However, the potential of IT frequently remains just that: a potential that is not actualized. Both barriers and problematic outcomes beset the application of IT in government.

- Data and information barriers, such as those that prevent data being shared between different governmental departments.
- Emergencies, such as the current need to divert substantial efforts and resources into the 'millennium bug' problem; something that, once solved, will have cost billions and yet generally left government systems exactly where they started in functional terms.

- Political and legal barriers, such as the lack of an adequate legal infrastructure to deal with electronic commerce, trans-border data flows, electronic records keeping, and other issues of information age government.
- Resource barriers, particularly the barriers of human resources, since the absence of adequate numbers of capable staff have long beset the public sector.
- Economic barriers, which have pushed themselves further up the agenda of late with the reality of national and regional recession and the threat of global recession.
- Socio-cultural barriers, such as the 'bureaucratic mindset' that may see IT as a tool for government automation, but not as a tool for government transformation.
- Technological barriers, such as the difficulties of internetworking.

These barriers also contribute to negative outcomes when IT is applied in government. IT applications can be regarded as failures, particularly if one extends failure to encompass not merely the total failure when no workable information system is produced, but also:

- Partial failures: when goals are unattained or there are undesirable outcomes.
- Sustainability failures: when a system works for a short while but is then abandoned, for example, when the donor

agencies, organizational champions or consultants move on to fresh pastures.

- Replication failures: when a successful pilot system cannot be reproduced on a larger scale.
- Rationality-reality gaps: failures that arise from the formal, rational way in which information systems are conceived, which mismatches the informal, subjective, self-interested realities of many public sector organizations.
- Private-public sector gaps: failures that arise from application in public sector contexts of information systems developed for the private sector.
- Country context gaps: failures that arise from application in developing countries of information systems developed in Western nations.

1.4.1.2 The Way Forward for IT, Government and Development

In seeking to realize the potential of IT to support government's contribution to the development process, the starting point must be to look beyond the technology. Four integrated starting points can be identified in harnessing IT:

- Aims and objectives

IT is a means to achieving organizational aims and objectives, not an end in itself. Therefore recognition of

those aims and objectives must be a starting point for IT application.

- Processes

The organizational processes that achieve the organization's objectives. The danger, otherwise, is that automation of ineffective processes will leave the organization with still-ineffective processes; only processes that are now more quickly, more expensively, and more voluminously ineffective than before.

- People

The human component of all organizational systems, including information systems, that is the key to performance. Any application of IT must comprehend this 'human component', building in a consideration of, for example, political/personal objectives and cultural values.

- Information:

The foundation of all information systems, yet one that seems often ignored in the idolization of technology. A learning-based approach that encourages public managers to think systemically, to identify their information needs, and to identify strategies to meet that information needs.

The forces of globalisation are fast gaining momentum with the new technological innovations facilitating the process. With the development of e-Commerce applications around the globe,

many countries have transitioned into electronic delivery of services in all levels of government legislature. This involves changes to existing systems, procedures and processes; and affects the way in which public and business communities deal with the government. The rapid adoption of e-Governance is facilitated by dynamic technological and telecommunication innovations. In many countries, Information and Communication Technologies (ICTs) are seen as a catalysing tool for digital governance. It is expected that digital governance will result in transparency, speedy information dissemination and improved service in public administration. In the era of informed citizens, digital governance is also seen as a vehicle for cost-effective and efficient way of public service delivery.

Information and communications technology ("ICT") is considered to hold a tremendous potential for facilitating increased levels of citizen participation in law and policy making and safeguarding processes. Time and again, cyber-commentators of all academic and professional stripes emphasize the empowering linkage between ICT and citizen participation. The democratizing potential of ICT with that originally associated with alphabets and printing presses, ICT has given rise to a fifth power of government (i.e., behind the legislature, executive, judiciary, and media) dominated by virtual citizens. ICT can enhance the citizen-government relationship. The citizen participation and democracy enhancing potential of ICT acquires an elevated significance when considered in the context of a country.

Online citizen participation mechanisms present an unprecedented opportunity to break away from traditional legislative-political practices to the extent that said mechanisms constitute a more practical and equitable means of subjecting law and policy making and safeguarding processes to the input of an expanded range of citizens.

Governments all over the world are trying to utilize IT for various purposes. The initial motivation usually comes from the need to improve efficiency of processes in the government. This may be concurred or followed by the second step comprising re-engineering of the processes.

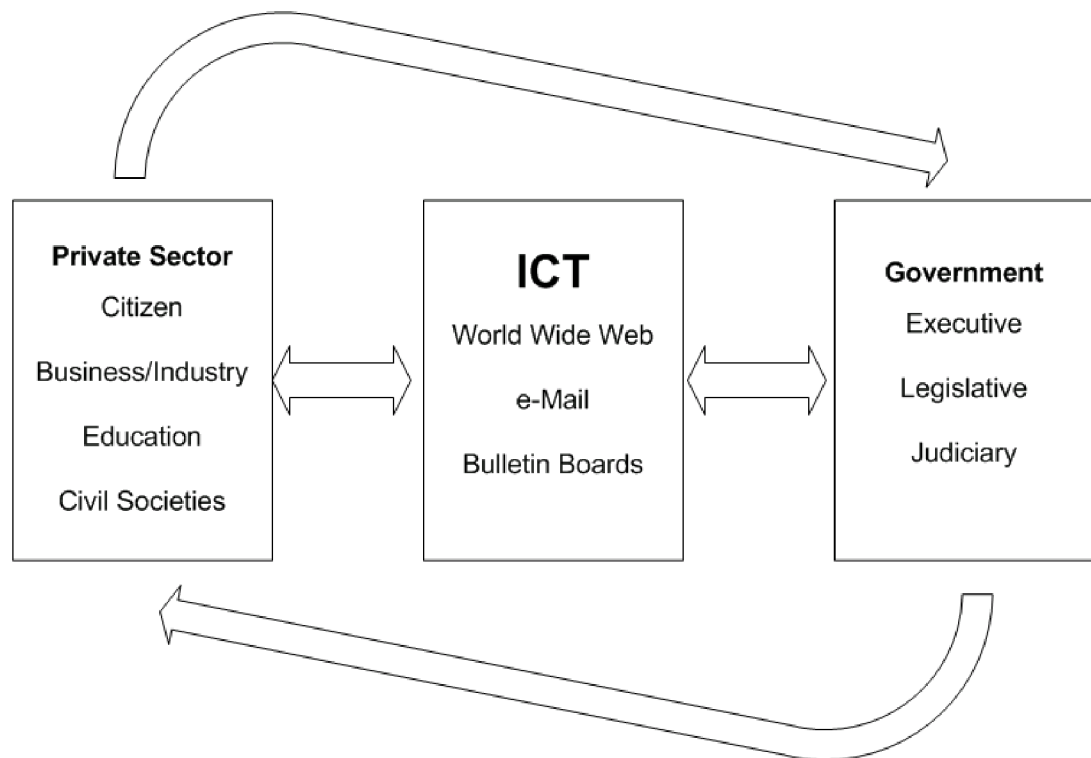


Figure: 1.4 ICT in e-Governance

Another set of motivation may come from the need to provide various social services to citizens for improving the quality of life of the citizens. A third set of motivation may be to strengthen the democratic foundations of governance (opinion polls, voting etc.). These social services and democratic enablement's correspond to the new activities that become economically viable due to the altered cost structure due to use of information technology.

Such complex requirements of electronic governance pose two big challenges to the field of computer science. The first challenge is of managing the development of the solutions on a continual basis and then managing the large number of applications that need to interact with each other while maintaining security and privacy of the data. This needs to be accomplished in such a manner that change requirement in a single application should not trigger changes in other applications. Also, these applications may need to be developed in a massively parallel way unlike conventional development processes. Hence their development should be such that they are developed to be integrable i.e. from bottom-up, the design and development should be such that once they are ready, and the applications automatically integrate with the rest of the solution and with future components. Also, the government should have the freedom to pick and choose the most appropriate application from any vendor and seamlessly plug in that application into the e-Governance middleware and

thereby, to the rest of the e-Governance solution, making the government independent of a single solution provider.

The second challenge is of scalability, arising primarily from a need to maintain large number of records that may be created in geographically distributed data repositories.

e-Governance will spew terabytes of data, with trillions of records. The amount of information being handled by government is expected to grow up exponentially once e-Governance is introduced. This is because the ease of transactions introduced by e-Governance would encourage citizens and businesses to have more transactions with the government. In order to manage this enormous amount of data such that system performance does not get degraded and such that the system is scalable, there is a need to automate the record management functions.

Although there exists solutions for document archival system based on network-centric group wares but they do not address the issue of archival based on policies of multiple applications. An example of such a policy is archiving be allowed only after auditing of the records has been completed. The solution should also be able to maintain the audit trail of all the records at a required detailed level.

1.4.2 Current Solution Trends

Various governments, involved in the task of building an e-Governance solution, are grappling with the problems of

developing such a large system. One of the key problems is how to select and entrust a solution provider to deliver a particular component of e-Governance. Given the numerous solution providers in the market with none having any experience in building a system as humongous as e-Governance, this is a tough decision.

However, a middleware that allows solutions of multiple vendors to be plugged in with ease would solve this problem to an extent. Another problem faced by governments is to contain costs by developing a portable/ replicable solution.

The rationale behind such a solution is that, just as in businesses, around 85% of the processes are same across firms, within the same industry, it is expected that 85% of the processes should be similar across different governments. Thus, it should be possible to reuse the solutions developed for one government, for another government. Reusing the e-Governance asset across different governments can substantially bring down the cost of developing e-Governance solutions.

One option for tackling the above problems that is being considered by some governments, like the Government of Maharashtra, is to introduce a programming model consisting of a network, Total Solution Providers (TSP) and a middleware that can impose standardizations and extract the commonalties between different e-government applications. The network would consist of the physical connectivity to the administrative

units, the data-centers and provide gateways for access through the Internet. Total Solution Providers or TSP's are solution providers who have domain expertise in some specific processes or departments of the government. Given their repeated exposure to the same processes, TSP's are expected to become efficient developers of applications for that particular domain and will maintain the applications, adapting them to changes in technology. The middleware provides the glue between the network and the solutions developed by the TSPs (figure 1.5). Thus the middleware imposes the standards that allow the government to choose multiple solution providers for its various departments/ processes. This feature facilitates the solution to the problem of selecting multiple vendors. It also facilitates creation of an integrable solution.

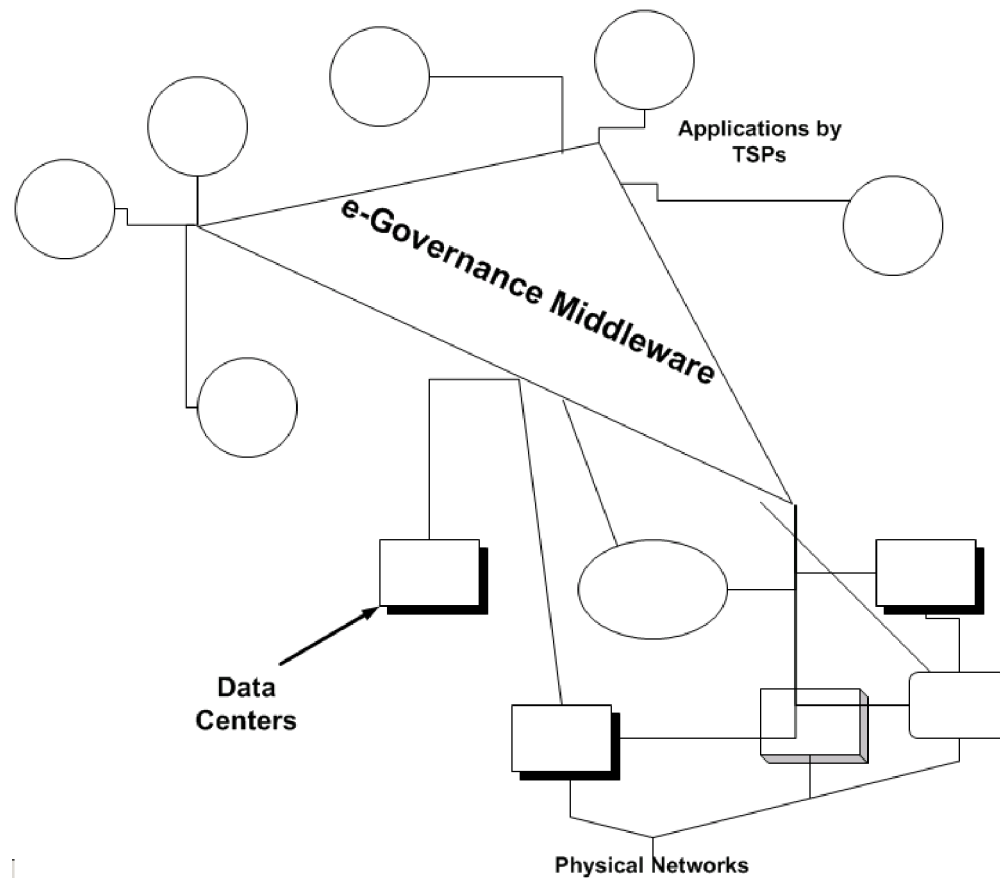


Figure: 1.5 Conceptual Positioning of the Middleware

1.4.3 Middleware Technology Requirements

Technologies for a middleware solution for a comprehensive e-Governance solution, that meets the objectives defined in the earlier sections, will have to address many diverse requirements that may be present due to various reasons.

These reasons may be economic, political, technical and cultural amongst others. The requirements are classified into two categories,

- a). Middleware technology requirements that discusses the core technology requirements and
- b). Application requirements, which discuss abstraction of common code, required for multiple applications/ departments.

1.4.3.1 Generic Middleware Requirements

The middleware should be able to support phased implementation i.e. it should be possible to have a unified approach but still implement the solution in phases. Since the government offices number in thousands and are geographically distributed, it may neither be economical nor technically feasible to roll out the entire system together.

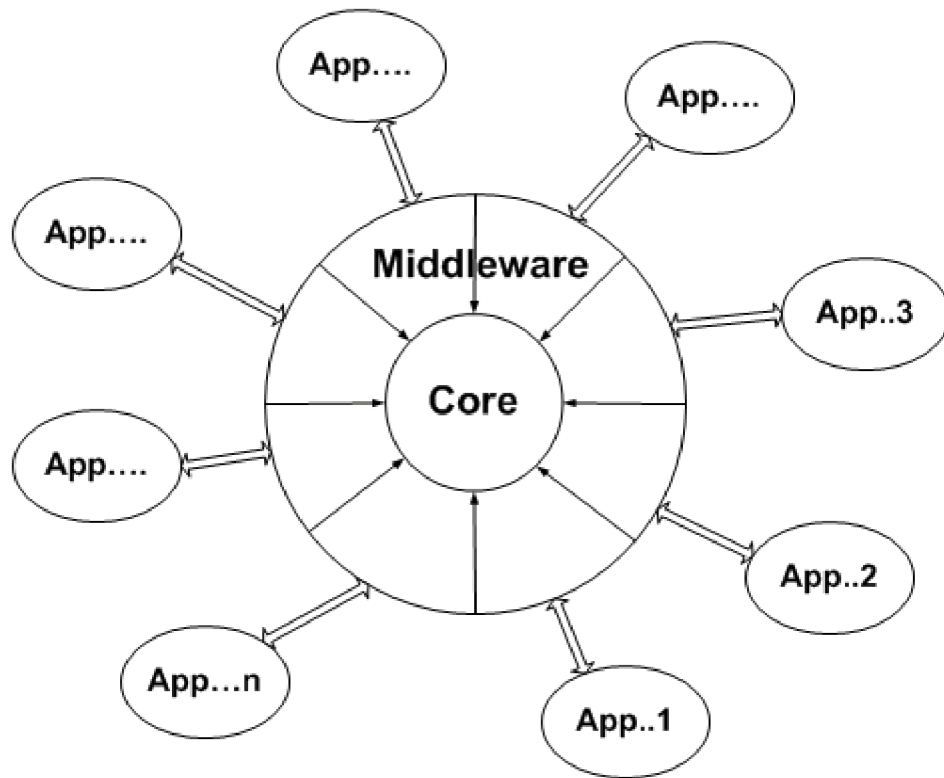


Figure: 1.6 Middleware Structure

Hence the middleware itself needs to be deployable component-wise, having a core structure with peripheral components being added as and when required (figure 1.6).

Thus all communication is routed through the middleware, which brokers the communications and ensure access control, security and privacy enforcement.

The middleware should support processes involving multi-department and multi-agency workflows. For this purpose, it is necessary that the different departmental offices (and also

external agencies) are interconnected and share the same underlying back-end databases and applications. The middleware should also be able to facilitate integration with legacy systems.

The middleware should be capable of scaling with time in terms of number and complexity of applications, number of locations and number of users / usage. It should be reliable, that is, provide assured levels of service for uptime, availability and performance. The solution should also incorporate efficient back-up capabilities and the ability to handle contingencies and recover from failures.

1.4.3.2 Application Requirements

Unlike conventional middleware, which only support the basic technology requirements of applications that are to be developed using the middleware, a middleware for e-Governance needs to also incorporate common code as part of the middleware itself. Such applications can be instant messaging, workflow etc. In addition to generic applications, the middleware should support interfaces to vertical-specific applications, which are government-to-business (G2B), government-to-citizens (G2C) and government-to-government (G2G), it should support citizen-to-citizen (C2C) applications also.

The most important application requirement is that of security and audit trail. Various security services like authentication,

multiple levels of access control, confidentiality, privacy, data integrity (prevention of forgery) and non-repudiation need to be provided. In addition, ability to generate access logs, especially for sensitive data should be present. The solution should integrate use of public key certificates and digital signatures, as applicable in India, in order to enable the transactions to have legal validity. Next is the record management requirement as highlighted in the introduction section itself. The middleware should be capable of managing very large number of records as implied by the legal and accounting norms and practices. A prototype of such a system, called the Policy Driven Data Administrator (PDDA) has been developed and is seen as step towards building the complete middleware for e-Governance.

Also, the middleware needs to provide a common human interface that needs to be simple enough to facilitate greater usage and that reduces the training costs. For citizen interfaces, this is all the more important where people may not be literate. Intuitive graphical user interface, use of speech and video technologies may be needed. Along with a simple human interface, the middleware should also be able to support local language interfaces for both employee and citizen applications.

Finally, the middleware needs to support a standard communication application and archiving, which may include messaging, instant messaging, video conferencing and mission-critical inter-application communication.

1.4.4 Standards

The key components of the technology standard that has been identified during interactions with various Indian state governments (Govt. of Maharashtra, Govt. of West Bengal, Govt. of Arunachal Pradesh, Govt. of Uttaranchal) are:

- (a) Architecture Standards
- (b) Technology Standards
- (c) Database Standards
- (d) Operating systems
- (e) Schema and nomenclature standards
- (f) Middleware standards
- (g) Security standards.

The technology standards help in building a solution within a framework. This framework is the architecture framework for the complete integrated solution across the state departments.

(a) Architecture Standards

The solutions options for architecture standards are 2- tier, 3- tier or n-tier. In late nineties three or n tier architecture came to be used along with object orientation.

The advent of platform independent languages like Java and browser based Internet technology further strengthened this approach. These architectures separated the applications into presentation, business and data tiers for better flexibility,

maintainability, performance and scalability. The presentation layer without business logic becomes thin and uses browser/Java technology to become platform independent. The business and data layers are generally hosted on separate servers. The business logic is typically hosted on system software called Application Servers providing common services e.g. security, locking etc. Because of the advantages of 3-tier architecture in a complex development environment, this architecture appears to be the preferred architecture standard. Hence any e-Governance solution needs to be based on a 3-tier architecture (where individual tiers need not be physically separate tiers) with deployment of distributed components, which can communicate across tiers.

One of the important requirements is that the architecture must be open and should allow interoperation with various standard products in the market. Hence, the solution needs to be based on open standards supporting HTML, XML, WML, HTTP, TCP/IP, SSL, SET, PKI, X.509v3, LDAP, Java, Servlets, JSP, EJB, Enterprise Java APIs (JDBC, JMS, JTS, JNDI etc.), CORBA, IIOP, IMAP4, POP3, CWMI, SOAP, UDDI etc.

(b) Technology Standards

Based on interactions with various Indian state governments, certain key parameters have evolved for determining the technology standards to be adopted. These parameters are:

- Applicability of the technology
- Scalability

- Robustness
- Availability of relevant skilled manpower
- Vendor commitment and availability of vendor support
- Cost of ownership.

Before adopting any standard, the standards need to be evaluated against the above parameters.

(c) Database Standards

Given the complexity of the solution requirement, any database chosen for the solution, needs to support full parallelism without any restrictions on Update /Insert /Delete, especially on LOBs. The database would also need to directly support Recursive SQL (and not through programming), in order to maintain the efficiency of the database. The database should also be devoid of any resource bottlenecks for efficiency reasons. The database also needs to have a robust Cost Based Optimizer for the same reason. Because of the distributed nature of the solution, the database needs to be based on the Shared Nothing Concept such that one lock manager serves one database node only.

Since it is expected that e-Governance solutions will have long running transactions, hence the database needs to have a log file architecture without the need for rollback segments so that the rollback segments do not get full forcing the work to be rolled back. Also, since one cannot stop the long running transactions, it is imperative that the database supports

efficient online backup and restore. It would also need to support optimal data buffering through unlimited number of buffer pools. The database also needs to support real data growth onto parallel servers for workload distribution.

Along with databases, there is a need to standardize the OLAP software also. The chosen OLAP needs to have multidimensional analysis capabilities, with support for a large number of dimensions. Moreover, given the varied sources of information, the OLAP should be able to access data from relational data source, spreadsheet and text files.

It should not require an RDBMS at the backend to build, run and operate the multidimensional database. Given the sensitivity of data, the OLAP needs to provide high level of security till the cell level. Given the diversity of platforms, the OLAP needs to be available on multiple platforms - Unix, NT, AS/400, S/390, and clients on Windows, Mac and Unix. Finally, for the tool to be used by a large section of people, the OLAP would need to allow multidimensional analysis to be web enabled.

(d) Operating Systems

The choice of the operating system (OS) is critical for the success of any e-Governance solution. The OS needs to be stable, secure, scalable, open and cost-effective. The essential features of OS are security (secure from hacking and viruses), vendor independence (so that no one vendor can hold the

government to ransom), application portability, skills availability, future survivability of the OS and support to the OS from the IT community.

(e) Schema standards and nomenclature standards

The need for such a standard arises because of the involvement of multiple developers. Standardizing schemas and nomenclatures brings down the cost of development and subsequent up-gradation and maintenance. Detailed study of few of e-Governance solution requirements needs to be done before this set of standards can be prescribed. Since multiple solution providers are typically involved in an e-Governance solution, hence these standards can be arrived at only after discussions with the application developers.

(f) Middleware Standards

Middleware needs to provide services such as identification, authentication, authorization, directories, and security to all applications. By promoting standardization and interoperability, middleware will make advanced network applications much easier to use. The key middleware components are

- Web Application Server
- Inter-application communication and messaging
- Mailing and Collaboration software
- Language and data interchange standards.

(g) Security Standards

Security is critical for the running of any e-Governance solution. Security is enforced through multiple components such as firewall, authentication & authorization mechanism, and audit control mechanisms. It needs to provide a secure, automated and role-based, policy-based user management. It should be able to centrally define and manage security policy for a broad range of e-Governance and other applications. It would also need to have role-based administration model for delegation of administrative privileges and group users according to business needs.

Security would also need to have a workflow to accommodate multilevel approval hierarchies and it should be configurable to the local government/departmental environment, planning system, or other workflow products to collect and process information from the various touch points throughout the government. Security also includes PKI enablement for existing Web-based application. It would need to support authentication and access control for web-browser user through Used IDs and passwords, client-side certificates, or RSA secured ID tokens.

e-Governance solutions are complex and expensive solutions that would need to be built brick by brick over a period of time, involving multiple solution providers.

In order to have a successful e-Governance solution, governments need to adopt middleware standards that are common across the entire e-Governance solution.

In addition to middleware standards, governments need to adopt certain technology standards. Such middleware and technology standards enable development of integrable, scalable and robust solutions and cut down the cost of development and maintenance of e-Governance solutions.

Cutting process costs

Improving the input/output ratio by cutting financial costs and/or time costs. Automation can replace higher human costs with lower ICT costs to support efficiency/productivity improvements. Informatisation can support decisions and implementation in downsizing or rightsizing exercises. The rationale is to address the large size of public sector expenditure and/or the inefficiency of many of its processes. The Egyptian case below is an example.

Managing process performance

Planning, monitoring and controlling the performance of process resources (human, financial and other). Informatisation supports this by providing information about process performance and performance

Making strategic connections in government

Connecting arms, agencies, levels and data stores of government to strengthen capacity to investigate, develop and

implement the strategy and policy that guides government processes. Examples of such connections are central-to-local, ministry-to-ministry, executive-to-legislature, and decision maker-to-data store. Automation and Informatisation support this by digitizing existing information channels. Transformation supports this by creating new digital channels. The rationale is to provide clearer direction for public sector and state processes and to provide for a more evidence-based approach to policy and process. The Chinese case below is an example.

Creating empowerment

Transferring power, authority and resources for processes from their existing locus to new locations. Typically that transfer is to lower, more localized levels of the public sector and may be seen as decentralization. Transformation supports this by creating new information flows to decision makers and process implementers in new locations. The rationale is to reduce the costs and increase the speed of processes and decision-making and/or to create more flexible and responsive processes.

1.5 Data warehousing for e-Governance

1.5.1 Need for Data Warehouse for e-Governance

Information is one of the valuable assets to any Government. When used properly, it can help planners and decision makers in making informed decisions leading to positive impact on targeted group of citizens. However to use information to its fullest potential, the planners and decision makers need instant access to relevant data in a properly summarized form. In spite of taking lots of initiative for computerization, the Government decision makers are currently having difficulty in obtaining meaningful information in a timely manner because they have to request and depend on IT staff for making special reports which often takes long time to generate. An Information Warehouse can deliver strategic intelligence to the decision makers and provide an insight into the overall situation. This greatly facilitates decision-makers in taking micro level decisions in a timely manner without the need to depend on their IT staff. By organizing person and land-related data into a meaningful Information Warehouse, the Government decision makers can be empowered with a flexible tool that enables them to make informed policy decisions for citizen facilitation and accessing their impact over the intended section of the population.

1.5.2 Benefits of a Data Warehouse for e-Governance

Citizen facilitation is the core objective of any Government body. For facilitating the citizens of a state or a country, it is important to have the right information about the people and the places of the concerned territory. Hence a data warehouse built for e-Governance can typically have data related to person and land. Such a data warehouse can be beneficial to both the Government decision makers and citizens as well in the following manner:

- Benefit for decision makers
 - They do not have to deal with the heterogeneous and sporadic information generated by various state-level computerization projects as they can access current data with a high granularity from the information warehouse.
 - They can take micro-level decisions in a timely manner without the need to depend on their IT staff.
 - They can obtain easily decipherable and comprehensive information without the need to use sophisticated tools.
 - They can perform extensive analysis of stored data to provide answers to the exhaustive queries to the administrative cadre. This helps them to formulate more effective strategies and policies for citizen facilitation

- Benefit for citizens
 - They are the ultimate beneficiaries of the new policies formulated by the decision makers and policy planner's extensive analysis on person and land-related data.
 - They can view frequently asked queries whose results will already be there in the database and will be immediately shown to the user saving the time required for processing.
 - They can have easy access to the Government policies of the state.
 - The web access to Information Warehouse enables them to access the public domain data from anywhere.

1.5.3 A Data Warehouse for e-Governance in India

The Center for Development of Advanced Computing (C-DAC) in collaboration with the Andhra Pradesh Technology Services (APTS) has developed a data warehouse for aiding the state level decision makers of Andhra Pradesh (AP) Government in their decision making process. The main objective of this effort is to organize the Multipurpose Household Survey (MPHS) data and the land records data of the AP Government into a meaningful information warehouse for enabling the decision makers in making informed decisions and accessing their impact over the intended section of the population.

The system installed in Andhra Pradesh Secretariat at Hyderabad is based on an 8-node PARAM 10000 configuration of C-DAC and provides a decision support capability to the state officials using industry standard tools and allowing

analyses to be made on historical data with scalability and dynamism on data from Taluka to District to State levels. It also provides web-based access besides access on LAN set up within the Secretariat, through both thick and thin clients and kiosk with bilingual information.

The data warehouse has enough potential to access the impact of various welfare schemes across the population of the state. The planners can design schemes focused on specific target groups and achieve high impact. The decision-makers can carry out analysis of population profile across the state in areas of economy, education, family units, shelter, etc. The warehouse can also be used for rural and urban development planning, agricultural yield and cropping patterns analysis and much more. These analyses will help in making decisions that are focused and the benefit of the government policies can reach the intended group.

The various types and number of queries that can be handled by the data warehouse are limited only by the intelligence of the person using the data warehouse and the data fed to it. Some of the simple queries that can be handled by the system are:

- What is the percentage of people in different occupation - qualification-wise, religion-wise, and age-group-wise?
- How much is the unemployment in men or women versus age, area, and religion?
- What is the growth rate of population region-wise versus resources food, shelter and education?

- What is the percentage of land holding of people having income below certain level?
- What is the crop-wise area and cultivation trend?

1.6 e-Governance - towards the Global Village

In India, the Information Technology Act has come into effect, ushering in the era of digital signatures. At least on paper, the citizens can conduct business with the government without leaving the comfort of their homes.

The Internet can help citizens in:

- (i) Paying bills (telephone, water, electricity, etc.), taxes and so on,
- (ii) Registration formalities for land, marriage and birth & death,
- (iii) Information and download application forms, and
- (iv) Lodging complaints.

The Internet has cut the frontiers of time and space. Anyone anytime can access information and give feedback. But this calls for not only Net-enabled governments but also Net-enabled citizens.

1.6.1 The Problem of Access

The present level of facilities in the country of one billion populations is highly deficient to enable the reach of IT services to the common man. Telephone networks continue to be the most prominent communication media for access to the Internet. As the telephone density in the country is extremely low, access to the Internet is concentrated in only limited parts of the country.

The availability of computers is also a major problem. There is no coordinated effort to bring the Internet to low-income groups. No doubt, digital divide based on economic criteria is real. This slows down adoption of IT tools and services. Even if with the good intentions the government provides every village with a free computer, there is no surety that the computers would find a place in community centers, instead of in the panchayat presidents' houses just as the free community television sets did. There is also a proposal to offer subsidized Internet connections at public telephone booths throughout the country. The emerging convergence of technology - computer, radio, digital television and phone/fax in one box - may bring down the cost of technology and help the spread of computerization.

The common man in the country continues to be largely unaware of the potential of IT in daily life. This calls for a mass campaign for creating awareness of IT benefits. At times with over-enthusiasm, IT is projected as a panacea for every problem. No doubt it can enhance the capability in every field, but it is not a substitute to economic and technical inputs in the respective fields. Particularly in a development initiative, 'the virtual world' can at best strive for the betterment of the real world by spreading information and creating awareness; but to convert awareness into action, an active intervention in the real world is needed.

Several states have gone in for Net-enabled administration and they are in the process of making the citizens too Net-enabled.

But little work has been done to find if e-Governance has had an impact at the grassroots. Whatever be the case, even a small provision for downloading application forms has helped eliminate the tyranny of middlemen.

1.6.2 Mindset Poses Hurdles

The Internet is set to transform business and governance. Those in business have realized that if they want to survive in a global competitive environment they should actively use the Internet - be it setting up a Web site or transacting with customers over the Net. But the question frequently asked is why e-commerce is a success whereas e-Governance is not so much a success. Is it not true that business is more enterprising than the government?

e-Governance could help reduce government controls to a bare minimum, and develop a system that can administer in an efficient manner. This calls for a change in the mindset of the bureaucracy that still carries with it the 'babu' legacy. If the change in the mindset does not take place, e-Governance will not go a step further than computerization of traditional manual activities.

In most states, e-Governance relies on private participation. In Andhra Pradesh, even the technical support comes from private firms. Hence some government employees feel that e-Governance would deprive them of power and status. They allege that this is nothing but handing over some of the functions of the government to the private sector. They also

fear that this may reduce government jobs. So they are reluctant to take to e-Governance. Not always the digital divide is in terms of haves & have-nots and urban & rural. It is, more often than not, in the mindset. The mindset prevents a vast majority of bureaucrats from taking to information technology, leave alone they propagating IT among the masses. The mindset can be changed to a large extent by providing enough number of computers at government offices and offering training to the staff.

1.6.3 Catering to Target Group

All major global portals are set to come to India by mid-2001. Microsoft Network and Yahoo portals already deal with India-specific stuff. Foreign portals incorporate UCD (User-Centered Design) that gives attention to the target audience's perspective. For instance, they have redesigned their sites to reduce graphic content for fast access from India's limited bandwidth. At the same time, several Indian portals concentrate on visuals that take long time to download, which could irritate the user. Many of them start with a big photograph of their institution's building or their crest that takes more than 10 seconds to download. The user is trigger-happy on the Net with a finger constantly on the mouse and he/she readily jump if the page does not respond quickly.

e-Governance is capable not only speeding up transactions but also allowing transparent functioning. When it is said that e-

commerce has shifted thrust from a company-driven market to a customer-driven one, so should it happen in e-Governance.

Web sites can host a large collection of data that would never appear in the print due to cost factor. On the Internet, the 'information hole' is nearly infinite, and the publisher need not have to worry about the 'shrinking information hole'. The only requirement is that the matter needs to be properly split and links given to subheads so as to be user-friendly. The Internet gives the user the option of accessing the material of his/her choice. Web sites, with their voluminous stuff catering to diverse interests, have helped empowering people and also curtailing opinion-making tyranny.

The content of a Web site can be updated round the clock. But often, bureaucratic hurdles bog down many a government Web site and the sites offer stale stuff. The sites have to be continually updated, as the user does not stand stale information. Any site that is not current is bound to lack credibility and lose its clients. Many a times, even e-mails seeking more information or clarification are either unanswered or answered months after sending. If the mindset of bureaucrats remains the same and it prevents many of the government information from being made public, going online would only be ornamental.

1.6.4 Governance Made Efficient

Some states have computerized vehicle registration, land records, birth & death registration, employment exchanges and

the like. This has resulted in effective governance in a limited sense. But e-Governance has not gone in for interactive aspect of the Net to create a government-citizen interface. Presented below are two cases of how e-Governance could take the next step from mere computerization of government records.

Case 1:

The Gujarat Road Transport Department's 'computerized check-post project' has eliminated corruption at 10 octroi posts on the state's borders, and increased the revenue from Rs. 60 crore in 1998-99 to Rs. 250 crore in 1999-2000. The moment a truck enters the state its weight is recorded and the vehicle is videographed, and the data is instantly accessible in Ahmedabad. This allows little room for local officials to take bribe. Compared to the additional revenue earned, the heavy capital investment of Rs. 18 crore is nothing.

Case 2:

The Water Resources Organization of the Public Works Department of the TamilNadu Government is in the preliminary stage of implementing Management Information System (MIS) for its irrigation basins. If implemented in toto, it would allow farmers in remote villages to key in water requirements and crop status on computers that would enable the officials sitting in towns to decide the quantum of supply based on the situations at various spots at times of water scarcity. MIS can check

political pressures and bribe-taking by officials, and thus eliminate the inequity in water distribution. But more often than not in such projects, computer use gets confined to government officials and e-Governance fails to serve the purpose.

1.6.4 Openness in governance

e-Governance has two aspects:

- (i) An easy interface among government departments, and
- (ii) Openness in governance. Of course, several states in India have attempted the former, but little has been done to use IT for ushering in openness in governance. This democratic aspect is conveniently given a goby.

The present e-Governance dishes out information just one-way about government policies with a lot of statistics. The recipient of information is not allowed to have a participatory role. Even the material provided is of outdated stuff clouded with bureaucratic jargons.

The right to information ushered in through e-Governance also calls for prior decentralization in power structure and decision-making. The Internet is an open medium with four major features: e-mail, Web site, search engines and MUD (multi-user domain). All these features should be optimally used for a participatory decision-making. The governance will be put through a high level of scrutiny by the transparency resulting out of the interactions.

1.6.5 Democratizing Politics and Press

Politics and the press are the two social institutions that have major impact on governance. Democracy holds leaders accountable to the people, and it allows the free flow of information and ideas. The Internet is set to usher in e-democracy that would influence political parties and news media (press). The Internet will change some social institutions and create new ones.

As already pointed out, many government departments do not give prompt replies to e-mails received. But a few elected representatives have realized the need to be interactive over the Net, at least during the election campaign. They could also inform their constituents in a cost effective manner about what they are doing in Parliament or the Assembly, and also get to know about the happenings in the constituency. Thus the Internet offers an easy option for an elected representative to carry on communication with the electorate, in the language of their choice, even when he/she is out of the constituency.

The Internet will affect politics by helping people to make more informed choices, based on a wide variety of information. Before the advent of the Internet, the voter only had limited information on which to base his/her choice, and was often hoodwinked by dishonest politicians. No more, politicians would find it easy to mislead the public.

The Internet is also poised to reorient news media. It has the potential to break the stranglehold of media barons and

journalists on public opinion. News media would feel the urge to be more people-oriented, with the more and more people of diverse backgrounds being outspoken over the Net. Today anyone with a computer and an Internet link can be a publisher, and can air his/her view. So news media will be more sensitive to the issues concerning various sections of society.

The Internet has become a powerful tool in the hands of advocacy groups, NGOs and the public. This is particularly so at times of distress. During Kargil war, the Internet not only provided people with information but also gave them an opportunity to air their views. In fact, the Internet has helped patriotism to transcend borders! The same is in the case of violence against Christians in far-off places which would otherwise have gone unnoticed: the exchange of chain emails set the agenda for the press, which in turn forced the Government to take notice of the events. The Internet is the best tool yet devised for communication between distant persons.

The Internet is emerged as a powerful alternative form of communication that could even set the agenda of politics, governance and mass media.

As the use of the Internet deepens and widens, social exclusion of the underprivileged would decrease. The Internet is the first mass medium wherein even a common man can carry on mass communication. No doubt, the Internet has the capability to go

back to a village panchayat-type, participant-based democracy where each individual would have a say in the decision-making. e-Governance is bound to accelerate this process up to village level.

1.7 e-Governance - Laws

The World Bank defines e-Governance as the use of information and communication technologies by government agencies to transform relations with citizens, business and other arms of the government. It is the information technology that has added a new dimension of governance.

When we look into the system of governance, we find it static, hierarchical, regulated and fixed, whereas Web is dynamic, flat and unregulated. Basically government's functions just like a mammoth corporation, where the right hand does not know what the left hand is doing. Governments by nature of its own system of governance could not be called ambidextrous.

There exists an inherent dichotomy between the two. One on hand the government system is regulated, hierarchical and static, whereas on the other technology is creative, non-hierarchical and dynamic. The question is how to collate the governance with technology. It seems that e-Governance has been able to redefine the old structure of governance by meshing it with the new structure of the web.

Law is one of the most important arms that facilitate governance. And as the system of governance is changing, it is time that the system of law should also keep pace with the changing times. The new dispensation of e-Governance requires new set of laws. Physical laws have limitations in the

sense that they are uni-dimensional in application. They are meant to govern the physical world, which is static, defined and incremental, whereas e-Governance represents new form of governance, which is dynamic, and exponential. It needs dynamic laws, keeping pace with the technological advancement.

Information Technology (IT) Law governs the processing and dissemination of information electronically. These are 'paper laws' for 'paperless environment'. These are technology intensive laws to control and safeguard electronic transactions in the electronic medium.

IT Act has given legal recognition to electronic records (like: data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche), subject to the requirements that the information remains accessible so as to be usable for a subsequent reference.

1.7.1 Use in Government and it's Agencies

Use of electronic records and digital signatures in government and its agencies for filing, issue, grant, receipt or payment of money is now an acceptable mode.

Electronic records or information, whenever retained, as required by law must be retained in the format in which it was originally generated, sent or received.

1.7.2 Electronic Gazette

Rule, regulation, order, byelaw, notification or any other matter could now also be published in the Electronic Gazette apart from the Official Gazette. The date of publication shall be deemed to be that date on which the Gazette was first published in any form.

1.7.3 Limited e-Governance Rights

Electronic governance as envisaged in the IT Act does not confer a right upon any person to insist that any Ministry or Department of the Central or State government (or any authority or body) to accept, issue, create, retain or preserve any document in the form of electronic records or to participate in any monetary transaction in the electronic form [S.9].

The IT Act provides limited e-Governance rights. The idea is to adopt technology uniformly across the length and breadth of the government rather than have selective adaptation. That is, e-Governance not at the cost of the digital divide.

1.7.4 Watch Out for One Act Syndrome

Moreover, it is time to amend the old Acts to bring them at par with the new technological developments. There could not be one Act to deal with all the questions of e-Governance. The

digitized developing countries have to go beyond one- Act syndrome for greater effectiveness.

A law reflects experience. The number of legislative enactments on a subject shows the degree of its importance and acceptability in the society. Law making is a long drawn and continuous process. It evolves over a period of time.

For example, as many as 16 different Acts (not including various Regulations) have been enacted by the UK's Parliament in a span of twelve years dealing with computers, computer systems or computer networks.

Although the IT Act defines data, computer data, information etc. but it is silent about ways and means to protect data and information. Without a proper privacy and data protection laws the effectiveness of e-Governance may remain a point of concern.

1.7.5 e-Governance and Privacy Issues

It is difficult to view 'privacy' in isolation-it has to be seen in the context of dynamic technologies of today. Privacy issues, which are relevant today, could not be judged from yesterday's perspective.

To a government, violation of privacy of individual is a serious issue. Governments have been trying to establish the primacy of privacy by addressing issues both at macro and micro levels.

At macro level, the individual privacy is not an issue. It is expendable in the national interest. Whereas, at micro level safeguarding individual's privacy is a systematic and continuous process.

Privacy is a very personal issue. It's about us and our personal space. We are the final authority to decide accuracy, access, security and control of our personal information as well as its use and whether it could be passed on to third parties.

1.7.6 e-Governance and Data Protection

One of the most important tasks in any e-Governance model is to protect and provide the security to the individual's data. When we talk about the security aspects, we are looking into both policing and preventive measures.

Virtual world is a place with its own dark corners and alleys. What we share, in good faith, can be exploited against us. The more we open up to share, the more vulnerable we make ourselves. We need a regulatory mechanism to protect and provide the security to the individual's data. Success of an e-Governance model would depend upon the perception of an individual about its effectiveness in securing his personal information. And without statutory enactments there are no guarantees as such.

UK's Data Protection Act, 1998, is one such enactment. It is built around eight data protection principles that apply to all

personal data processed by Data Controllers (it includes companies, businesses, organizations - employers, local and central governments). Data Controllers determine the purposes for which and the manner in which any personal data is (or is to be) processed.

- Personal Data
 - Personal data relates to a living individual who can be identified:
 - From the data
 - From the data & other information in the possession of, or likely to come into the possession of, data controller
 - Any expression of opinion about the individual
- Sensitive Personal Data
 - Racial or ethnic origin
 - Political opinions
 - Religious beliefs or other beliefs of similar nature
 - Membership of a trade union
 - Physical or mental health condition
 - Sex life
 - Criminal offences
 - Criminal proceedings and convictions
- Eight Principles of Personal Data

Personal data shall:

 - Be obtained & processed fairly and lawfully
 - Be held only for lawful purposes, which are described in the register entry

- Be used or disclosed only for lawful or compatible purposes
- Be adequate, relevant and not excessive in relation to the purpose for which they are held
- Be accurate and, where necessary, kept up to date
- Be held no longer than is necessary for the purpose for which they are held
- Be accessible to individuals it concerns, who may, where appropriate, correct or erase it
- Be surrounded by proper security

For effective e-Governance, proper attention and care has to be given to the privacy and security of personal information.

1.7.7 e-Governance: Extending Rule of Law in Cyberspace

e-Governance is also about extending rule of law in the cyberspace. Crimes of 'physical space' have found a virtual extension in cyberspace. The weapons of crime are sophisticated technological tools, which are not easy to detect. Every day, technology is adding new weapons in the virtual arsenal. It's going to get worse before it gets better.

Technology is a great leveler. It has created a very piquant situation where the criminals and the law enforcement agencies are at par with one another with respect to technical know-how. In fact, both of them are on the learning curve, upgrading their skill sets by each passing day. The question is who will win this game? Stakes are very high.... winner takes all. It is

imperative that the Governments should recognize that the future is imperfect and while developing e-Governance models they should also look into security and safety measures.

1.7.8 Future is Imperfect

- Wireless applications (Personal Digital Assistants, PDAs, mobile phones) will be the new territory for cyber criminals to move-in. In fact, virus writers have already created the Palm OS/Phage virus, which recently hit the Palm OS PDA operating system.
- Cyber- terrorists and Hackers will become more organized and visible. Cyber terrorists and hackers are too on a learning curve. They are mastering the technology and upgrading their critical infrastructure to conduct successful attacks.
- Virus mutations and transmission / delivery mechanisms will increase.
- Virus attacks will be more vicious and cut across all kinds of technological platforms (both wired and wireless).
- Disgruntled employees will cause havoc. More and more senior level executives will get involved in disrupting the cyber-functioning of their organization. Also, employees with access to critical data (source code / program code) will become security risks.

- Hackers will join the mainstream companies and government organizations. They will wait for an opportunity and the right price to strike.
- Like it or not, the future presents some interesting problems in the area of recruiting people with computer skills.

The e-Governance models must take into account such threat perceptions. More so, when technology has made possible the phenomenon of global jurisdiction. Both digitized developed and developing countries have been enacting laws that go beyond their geographical boundaries.

Cyberspace is a huge melting pot of different cultures. It has the capacity to give space to every thought, every idea and every expression. Cyberspace represents a new culture and an open resource growing exponentially, every minute! What we are witnessing is the emergence of a new system of 'community governance'.

1.8 e-Governance - Challenges for Development

Most developing countries have only undertaken a limited number of e-Governance initiatives. This mainly relates to a lack of e-readiness. Most e-Governance initiatives that are begun currently fail. Surveys of e-Governance initiatives are incredibly rare; a shortcoming that needs to be addressed. Even donors, who should be committed to monitoring and evaluation, rarely seem to produce reports. From the material that is available, two main types of e-Governance failure can be identified. In some cases, there is the total failure of an initiative never implemented or in which a new system is implemented but immediately abandoned. For example, India's Indira Gandhi Conservation Monitoring Center was intended to be a national information provider based on a set of core environmental information systems. Despite more than a year of planning, analysis and design work, these ICT-based systems never became operational, and the whole initiative collapsed shortly afterwards.

Alternatively, there is the partial failure of an initiative in which major goals are unattained or in which there are significant undesirable outcomes. For example, the Tax Computerization Project in Thailand's Revenue Department set out seven areas of taxation that was to be computerized. At the end of the project, only two areas had been partly computerized, and five others were not operational. One type of partial failure that particularly seems to affect e-Governance initiatives is the

sustainability failure of an initiative that succeeds initially but then fails after a year or so. An example is the creation of a set of touch-screen kiosks for remote rural communities in South Africa's North-West Province. These were initially well received. However, the kiosks' lack of updated or local content and lack of interactivity led to disuse, and the kiosks were removed less than one year later. Sustainability question marks also hang over some of the case studies cited above.

As noted, we have only glimpses of evidence about the prevalence of such failure. A few surveys have been conducted, with examples summarized below:

- Use of ICTs for health reform in South Africa's public sector: widespread partial failure of high cost systems with little use of data.
- Use of ICTs in the Thai public sector: 'failure cases seem to be the norm in Thailand at all governmental levels'.
- Donor-funded public sector ICT projects in China: all were found to be partial failures.
- World Bank-funded public sector ICT projects in Africa: almost all were partial – often sustainability – failures.

Likewise, independent reports on ICT use in the public sectors of individual developing countries find failure to be the dominant theme. It is important to acknowledge that developing countries are not alone in suffering high levels of failure with e-Governance initiatives. However, they do face a particular set of constraints that arise from two related challenges: lack of e-readiness and large design—reality gaps.

1.8.1 The Strategic Challenge: e-Readiness for e-Governance

Lack of e-readiness contributes to both lack of and failure of e-Governance initiatives. Six key issues could be rise to the developing country governments in order to assess how strategically prepared they are for e-Governance.

- Data Systems Infrastructure

Are the management systems, records and work processes in place to provide the quantity and quality of data to support the move to e-Governance? In many countries, data quality and data security – for example – are very poor, and there are few mechanisms to address these issues.

- Legal Infrastructure

Are the laws and regulations required to permit and to support the move to e-Governance in place? In many countries, for example, digital signatures cannot be accepted.

- Institutional Infrastructure

e-Governance can only be progressed if the institutions exist to act as a focus for awareness and to act as a means for facilitation of e-Governance. In many countries, there are no institutions to co-ordinate and lead and drive e-Governance.

- Human Infrastructure

Are the attitudes, knowledge and skills in place – especially within the public sector – that are required to initiate, implement and sustain e-Governance initiatives? In many countries, key skills gaps relate to business analysis and system design, and to project management, contract management and vendor management. There are also 'mindset' gaps: general resistance to change; lack of customer-orientation; resistance to at sharing etc.

- Technological Infrastructure Ready

Although there have been great strides forward, the fact remains that most developing countries are a long way short of the computing and telecommunications infrastructure on which many Northern e-Governance initiatives have been based.

- Leadership and Strategic Thinking

A critical pre-condition in successful e-Governance for development is an e-champion or small group of e-champions: leaders with vision who put e-Governance onto the agenda and make it happen. Cases like those described above show that such leadership can smash through many operational barriers. Conversely, all the operational e-readiness in the world is of limited value if there is no vision and leadership to give direction to e-Governance. All the e-readiness issues, then, this

is probably the most critical, and it will be addressed in some detail under the following five headings:

a). No captains on the bridge

Because of lack of awareness, knowledge, skills and confidence there is a generic lack of e-Governance leadership and commitment amongst senior public officials. Related to this, there is a dearth of any vision or strategy on e-Governance from within many developing countries.

b). One man's meat is another man's poison

Because of the lack of leadership confidence and capacity within government, e-Governance initiatives are frequently driven from outside government by vendors or by donors or by consultants. The locus and focus of strategy is therefore not always right. As a result, inappropriate systems are being forced in; systems from other sectors or countries that do not fit specific DC realities.

c). Missing the g-spot:

The spots where donors set the e-Governance for development agenda, their strategic focus will be critical. But, as noted above, many recent e-development initiatives from bilateral and multilateral donors appear to be deliberately avoiding government. This is partly because of the human capacity and regulatory constraints within government, and partly because of continuing 'government bad, markets/NGOs good' undercurrents within development. Many such initiatives are therefore bypassing the state and going for community

telecentres, ICTs in schools, telemedicine, e-commerce and the like: e-business and non-governmental e-society. e-Administration, e-citizen and e-services initiatives, and the government-related components of e-society – altogether representing the 'Networked Government' model for e-Governance – have been too greatly ignored, leaving a growing opportunity gap.

d). With or without donors

Because of attitude and knowledge gaps, e-Governance for development is not being approached properly.

In some cases, ICTs are ignored – as if they didn't exist; at least some good governance initiatives act as if the last 50 years of ICT development never happened.

In other cases, ICTs are isolated – separated from the main thrust of the governance project, and so making no effective contribution to it. Ignorance or isolation seems to characterize many identifiable initiatives. For an example of the latter, one only has to look to the programmed structures of major development institutions. Frequently, there will be a structure for governance and a separate structure for ICTs, but no effective communication or synergy between the two. - In still other cases, ICTs are idolized – put as the centerpiece of governance initiatives, becoming an end rather than a means. This is increasing as public officials find out about ICTs and/or fall for the vendors' hype. It has something to recommend it –

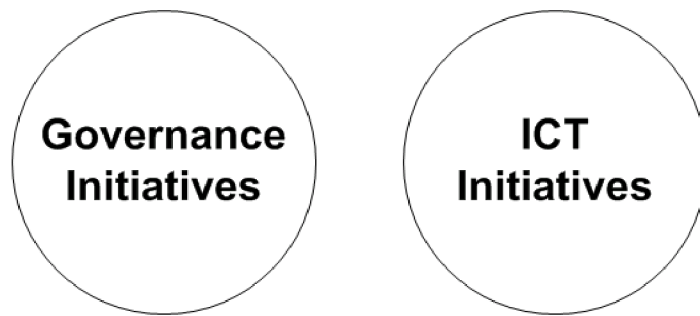
ICTs can be a useful lever to change – but governance goals are often mislaid.

Only rarely are ICTs properly integrated into good governance reforms, with reform objectives in the driving seat, with information requirements well understood, and with ICTs serving those requirements and objectives.

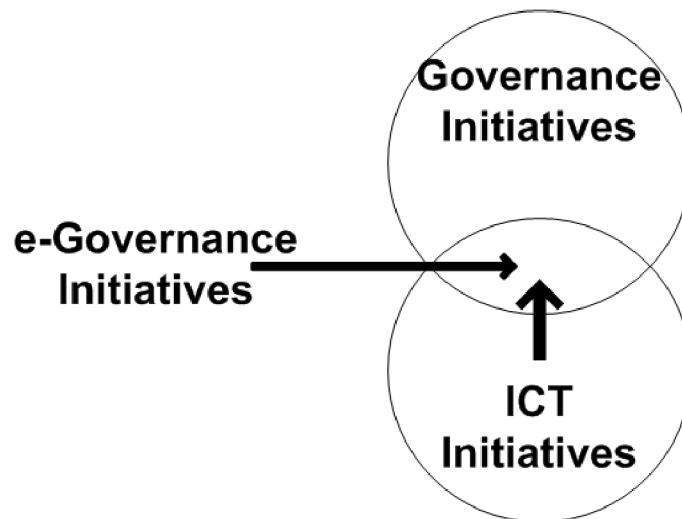
e). I'm not listening

Because of attitude and knowledge gaps but also because of cultural and political realities in some developing countries, the strategic approach to key stakeholders (users, clerical operators, citizen beneficiaries, community members) is sometimes ineffective. These stakeholders are sometimes completely ignored in the planning of e-Governance projects. Quite aside from any ethical questions, this leads to the direct practical consequence of e-Governance failure.

Situation : Ignored / Isolated



Situation : Idolized



Required Situation : Integrated

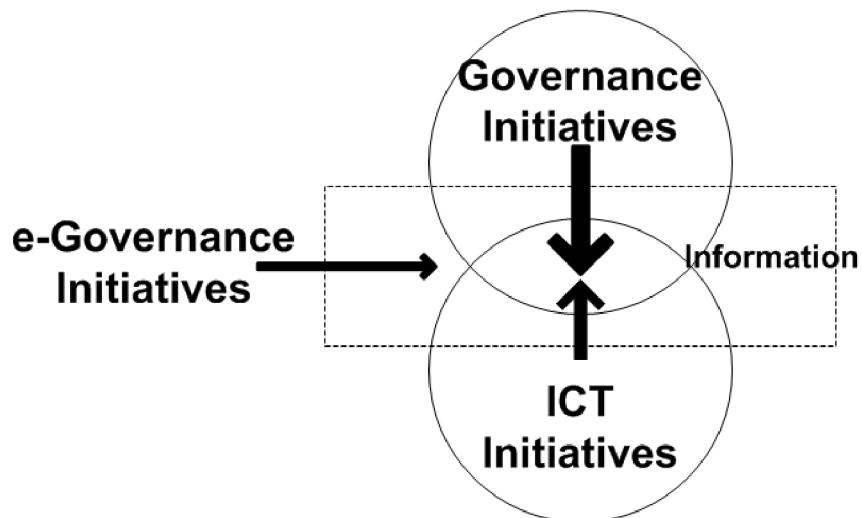


Figure: 1.7 e-Governance challenges

1.8.2 The Tactical Challenge: e-Governance Design—Reality Gaps

The strategic challenge of e-readiness addresses e-Governance at the macro-level of the whole nation as a precursor to e-Governance. In addition, though, there is a tactical challenge that faces the micro-level of individual e-Governance projects during their implementation. This is the challenge of avoiding failure and achieving success. From a study analyzing dozens of e-Governance projects, a new model has been developed to explain and predict e-Governance success and failure. The model centers on design—reality gaps: the difference between design ideas and organizational realities. The study showed that, the larger this design—reality gap, the greater the risk of e-Governance failure. Conversely, the smaller the gap, the greater the chance of success.

- The information dimension: the intranet was designed to provide just the kind of information that Council users wanted, creating little gap between designed and actual information needs.
- The technology dimension: the project plan relied mainly on existing technology within the Council, creating little gap between designed and actual technology.
- The objectives and values dimension: the project met the real (sometimes personal) political aspirations of senior councilors and officials, and gained their support,

creating little gap between designed and actual objectives.

- The staffing and skills dimension: intranet developers had the necessary skills to produce the system that had been designed, creating little gap between designed and actual skill requirements.
- The other resources dimension: the project was set up cheaply and incrementally, without particular time pressures, creating little gap between designed and actual resource requirements. All of this meant only limited gaps between e-Governance project design and Council reality. The result was success. However, as noted, failure has been more common than success, and archetypes of e-Governance failure did emerge from the study: situations when a large design—reality gap – and, hence, failure – was more likely to emerge:
- Hard—soft gaps: ICTs are often conceived in terms of machinery and engineering, rationality and objectivity. Many e-Governance systems get designed according to these conceptions. The trouble is that many government and civil society organizations do not adhere to these 'hard' ideas. In reality, they are dominated by 'soft' factors: people, politics, emotions and culture. When a hard IT design meets a soft reality, there is a large gap, and a strong likelihood of failure.

- Private—public gaps: despite the best efforts of 'new public management', the public sector remains fundamentally different from the private sector. This seems to be forgotten by too many ICT vendors, donors and consultants – a particular problem when, as mentioned above, they are often in the e-Governance driving seat. They may pick up an information system designed for the private sector. Then they try to shoehorn it into a very different public sector reality. The large design—reality gap generates lots of heat and noise, not much light and, ultimately, plenty of e-Governance failure.
- Country context gaps: it sometimes seems that only the first half of 'Think Global, Act Local' gets remembered. Designers seeking quick fixes try to pull e-Governance solutions off-the-shelf from other countries. But New York is not New Delhi, and Kuala Lumpur is not Kingston. So there is often a large design—reality gap when trying to introduce in country X an e-Governance system designed for country Y. The frequent result is failure.

1.8.3 Strategy and Tactics for e-Governance

e-Governance lies at the heart of two global shifts: the information revolution and the governance revolution. Both shifts are changing the way society works and the way that society is governed. They bring the opportunity for not just incremental but radical gains in efficiency and effectiveness.

But, at present, any such benefits are accruing to the few, not the many. It is the few who have access to ICTs, to digital information and knowledge, and to the benefits of reform in governance. We can thus talk of an 'e-Governance Divide' that is increasingly separating developed and developing countries, and elites and ordinary citizens within developing countries.

This growing divide must be addressed if the poor in developing countries are not to fall even further behind. We must seize the digital opportunity for governance and seize it now. Delay for the South as the North pushes ahead will only reinforce historical patterns of inequality. In short, there must be both a strategic and a tactical response that attacks the current challenges to e-Governance for development hard and head-on.

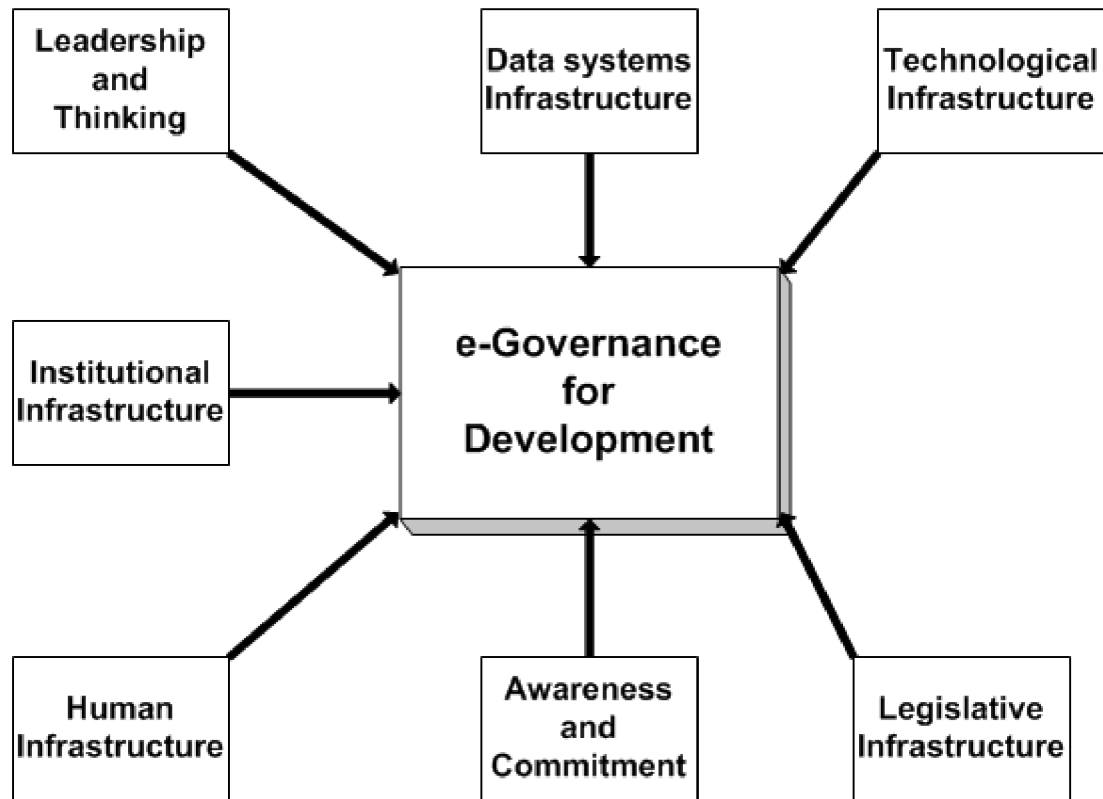


Figure: 1.8 The Strategic Response to the e-Governance

Figure 1.8 summarizes the package of strategic initiatives that is required. At the tactical level of individual e-Governance projects, identified best practice on design—reality gap closure must be adopted. Examples of such best practice include:

Legitimizing and mapping current reality

Integral to e-Governance project success is an understanding of reality. Yet this may be difficult to achieve. e-Governance project leaders can help by 'legitimizing reality': by encouraging stakeholders to articulate the difference between rational, prescriptive models of what they should be doing and

real depictions of what they are actually doing. Techniques for exposing and mapping organizational realities play a role here. Self and third party observation helps expose realities. Use of soft systems tools such as 'rich pictures' helps map realities. Prototyping helps both, particularly helping users to understand their real information needs.

Customization to match realities

As described above, e-Governance solutions designed for one sector or country are being forced directly into a very different reality, creating failure. To combat this, leaders of e-Governance projects must be competent enough and confident enough to demand designs that match their situation's unique reality. The keywords for such projects must be 'customized' not 'off-the-shelf'; 'adapt' not just 'adopt'.

Modularity and instrumentalism

With the growth in connectivity and as a natural consequence of dealing with millions of entities, e-Governance projects are frequently large. With pressures from donors/vendors and pressures to play catch-up with the private sector, e-Governance projects are frequently ambitious. But, the bigger and bolder the project, the greater the risk of failure. Designers must reconfigure such projects to limit the extent of change at any given time. Stretching project time horizons is one technique. There is also a growing consensus behind modularity (supporting one business function at a time) and instrumentalism (providing stepped levels of support for business functions) within e-Governance projects.

Hybrids and terminology

Design—reality gaps often arise because of a 'two tribes' mentality. IT designers understand technology but not the realities of governance. Officials and politicians understand the realities of governance but not the technology. 'Hybrid managers', who understand both perspectives, are the answer. Yet hybrid training is practically non-existent. Worse, the tribal gap is growing with increasing outsourcing of e-Governance work to the private sector. This exacerbates the clash of culture and values between designers and users. Terminology, too, is part of the problem. 'e-Governance' (electronic governance) may be unhelpful by suggesting, wrongly, that delivery of ICTs is an end in itself. As stated above, it may be more appropriate to talk of 'i-Governance' (integrated governance or, perhaps, intelligent governance) that places governance objectives in the driving seat, with ICTs seen as one part of the means to deliver those objectives alongside people, processes and information.

Closing specific gaps

As well as applying generic best practices such as those just described, it will also be important to address specific design—reality gaps. Early analysis of these gaps in e-Governance projects means moving beyond the narrow confines of typical risk assessment models, with their focus on the simple parameters of project resources. It means, instead, converting each of the ITPOSMO dimensions into a set of rating scales. Key project stakeholders then discuss and score these scales. The whole process can be undertaken as a facilitated workshop

with an iterative approach. The major design—reality gaps are identified, and the workshop then move to work out how to close those gaps. This process can become even more iterative if it forms part of a cycle of learning and reflection during the project.

In summary, the cases analyzed show that e-Governance has a key role to play in current and future development. It can offer critical improvements to the efficiency and effectiveness of governance; and probably offers critical future legitimacy for government. The issue for developing countries, therefore, is not 'if e-Governance' but 'how e-Governance'.

In addressing the 'how', that improvements and legitimacy will only be delivered if two things are in place. First, the strategic e-readiness infrastructure, especially the leadership and integrated vision on which e-Governance depends. Second, the tactical best practices that are needed to close design—reality gaps and to steer e-Governance projects from failure to success.

Footnote Reference:

- E-Governance Concepts & Case Studies, PHI publication - (India)
- Handbook of Cyber Laws, Macmillan publication - (India)
- "Television in Education" written by Dr. I. Arul Aram (The HINDU)
- www.netizens-cyberlaws.com
- www.egov.mit.gov.in
- www.compulsolsoftware.com
- www.delvelopmentgateway.org
- www.bagloreit.com
- www.bytesforall.org
- www.cadacindia.com
- www.man.ac.uk

Chapter – 2

Current Election System

2.1 Indian Election – an Overview

2.2 System of Election

2.3 Election Commission – to Conduct the Elections

2.4 Electronic Voting Machine (EVM)

2.5 Counting of Votes

2.1 Indian Election – an Overview

India is a constitutional democracy with a parliamentary system of government, and at the heart of the system is a commitment to hold regular, free and fair elections. These elections determine the composition of the government, the membership of the two houses of parliament, the state and union territory legislative assemblies, and the Presidency and vice-presidency.

2.1.1 Scale of Operation

Elections in India are events involving political mobilization and organizational complexity on an amazing scale. In the 1999 election to Lok Sabha there were 1299 candidates from 7 National parties, 750 candidates from 40 State parties, 654 candidates from officially recognized parties and 1945 Independent candidates. A total number of 37,16,69,282 people voted out of total electorate size of 61,95,59,944. The Election Commission employed almost 40,00,000 people to run the election. A vast number of civilian police and security forces were deployed to ensure that the elections were carried out peacefully.

2.1.2 Constituencies & Reservation of Seats

The country has been divided into 543 Parliamentary Constituencies, each of which returns one MP to the Lok Sabha,

the lower house of the Parliament. The size and shape of the parliamentary constituencies are determined by an independent Delimitation Commission, which aims to create constituencies, which have roughly the same population, subject to geographical considerations and the boundaries of the states and administrative areas.

2.1.3 Constituency Boundaries

Delimitation is the redrawing of the boundaries of parliamentary or assembly constituencies to make sure that there are, as near as practicable, the same number of people in each constituency. In India boundaries are meant to be examined after the ten-yearly census to reflect changes in population, for which Parliament by law establishes an independent Delimitation Commission, made up of the Chief Election Commissioner and two judges or ex-judges from the Supreme Court or High Court. However, under a constitutional amendment of 1976, delimitation was suspended until after the census of 2001, ostensibly so that states' family-planning programmes would not affect their political representation in the Lok Sabha and Vidhan Sabhas.

This has led to wide discrepancies in the size of constituencies, with the largest having over 25,00,000 electors, and the smallest less than 50,000. Delimitation exercise, with 2001 census data released on 31st December 2003, is now under process.

2.1.4 Reservation of Seats

The Constitution puts a limit on the size of the Lok Sabha of 550 elected members, apart from two members who can be nominated by the President to represent the Anglo-Indian community. There are also provisions to ensure the representation of scheduled castes and scheduled tribes, with reserved constituencies where only candidates from these communities can stand for election.

2.2 System of Election

Elections to the LokSabha are carried out using a first-past-the-post electoral system. The country is split up into separate geographical areas, known as constituencies, and the electors can cast one vote each for a candidate (although most candidates stand as independents, most successful candidates stand as members of political parties), the winner being the candidate who gets the maximum votes.

2.2.1 Parliament

The Parliament of the Union consists of the President, the LokSabha (House of the People) and the RajyaSabha (Council of States). The President is the head of state, and he appoints the Prime Minister, who runs the government, according to the political composition of the LokSabha. Although the government is headed by a Prime Minister, the Cabinet is the central decision making body of the government. Members of more than one party can make up a government, and although the governing parties may be a minority in the LokSabha, they can only govern as long as they have the confidence of a majority of MPs, the members of the LokSabha. As well as being the body, which determines whom, makes up the government, the LokSabha is the main legislative body, along with the RajyaSabha.

2.2.2 RajyaSabha - The Council of States

The members of the RajyaSabha are elected indirectly, rather than by the citizens at large. RajyaSabha members are elected by each state VidhanSabha using the single transferable vote system. Unlike most federal systems, the number of members returned by each state is roughly in proportion to their population. At present there are 233 members of the RajyaSabha elected by the VidhanSabhas, and there are also twelve members nominated by the President as representatives of literature, science, art and social services. RajyaSabha members can serve for six years, and elections are staggered, with one third of the assembly being elected every 2 years.

- RajyaSabha - Nominated members

The president can nominate 2 members of the LokSabha if it is felt that the representation of the Anglo-Indian community is inadequate, and 12 members of the RajyaSabha, to represent literature, science, art and the social services.

2.2.3 State Assemblies

India is a federal country, and the Constitution gives the states and union territories significant control over their own government. The VidhanSabhas (legislative assemblies) are directly elected bodies set up to carrying out the administration of the government in the 28 States of India. In some states there is a bicameral organization of legislatures, with both an

upper and Lower House. Two of the seven Union Territories viz., the National Capital Territory of Delhi and Pondicherry, have also legislative assemblies.

Elections to the VidhanSabhas are carried out in the same manner as for the LokSabha election, with the states and union territories divided into single-member constituencies, and the first-past-the-post electoral system used. The assemblies range in size, according to population. The largest VidhanSabha is for Uttar Pradesh, with 403 members; the smallest Pondicherry, with 30 members.

2.2.4 President and Vice-President

The President is elected by the elected members of the VidhanSabha, LokSabha, and RajyaSabha, and serves for a period of 5 years (although they can stand for re-election). A formula is used to allocate votes so there is a balance between the population of each state and the number of votes assembly members from a state can cast, and to give an equal balance between state and national assembly Parliament members. If no candidate receives a majority of votes there is a system by which losing candidates are eliminated from the contest and votes for them transferred to other candidates, until one gain a majority. The Vice President is elected by a direct vote of all members elected and nominated, of the LokSabha and RajyaSabha.

2.2.5 The single transferable vote system

Election for the members of the Rajya Sabha and the President are carried out using the single transferable vote system. The single transferable vote system is designed to ensure more diverse representation, by reducing the opportunity for blocks of voters to dominate minorities. The ballot paper lists all candidates standing for election and the voters' list them in order of preference. A threshold number of votes, known as the 'quota' are set, which candidates have to achieve to be elected. For presidential elections the quota is set at one more than half the number of votes, ensuring that the winner is the candidate who gets a clear majority. For the Rajya Sabha the quota is set at the number of votes that can be attained by just enough MPs to fill all the seats but no more. Votes that are deemed surplus, those given to candidates who have already got a full quota of votes, or votes given to candidates who are deemed to be losing candidates, are transferred according to the voter's listed preferences, until the right number of candidates have been elected.

2.3 Election Commission – to Conduct the Elections

An independent Election Commission has been established under the Constitution in order to carry out and regulate the holding of elections in India.

The Election Commission was established in accordance with the Constitution on 25th January 1950. Originally a Chief Election Commissioner ran the commission, but first in 1989 and later again in 1993 two additional Election Commissioners were appointed. The Election Commission is responsible for the conduct of elections to parliament and state legislatures and to the offices of the President and Vice-President.

The Election Commission prepares, maintains and periodically updates the Electoral Roll, which shows who is entitled to vote, supervises the nomination of candidates, registers political parties, monitors the election campaign, including candidates' funding. It also facilitates the coverage of the election process by the media, organizes the polling booths where voting takes place, and looks after the counting of votes and the declaration of results. All this is done to ensure that elections can take place in an orderly and fair manner.

At present, there are two Election Commissioners appointed by the President. Chief Election Commissioner can be removed from office only by parliamentary impeachment.

The Commission decides most matters by consensus but in case of any dissension, the majority view prevails. The Commission has its headquarters in New Delhi, with a Secretariat of some 300 staff members. At the state level a Chief Electoral Officer with a core staff of varying numbers, is available on a full time basis. At the district and constituency level, officers and staff of the civil administration double up as Election officials. During actual conduct of elections, a vast number of additional staff is temporarily drafted for about two weeks. They function mainly as polling and counting officials.

2.3.1 Eligibility to vote

The democratic system in India is based on the principle of universal adult suffrage; that any citizen over the age of 18 can vote in an election (before 1989 the age limit was 21). The right to vote is irrespective of caste, creed, religion or gender. Those who are deemed unsound of mind, and people convicted of certain criminal offences are not allowed to vote.

There has been a general increase in the number of people voting in Indian elections. In 1952 61.16 per cent of the electorate voted. By 1999 the turnout for the general election was 59.99 per cent. There have been even more rapid increases in the turnout of women and members of the scheduled castes and scheduled tribes, who had tended to be far less likely to participate in elections, and voting for these groups has moved closer to the national average.

2.3.2 The Electoral Roll

The electoral roll is a list of all people in the constituency who are registered to vote in Indian Elections. Only those people with their names on the electoral roll are allowed to vote. The electoral roll is normally revised every year to add the names of those who are to turn 18 on the 1st January of that year or have moved into a constituency and to remove the names of those who have died or moved out of a constituency. If you are eligible to vote and are not on the electoral roll, you can apply to the Electoral Registration Officer of the constituency, who will update the register. The updating of the Electoral Roll only stops during an election campaign, after the nominations for candidates have closed.

2.3.3 Computerization of Rolls

In 1998 the Commission took a historic decision to computerize the entire electoral rolls of 620 million voters. This work has been completed and now well-printed electoral rolls are available. The photo identity card number of the voter has also been printed in the electoral rolls, for cross-linking. The books of individual Parliamentary constituency rolls have also been put on CDs Rom. Both books and CDs are available for sale to general public. National and State parties are provided copies of such books and CDs free of cost after every revision of electoral rolls.

2.3.4 Electors' Photo Identity Cards

In an attempt to improve the accuracy of the electoral roll and prevent electoral fraud, the Election Commission ordered the making of photo identity cards for all voters in the country in Aug 1993. To take advantage of latest technological innovations, the Commission issued revised guidelines for EPIC Programme in May 2000. More than 400 million Identity cards have been distributed till now.

2.3.5 Occurrence of Elections

Elections for the Lok Sabha and every State Legislative Assembly have to take place every five years, unless called earlier. The President can dissolve Lok Sabha and call a general election before five years is up, if the government can no longer command the confidence of the Lok Sabha, and if there is no alternative government available to take over.

Governments have found it increasingly difficult to stay in power for the full term of a Lok Sabha in recent times, and so elections have often been held before the five-year limit has been reached. A constitutional amendment passed in 1975, as part of the government declared emergency, postponed the election due to be held in 1976. This amendment was later rescinded, and regular elections resumed in 1977.

Holding of regular elections can only be stopped by means of a constitutional amendment and in consultation with the Election

Commission, and it is recognized that interruptions of regular elections are acceptable only in extraordinary circumstances.

2.3.6 Scheduling the Elections

When the five-year limit is up, or the legislature has been dissolved and new elections have been called, the Election Commission puts into effect the machinery for holding an election. The constitution states that there can be no longer than 6 months between the last session of the dissolved Lok Sabha and the recalling of the new House, so elections have to be concluded before then.

In a country as huge and diverse as India, finding a period when elections can be held throughout the country is not simple. The Election Commission, which decides the schedule for elections, has to take account of the weather - during winter constituencies may be snow-bound, and during the monsoon access to remote areas restricted -, the agricultural cycle - so that the planting or harvesting of crops is not disrupted, exam schedules - as schools are used as polling stations and teachers employed as election officials, and religious festivals and public holidays. On top of this there are the logistical difficulties that go with holding an election sending out ballot boxes, setting up polling booths, recruiting officials to oversee the elections.

2.3.7 Eligibility to stand for Election

Any Indian citizens who are registered as a voter and are over 25 years of age are allowed to contest elections to the Lok Sabha or State Legislative Assemblies. For the Rajya Sabha the age limit is 30 years. Candidates for the Rajya Sabha and Vidhan Sabha should be a resident of the same state as the constituency from which they wish to contest.

Every candidate has to make a deposit of Rs. 10,000/- for Lok Sabha election and 5,000/- for Rajya Sabha or Vidhan Sabha elections, except for candidates from the Scheduled Castes and Scheduled Tribes who pay half of these amounts. The deposit is returned if the candidate receives more than one-sixth of the total number of valid votes polled in the constituency. Nominations must be supported at least by one registered elector of the constituency, in the case of a candidate sponsored by a registered Party and by ten registered electors from the constituency in the case of other candidates. Returning Officers, appointed by the Election Commission, are put in charge to receive nominations of candidates in each constituency, and oversee the formalities of the election.

In a number of seats in the Lok Sabha and the Vidhan Sabha, the candidates can only be from either one of the scheduled castes or scheduled tribes. The number of these reserved seats is meant to be approximately in proportion to the number of people from scheduled castes or scheduled tribes in each state.

There are currently 79 seats reserved for the scheduled castes and 41 reserved for the scheduled tribes in the Lok Sabha.

2.3.8 Political Parties and Elections

Political parties are an established part of modern mass democracy, and the conduct of elections in India is largely dependent on the behavior of political parties. Although many candidates for Indian elections are independent, the winning candidates for Lok Sabha and Vidhan Sabha elections usually stand as members of political parties, and opinion polls suggest that people tend to vote for a party rather than a particular candidate. Parties offer candidates organizational support, and by offering a broader election campaign, looking at the record of government and putting forward alternative proposals for government, help voters make a choice about how the government is run.

2.3.9 Registration with Election Commission

Political parties have to be registered with the Election Commission. The Commission determines whether the party is structured and committed to principles of democracy, secularism and socialism in accordance with the Indian Constitution and would uphold the sovereignty, unity and integrity of India. Parties are expected to hold organizational elections and have a written constitution. The Anti-defection law, passed in 1985, prevents MPs or MLAs elected as candidates from one party forming or joining a new party,

unless they comprise more than one-third of the original party in the legislature.

2.3.10 Recognition and Reservation of Symbols

According to certain criteria, set by the Election Commission regarding the length of political activity and success in elections, parties are categorized by the Commission as National or State parties, or simply declared registered-unrecognized parties. How a party is classified determines a party's right to certain privileges, such as access to electoral rolls and provision of time for political broadcasts on the state-owned television and radio stations - All India Radio and Doordarshan - and also the important question of the allocation of the party symbol. Party symbols enable illiterate voters to identify the candidate of the party they wish to vote for. National parties are given a symbol that is for their use only, throughout the country. State parties have the sole use of a symbol in the state in which they are recognized as such. Registered-unrecognized parties can choose a symbol from a selection of 'free' symbols.

2.3.11 Limit on poll expenses

There are tight legal limits on the amount of money a candidate can spend during the election campaign. Since December 1997, in most Lok Sabha constituencies the limit was Rs. 15,00,000/-, although in some States the limit is Rs 6,00,000/- (for Vidhan Sabha elections the highest limit is Rs

6,00,000/-, the lowest Rs 3,00,000/-). Recent amendment in October 2003 has increased these limits. For Lok Sabha seats in bigger states, it is now Rs 25,00,000. In other states and Union Territories, it varies between Rs 10,00,000 to Rs 25,00,000. Similarly, for Assembly seats, in bigger states, it is now Rs 10,00,000, while in other states and Union Territories; it varies between Rs 5,00,000 to Rs 10,00,000. Although supporters of a candidate can spend as much as they like to help out with a campaign, they have to get written permission of the candidate, and whilst parties are allowed to spend as much money on campaigns as they want, recent Supreme Court judgments have said that, unless a political party can specifically account for money spent during the campaign, it will consider any activities as being funded by the candidates and counting towards their election expenses. The accountability imposed on the candidates and parties has curtailed some of the more extravagant campaigning that was previously a part of Indian elections.

2.3.12 Splits and mergers and anti-defection law

Splits, mergers and alliances have frequently disrupted the compositions of political parties. This has led to a number of disputes over which section of a divided party gets to keep the party symbol, and how to classify the resulting parties in terms of national and state parties. The Election Commission has to resolve these disputes, although its decisions can be challenged in the courts.

2.3.13 Election Campaign

The campaign is the period when the political parties put forward their candidates and arguments with which they hope to persuade people to vote for their candidates and parties. Candidates are given a week to put forward their nominations. The Returning Officers scrutinize these and if not found to be in order can be rejected after a summary hearing. Validly nominated candidates can withdraw within two days after nominations have been scrutinized. The official campaign lasts at least two weeks from the drawing up of the list of nominated candidates, and officially ends 48 hours before polling closes.

During the election campaign the political parties and contesting candidates are expected to abide by a Model Code of Conduct evolved by the Election Commission on the basis of a consensus among political parties. The model Code lays down broad guidelines as to how the political parties and candidates should conduct themselves during the election campaign. It is intended to maintain the election campaign on healthy lines, avoid clashes and conflicts between political parties or their supporters and to ensure peace and order during the campaign period and thereafter, until the results are declared. The model code also prescribes guidelines for the ruling party either at the Center or in the State to ensure that a level field is maintained and that no cause is given for any complaint that the ruling party has used its official position for the purposes of its election campaign.

Once an election has been called, parties issue manifestos detailing the program they wish to implement if elected to government, the strengths of their leaders, and the failures of opposing parties and their leaders. Slogans are used to popularize and identify parties and issues, and pamphlets and posters distributed to the electorate. Rallies and meetings where the candidates try to persuade, cajole and enthuse supporters, and denigrate opponents, are held throughout the constituencies. Personal appeals and promises of reform are made, with candidates traveling the length and breadth of the constituency to try to influence as many potential supporters as possible. Party symbols abound, printed on posters and placards.

2.3.14 Free Campaign time on state owned electronic-media

By Election Commission, all recognized National and State parties have been allowed free access to the state owned electronic media-AIR and Doordarshan- on an extensive scale for their campaigns during elections. The total free time allocated extends over 122 hours on the state owned Television and Radio channels. This is allocated equitably by combining a base limit and additional time linked to poll performance of the party in recent election.

2.3.15 Polling Days

Polling is normally held on a number of different days in different constituencies, to enable the security forces and those monitoring the election to keep law and order and ensure that voting during the election is fair.

2.3.16 Ballot Papers & Symbols

After nomination of candidates is complete, the Returning Officer prepares a list of competing candidates, and ballot papers are printed. Ballot papers are printed with the names of the candidates (in languages set by the Election Commission) and the symbols allotted to each of the candidates. Candidates of recognized Parties are allotted their Party symbols.

2.3.17 Supervising Elections, Election Observers

The Election Commission appoints a large number of Observers to ensure that the campaign is conducted fairly, and that people are free to vote as they choose. Election expenditure Observers keeps a check on the amount that each candidate and party spends on the election.

2.3.18 Media Coverage

In order to bring as much transparency as possible to the electoral process, the media are encouraged and provided with facilities to cover the election, although subject to maintaining

the secrecy of the vote. Media persons are given special passes to enter polling stations to cover the poll process and the counting halls during the actual counting of votes.

2.3.19 Voting with traditional Ballot Paper

Voting is by secret ballot. Polling stations are usually set up in public institutions, such as schools and community halls. To enable as many electors as possible to vote, the officials of the Election Commission try to ensure that there is a polling station within 2km of every voter, and that no polling stations should have to deal with more than 1500 voters. Each polling station is open for at least 8 hours on the day of the election.

On entering the polling station, the elector is checked against the Electoral Roll, and allocated a ballot paper. The elector votes by marking the ballot paper with a rubber stamp on or near the symbol of the candidate of his choice, inside a screened compartment in the polling station. The voter then folds the ballot paper and inserts it in a common ballot box, which is kept in full view of the Presiding Officer and polling agents of the candidates. This marking system eliminates the possibility of ballot papers being surreptitiously taken out of the polling station or not being put in the ballot box.

Since 1998, the Commission has increasingly used Electronic Voting Machines instead of ballot boxes. In 2003, all state elections and bye-elections were held using EVMs. Encouraged

by this the Commission had taken a historic decision to use only EVMs for the Lok Sabha election in 2004.

2.4 Electronic Voting Machine (EVM)

Electronic Voting Machine (EVM) retains all the characteristics of voting by ballot papers, while making polling a lot more expedient. Being fast and absolutely reliable, the EVM saves considerable time, money and manpower. And, of course, helps maintain total voting secrecy without the use of ballot papers. The EVM is 100 per cent tamper proof. And, at the end of the polling, just press a button and there you have the results.

The EVM consists of two units that can be inter-linked.

1. Ballot Unit, which a voter uses to exercise his vote.
2. Control Unit – used by the polling officials.

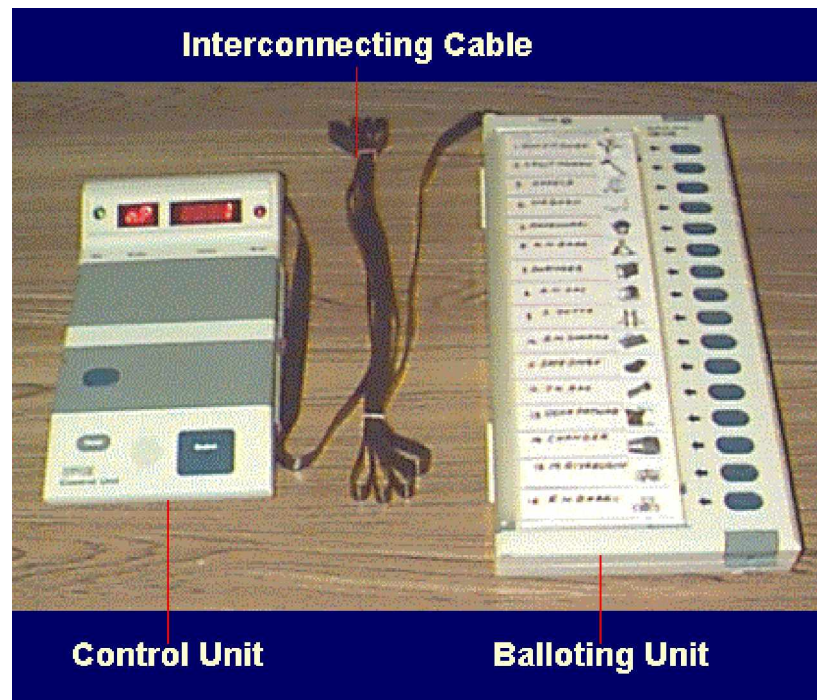


Figure 2.1 Components of Electronic Voting Machine

2.4.1 The Ballot Unit: An electronic ballot box.

A simple voting device, it displays the list of candidates. A facility to incorporate party names and symbols is in-built. All the voter has to do is press the desired switch located next to the name of each candidate. The main advantage is the speed, apart from the simplicity of operation, which requires no training at all. A single ballot unit takes in the names of 16 candidates. And thus, by connecting four ballot units the EVM can accommodate a total of 64 candidates in a single election.

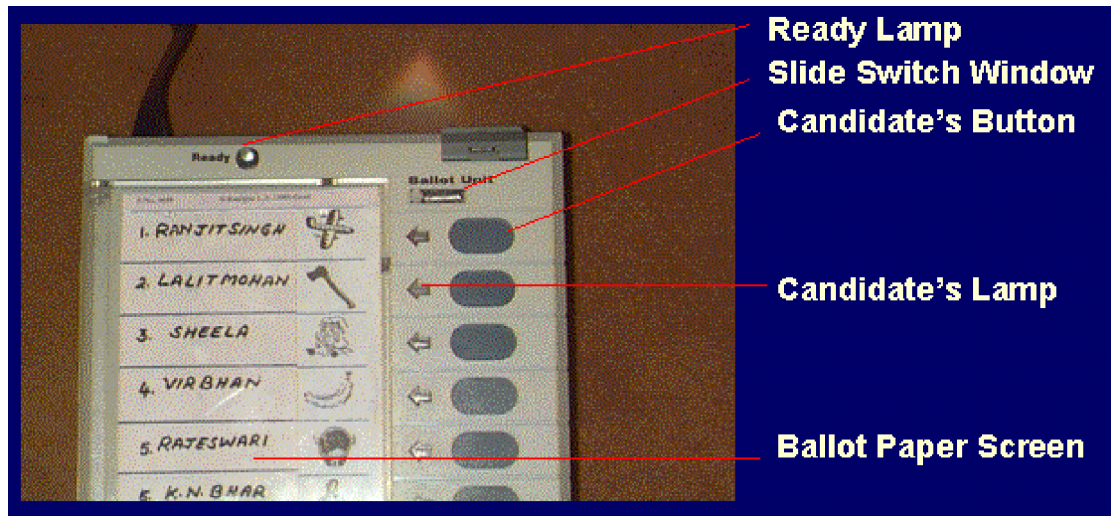


Figure: 2.2 Balloting Unit

2.4.2 The control Unit: In Total control of the polling

Conduction of polling, display of total votes polled, sealing at the end of the poll, and finally, declaration of results – these are the various accomplishments of just one gadget: the control unit. In total control of the polling, this electronic unit

gives you all necessary information at a press of a few buttons. For instance, if you need to know the total number of votes, you just have to press the Total switch. Candidates-wise results can be had only at the end of polling.

2.4.3 Cast Vote Through Electronic Voting Machine

- A. Voter will be called by name as usual to put his signature on Voting Register.
- B. Electoral Officer will put special ink on his finger as usual.
- C. Electoral Officer will hand over a slip containing voter's serial number as shown in the Voter Register.
- D. Voter will hand over the slip to Presiding Officer. He will satisfy himself about the genuineness of the particulars of the voter.
- E. After all these formalities, voter will be asked to reach at Electronic Voting Machine kept in a corner covered from sides to maintain secrecy of the vote.

Voting Machine will contain candidates name and symbol against each name. There will be a red light and a blue button. Voter shall have to press the blue button against the candidate of the choice. Red light will appear on the pressing of blue button and sound like whistle will also be heard which will indicate that the ballot has been casted. If red light does not appear voter can press the blue button again.

2.4.4 Preparation of EVM for Voting

2.4.4.1 Fixing the ballot paper

On every balloting unit, a printed ballot paper shall be displayed in the space specially provided for the purpose under a transparent acrylic sheet (ballot paper screen). The ballot paper shall contain the serial number of each candidate, his name and the election symbol allotted to him as per the list of contesting candidates. Where the number of contesting candidates exceeds sixteen the ballot paper shall be printed on more sheets than one as each balloting unit will cater up to sixteen candidates only. Where the number of candidates exceeds sixteen but is equal to or less than thirty two, the ballot paper shall be printed on two sheets – the first sheet containing the names, etc., of candidates from Sl. No. 1 to 16 and the second sheet containing the names, etc., of candidates from Sl. No.17 onwards. Likewise, where the number of candidates exceeds thirty-two and is up to forty eight, the third sheet will contain the names, etc., of candidates from Sl. nos. 33 onwards and up to 48, and where the number of candidates exceeds forty-eight; the fourth sheet will contain the names etc., of candidates from Sl No. 49 onwards. In such cases, each sheet of the ballot paper will be displayed on separate balloting units.

Every ballot paper shall have a serial number and sheet number where printed on more than one sheet. The sheet number will be indicated as ½, if it is the first sheet and two

sheets are used 3/4, if it is the third sheet and four sheets are used and 50 on. Before it is inserted and fixed on a balloting unit, it shall be either signed on its back by the Returning Officer or stamped on its back with a rubber stamp bearing the facsimile signature of the Returning Officer.

For fixing the ballot paper under the ballot paper screen, first the top cover of the balloting unit has to be opened. This can be done by pressing simultaneously, towards right, the latches at the top and bottom on the right edge of the unit and swinging the cover up. The top cover and the lower portion of the balloting unit will then open like a book. Thereafter, the ballot paper screen, which is hinged to the top cover on the extreme left side, will be opened. The release latches of the screen are inside the top cover. By pressing the latches simultaneously, first slightly towards right and then pushing them downwards the ballot paper screen will become free for opening on the upper side of the top cover. After so opening the ballot paper screen, the ballot paper will be placed in the space provided for the purpose on the upper side of the top cover of the balloting unit. The ballot paper will be properly aligned so that each candidate's name and his symbol are in line with the corresponding lamp and button and the thick lines dividing the panels of candidates on the ballot paper are in line with the corresponding grooves on the balloting units.

After ballot paper has been firmly fixed and the ballot paper screen has been closed and pressed-fit on the upper side of the top cover, the screen will be sealed on the inner side of the top

cover, by passing a thread through the two holes on the screen specially provided for the purpose on the inner side. The two ends of the thread will be placed on an address tag and the Returning Officer will put his seal on the thread and the address tag. The address tag will contain the following particulars: -

Election to the
 From Constituency
 Serial No. of balloting unit
 Date of poll.....

2.4.4.2 Masking of candidates' buttons, which are not to be used

On the balloting unit, only those candidates' buttons should be visible which are to be used by voters. In other words, the number of candidates' buttons, which should be visible, will be equal to the number of contesting candidates. For example, if the number of candidates is nine, only the nine buttons from the top (i.e., 1 to 9) should be visible and the remaining seven buttons (i.e., 10 to 16) should be masked. The masking of the unwanted buttons will be done by moving the white masking tabs on to the candidates' button, when the balloting unit is still open like a book as explained above.

2.4.4.3 Setting of slide switch

Inside the balloting unit, on the top right side, there is a slide switch that has four positions 1,2,3 and 4. The positioning of this slide switch determines the serial order in which a particular balloting unit is to be linked with the control unit and kept inside the voting compartment for use at a polling station.

Where the number of contesting candidates is up to sixteen only one balloting unit will be used. In such case, the slide switch shall be set to the position marked '1'. Where the number of contesting candidates is more than sixteen and up to thirty-two, two balloting units will be used. In the first balloting unit, the ballot paper containing the names of candidates at serial nos. 1 to 16 will be fixed, and its slide switch shall be set to the position marked '1' and in the second balloting unit where the ballot paper containing the names of candidates from 17 onwards is fixed its slide switch shall be set to the position marked '2'.

Likewise, if three balloting units are to be used in a constituency where the number of contesting candidates exceeds 32 and is up to 48, the slide switch will be set to the position marked '3' in the third balloting unit. Similarly, if the fourth balloting unit is also to be used in case the number of contesting candidates exceeds 48, then the slide switch will be set to the position marked '4' in the last balloting unit. Any wrong setting of a slide switch will render the whole voting machine nonfunctional.

2.4.4.4 Sealing of the balloting unit

After the ballot paper has been inserted, fixed and sealed under the ballot paper screen, the candidates' buttons which are not required for use have been masked and the slide switch has been set to the required position, the balloting unit will be closed by bringing the top cover back to its original position. The balloting unit will then be sealed by the Returning Officer with his own seal, by passing two threads, one through the three holes at the top and the other through the three holes at the bottom specifically provided for the purpose, and attaching an address tag containing the following particulars: -

Election to the

FromConstituency

Balloting Unit No.

Serial No. and name of polling station where used.....

Date of poll.....

The candidates and their agents will be allowed, if they so desire to affix their seals on these address tags, in addition to the Returning Officers' seal.

After the balloting unit has been so prepared and sealed, it will be kept back in its carrying case. An address tag containing the above particulars will be attached to the handle of the carrying case.

2.4.4.5 Inter-linking of balloting units and control unit

Where the number of contesting candidates exceeds sixteen, balloting units more than one, depending upon the actual number of contesting candidates, will be used. All such balloting units to be used at a polling station are to be inter-linked and the first balloting unit will alone be linked with the control unit.

The balloting units shall be so inter-linked that the second balloting unit, i.e., the balloting unit in which the slide switch is set at position 2, is linked with the first balloting unit in which the slide switch is set at position 1, where the balloting units are to be used, the third balloting unit will be linked with the Second balloting unit and the second with the first, and where all the four balloting units are to be used, the fourth unit will be linked with the third unit, the third with the second and so on.

For linking one balloting unit with another, there is a socket provided in a compartment at the bottom portion of the balloting unit. The connector of the interconnecting cable of the second balloting unit will be plugged into the abovementioned socket of the first balloting unit. Likewise, the connector of the third balloting unit's interconnecting cable will be plugged into the second unit and that of the fourth unit into the third unit.

As mentioned above, the first balloting unit alone will be plugged into the control unit. The socket for plugging the interconnecting cable of the balloting unit into the control unit is provided in the rear compartment of the control unit.

That rear compartment in the control unit also contains the 'Power' switch and this switch when put to 'ON' position makes the battery of the voting machine operational and supplies the power both to the control unit as well as to all the balloting units when linked to the control unit in the manner described above.

Any wrong linking of the balloting units will render the machine non-functional and on pressing any button on the control unit the letters 'LE; indicating linking error will appear on the display panel of the control unit. The linking error can be set right by re-interlinking the balloting units in the proper sequential order.

2.4.4.6 Preparation of control unit

Like the balloting unit, some preparations are to be made in the control unit also of the voting machine at the Returning Officer's level. These preparations are: -

- (1) Installation of the battery;
- (2) Setting the number of contesting candidates; and

- (3) Sealing that election of the Control unit which is called 'Candidate Set Section' and which contains the battery and the button to set the number of candidates.

2.4.4.7 Battery installation

The Electronic Voting Machine operates on a special battery, which is supplied by the manufacturing company. A new battery will be used whenever a machine is used at any election. There is provision for installation of the battery in compartment on the topside of the control unit in the 'Candidate Set Section'.

2.4.4.8 Setting the number of contesting candidates

A control unit of the voting machine can cater up to sixty-four candidates. Therefore, at every election where the voting machine is used, the control unit has to be set according to the number of contesting candidates at that election. For setting the number of contesting candidates, the following operations shall be performed: -

- (i) The number of contesting candidates can be set in the control unit only by linking this unit with the balloting unit or with all the balloting units where more than one balloting units are to be used.
- (ii) After the control unit and the balloting unit(s) have been linked, the 'Power' switch will be pushed to 'ON'

position so that both the units get the necessary power to make them operational.

- (iii) The button marked 'Cand Set' in the 'Candidate Set Section' of the control unit will then be pressed. Thereupon, the two-digit Display Panel on the left side of the Display Section of the control unit will flash the letters 'Cd' and the four digits Display Panel on the right side will flash.
- (iv) When the letters 'Cd-' start flashing on the Display Panels on the control unit, the Candidate's button against the last contesting candidate in the balloting unit will be pressed. For example, if there are nine contesting candidates and the machine is to be set for new candidates, candidate's button of the ninth candidate on the balloting unit will be pressed. If the number of contesting candidates is more than 16, say, 23 the candidates button against the name of the contesting candidate at serial no. 23 in the second balloting unit will be pressed. On that button being pressed, the Display Panels will stop flashing the letters 'Cd-' and instead the full Panel will display the number of candidates for which the machine has been so set, like Cd 9' or, as the case may be 'Cd 23'.

If by mistake, a wrong button on the balloting unit has been pressed which will set either less or more number of contesting candidates, such wrong setting can be corrected by pressing the 'Cand Set' button again. The machine will again flash the letters 'Cd -' and the correct button on the balloting unit can

be pressed so as to set the correct number of contesting candidates.

The number of contesting candidates can be set in any number of Control Units by using only one balloting unit on one set of balloting units (where more than one balloting units are to be used depending upon the number of contesting candidates).

2.4.4.8 Clearing the machine

After the number of contesting candidates has been set in the control unit in the manner described above, all the data recorded in the machine relating to a previous election, if any, will be cleared. For this purpose, the button marked 'Clear' in the Result section of the control unit will be pressed. On the 'Clear' button being pressed, all the counts in the machine shall be automatically set to ZERO and the display panels on the control unit will start displaying that the number of votes recorded in the machine for each contesting candidate is '0' (zero).

After the control unit has been set according to the number of contesting candidates at the election and the previous data cleared, the power will be switched off and the control unit and the balloting unit(s) will be delinked by removing the interconnecting cable from the control unit.

2.4.4.9 Sealing the 'Candidate Set Section'

After the battery has been installed in the 'Candidate Set Section' and the control unit has been set according to the number of contesting candidates, the 'Candidate Set Section' will be closed and sealed so that nobody can have access to the battery and the 'Cand Set' button in the 'Candidate Set Section' thereafter.

Replacing the cover and pressing it tight will close the 'Candidate Set Section'. It will be sealed by passing a thread through the two holes provided for the purpose on the left side giving a light knot to the thread and placing the two ends of the thread on an address tag which will be sealed with the Returning Officer's seal. The address tag will contain the following particulars: -

Election to the.....

From.....

Constituency.....

Control Unit No.

Serial No. and name of polling station where used.....

Date of Poll.....

The candidates and their agents shall be allowed to put their seals, if they so desire, on the address tag along with the seal of the Returning Officer. The Control unit will then be put in its carrying case, which will now be ready for transportation to the

polling station. On the handle of the carrying case of control unit also, an address tag will be attached containing the above particulars.

2.4.4.10 Random checking of voting machine

Though each and every voting machine has already been fully tested, the Returning Officer will again get 5% of the machines to be used at the election, subject to a minimum of 10 machines, tested and checked at random for their 100% error free performance after the machines have been prepared in the manner described in the foregoing paragraphs. For this purpose, he may ask the candidates and their agents present to choose the machines, which may be tested for such random check.

For conducting the above random test and check, the Returning Officer will hold a mock poll on those machines by casting a few votes at random for each of the contesting candidates.

After the conduct of the mock poll, the machines will be cleared of the data recorded at the mock poll and all counts will again be put to ZERO in all in the machines used for the mock poll.

2.4.4.11 Safe preservation of prepared voting machines

All the voting machines which have been prepared for use at the election, including the reserve machines, will be kept and preserved in safe custody in a strong room under double lock

which will be sealed with the seal of the Returning Officer. The candidates and their agents will also be permitted to put their seals on the lock, if they so desire.

The strong room will be opened only on the appointed date and time when the machines are to be supplied to polling parties before they leave for their polling stations. All contesting candidates or their election agents will be given prior notice in writing of such date and time of opening of the strong room. A proper logbook will be maintained giving details of such closing and opening of the strong room. The strong room will be kept fully guarded of all times under the charge of a Senior Police Officer.

2.4.4.12 Maintenance of records of voting machines

The Returning Officer will maintain complete record of all the control units and balloting units used at the election. That record will show clearly the number of control unit and balloting unit(s) used at each polling station along with the serial numbers of each such unit. The record will also show the number of control units and balloting units along with their serial numbers, which have been prepared for use and kept in reserve. If any of such control units or balloting units is put to use, a complete record as to where each such unit was used will be properly maintained which will also show the reasons for which the use of such reserve unit became necessary.

2.4.4.13 Supply of voting machines to polling parties

The voting machines will be supplied only to the Presiding Officers or in their unavoidable absence, to the first polling officers of the polling stations against a proper receipt to be obtained from each Presiding Officer in a register to be kept separately for the purpose.

That register will have further provision for keeping proper account of the machines received back from the Presiding Officers.

The reserve machines will be kept at a central place or places in the constituency on the day of poll so that the same may be supplied with least possible delay to any polling station where an emergent need arises for replacement of any control unit or balloting unit(s). These machines will be kept under the charge of one of the Assistant Returning Officers or some other senior officer specifically nominated for the purpose by the Returning Officer.

2.4.5 The advantages in using EVMs

The most important advantage of EVM is that the printing of lakhs of ballot papers can be dispensed with, as only one ballot paper is required for fixing on the Balloting Unit at each polling station instead of one ballot paper for each individual elector. This results in huge savings by way of cost of paper, printing, transportation, storage and distribution.

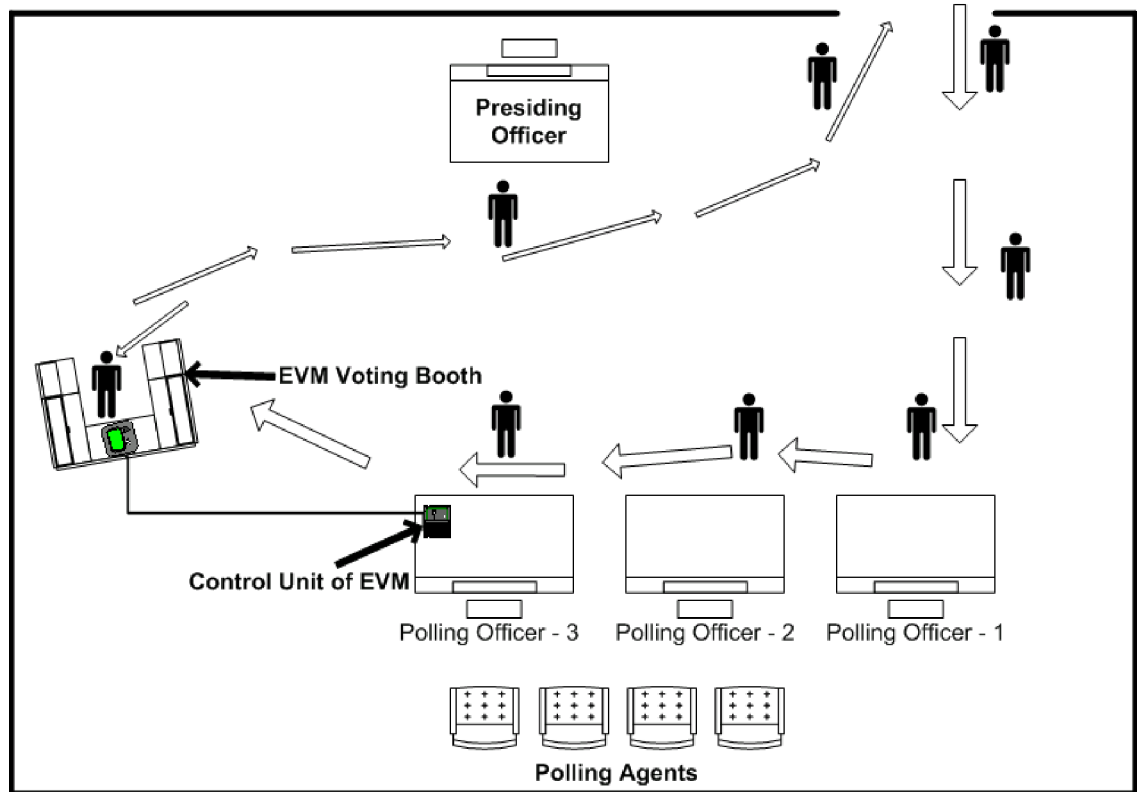


Figure: 2.3 Model Layout of EVM Polling Station

Counting is very quick and the result can be declared within 2 to 3 hours as compared to 30-40 hours, on an average, under the conventional system.

There are no invalid votes under the system of voting under EVMs. The importance of this will be better appreciated, if it is remembered that in every General Election, the number of invalid votes is more than the winning margin between the winning candidate and the second candidate, in a number of constituencies. To this extent, the choice of the electorate will be more correctly reflected when EVMs are used.

- Independent & Reliable

The EVM is compact and comes in its reusable carry pack. Further, the EVM works/operates on a battery power source. Making it independent and totally reliable.

- Hi-tech Simplicity

To commence polling, the polling officer activates the "Ballot" switch on the control unit. The voter then has to press the button of his choice on the ballot unit. This is followed by a short beep sound, indicating that the vote has been cast. Once again, the polling officer has to press the "Ballot" switch to clear the machine for the next voter to cast his vote.

- Super-sensitive circuitry: No invalid votes

Inside the control unit, hidden from you, is an extremely sensitive circuitry that takes care of common election errors or malpractices like vote duplication. For instance, if one were to press two or more buttons simultaneously, then no vote would be cast. Even if there was a microsecond difference in the pressing of the switches, the EVM is sensitive enough to trace and identify the twitch that was press first.

- Instant results

Once polling is completed, the election results can be known instantly at the counting station by pressing the "Result"

switch. This switch is located in a sealed compartment of the control unit.

- Tamper proof design

The EVM is designed to be totally tampering proof. Each EVM comes with a sophisticated program in assembly language: software fully seated against outside influence. And the program is itself fused on to a customized microprocessor chip at the manufacturer's end. This ensures that the program is rendered tamper proof and inaccessible.

- Result Printout

Normally, an EVM displays results on the display panel of the control unit. But a printout option is available with the use of a Download Adaptor Unit (DAU). The DAU has to be connected to the control unit and any standard printer. Further, with the help of a modem, the DAU can also enable transmission of voting information to a distant centralized computer.

2.5 Counting of Votes

After the polling has finished, the votes are counted under the supervision of Returning Officers and Observers appointed by the Election Commission. After the counting of votes is over, the Returning Officer declares the name of the candidate to whom the largest numbers of votes have been given as the winner, and as having been returned by the constituency to the concerned house.

2.5.1 Maintenance of Secrecy

Every person inside the counting hall is required by law to maintain, and aid to maintaining, the secrecy of voting and should not communicate to any person any information calculated to violate such secrecy. They should note that any person contravening the provisions of law in this respect is liable to be punished with imprisonment for a term, which may extend to 3 months or with fine or with both (Section 128 of the R.P. Act, 1951)

"The counting of votes will, as far as practicable, be proceeded with continuously till it is over."

The counting of postal ballot papers will be taken up first. This will be done by the Returning Officer himself at the place of counting of votes in the case of election from an assembly constituency and at the place where the results of the various

assembly segments of a parliamentary constituency are consolidated in the case of election to the House of the People.

2.5.2 Counting of Votes from Polling Stations

At the time of counting, only the control unit of the voting machine is required for ascertaining the result of poll at the polling station at which the control unit has been used. The balloting unit is not required.

While the postal ballot papers are being counted by the Returning Officer at his table, the counting of votes recorded at polling stations by means of voting machines will also be taken up by the Assistant Returning Officer(s) at the other tables provided in the counting hall. For that purpose, the control units of voting machines received from the polling stations will be distributed to the various counting tables, beginning with the control unit of voting machine of polling station No. 1, being distributed to table No. 1, the control unit of voting machine of polling station No.2 being distributed to table No.2 and so on. At each counting table, votes cast at one polling station shall be taken up at a time. Thus the counting of votes of as many polling stations as there are the number of counting tables will be simultaneously taken up in the first round of counting.

The counting will be done and completed in as many rounds as are necessary, having regard to the number of counting tables and number of polling stations. The control units for the next round will not be brought on the counting tables, unless the

counting of the previous round is over. In case of simultaneous elections the total number of counting tables should be divided into two groups of equal number of tables. The first group should be for Assembly election and the other group for the Parliamentary election. For example, if the total number of counting tables is 14 (fourteen), in the first round of counting, control unit for Assembly election used at polling station number 1 should be given to table number 1 and the control unit used for Lok Sabha election at polling station number 1 should be given to table number 8, i.e., the first table for the counting of votes for Lok Sabha election, and control unit for Assembly election used at polling station number 2 should be given to table number 2 and the control unit used for Lok Sabha election at polling station number 2 should be given to table number 9, i.e., the second table for the counting of votes for Lok Sabha election and so on. Keep an account of such distribution with you for your information. It is to be noted that in the case of counting for simultaneous elections, the next round of counting shall be taken up only after the counting in the previous round, in respect of both Assembly and Parliamentary elections is completed and Control Units used in the polling stations covered by the round completed are removed from the counting tables.

2.5.3 Recount

Normally, there will be no question of recount of votes recorded in the voting machines. Every vote recorded by the voting machines is a valid vote and no dispute will arise as to its

validity or otherwise. At the most, some candidates or their agents may not have noted down properly the result of voting at any particular polling station when the control unit displayed that information. If necessity arises for re-verification, pressing the Result Button can do the same, whereupon the result of voting at that polling station will again be displayed in the Display Panels of that control unit.

2.5.4 Result Declaration

Accordingly, after the entire counting is over, the Returning Officer will announce that result giving the total number of votes polled by each candidate as recorded in the Final Result Sheet. After the announcement is made, a candidate, or in his absence his election agent or any of his counting agents, may apply in writing for a recount of votes recorded at all or any of polling stations stating the grounds on which he demands such recount. For this purpose, the Returning Officer will announce the exact hour and minute up to which he will wait for receiving the written application for recount. When such an application for recount is made, the grounds urged for the recount will be considered and a decision taken by the Returning Officer. He may allow the application in whole or in part if it is reasonable, or he may reject it in to if it appears to be frivolous or unreasonable. The decision of the Returning Officer will be final. If, in any case, an application for recount either wholly or in part is allowed, the Returning Officer will direct counting of the votes over again. The postal ballot papers may also be recounted if a request is made for their recount and such a

request is allowed by the Returning Officer. After such recount has been completed, the result sheet will be amended to the extent necessary and the amendments so made announced. After the total number of votes polled by each candidate has been announced, the result sheet will be completed and signed.

Footnote Reference:

- "Handbook for Returning Officers",
Election Commission of India, New Delhi - INDIA.
- "Handbook for Counting Agents",
Election Commission of India, New Delhi - INDIA.
- www.eci.gov.in
- www.indian-elections.com
- www.indiademocracy.com

Chapter – 3

Unique Identity Smart Citizen Card

- 3.1 Unique Identity Citizen Card – Need for common people
- 3.2 Smart Card Technology – an Overview
- 3.3 Smart Card as a unique identity Citizen Card
- 3.4 Central Database for the card

3.1 Unique Identity Citizen Card – Need for common people

The need of multipurpose Citizen Card has been felt now instead of multiple cards, multiple databases by various government departments. The current approach of e-Governance is not integrated and does not give convenience to the citizen in getting information and services. Looking to the needs for easy access of information and services by citizen, effective and better management of e-Governance by government and integrated approach for Citizen Card serving multipurpose for e-Governance has been represented as a model in this chapter.

An average citizen of a country considers Government as one single entity. Only an educated person would know that the affairs of the Governments are dealt at various levels. In India, for example, the subjects of the Governance are broadly distributed in the Central, State, Municipal and Panchayat levels. The Governments are further divided into various departments. Each department of the Government is independent and dealing with the governance separately. Some governments and some departments have made rapid progress in the implementation of the e-Governance while others have not taken even the first step toward e-Governance. Today, the citizen has to probably visit dozens of websites to locate the departments and then probably get them registered on the website to obtain information. The information, which can be

obtained today, is general in nature and can rather be classified in the category of news other than fruitful information.

A common citizen would like to deal the Government as a whole. He does not want to waste time in understanding the intricacies of the Government and visit to numerous offices of different departments to get solution of his problems. Therefore, integrated and co-coordinated efforts from all the government departments are required in the implementation of e-Governance. A model of citizen card is ideal logical step in the direction of the nationally integrated & coordinated e-governance.

The need of Identity Card for social security & nationality felt in India from quite some time. The I-card was intended to serve different purposes for different departments. For example in border areas, the purpose of the card would be to identify the illegal migrants, terrorists. In other areas it could help the officers to verify the authenticity of the voters during elections.

As per the current scenario a citizen has to submit his personal details to various government and private departments like Income Tax, Customs & Excise, RTO, Municipalities, Sales Tax Departments, Industry department, Banks, Post Offices, Credit Card companies, home/consumer loan companies, Insurance companies etc. This generates data redundancies to government entity as a whole and the system generates complex problems e.g. whenever any citizen changes his

address, he has to intimate all the departments individually. Since the departments do not share the information the citizen may intimate only some department regarding the change while he may miss to make changes or deliberately omit some departments. It has been noticed that very many criminals, tax/loan defaulters continue to enjoy the fruits by evading tax / non-paying of loan installments just by changing the address frequently. The genuine citizen may however loose dividends, refunds and other benefits, important information / deadlines as he just missed to communicate the change of address to the concerned department at the right time.

It would be a great benefit to the Citizens and the Government, if one single agency maintains all the personal details of the citizen and the citizen is required to intimate only to one agency for the change. All the agencies can access the database and maintain their local data always updated. All state governments, local governments, other departments' can use this information for their purpose.

The information can be broadly divided into two categories i.e. general and confidential. All the contracting parties can share the general information. However, the confidential information should be shared only among the selected parties/ department. Other parties can also be supplied the information in deserving cases on the basis of specific request on sanction by competent authority.

The card needs a design to serve multiple applications. Looking to the benefits, it can offer must attract every citizen to have this card. The card is desired to be a Smart Card with Biometric Authentication (Bio-Smart Card) offering following benefits to its user. This card can be popularly called as Citizen Card (CC).

- The card is to act like multipurpose identity card.
- It is to act like an ATM/ Debit Card for drawing salary, pension, scholarships unemployment allowance, insurance, etc from any ATM machine.
- A citizen can use this card as ATM card to deposit their taxes, telephone bills, Customs and Excise duty, Income Taxes etc at ATM Machine.
- The card is to be used as Security Device cum Identification card to access any secured site from the web, to access personal page information and to edit any particular online.
- The card is to be used to verify the authenticity of the user of the e-commerce / e-business.
- It is to act like a Driving License (DL) and I-card for the Government Officers. The existing DL holders can surrender their DLs to the Vendors and get a composite card made. Those who had been already issued the Citizens card will have the option to get a Composite Card from RTO office after surrendering their CC.
- The unemployed youths would be automatically registered with the employment exchange and be intimated about

any job opportunity from Government / Private Sector Enterprises as per his qualification and experience.

- Credit ratings can be assigned to each citizen depending upon his past records and his economical soundness to enable him to take loan, overdrafts, police verification, passport issue etc before any Government/ private enterprises.
- Various Departments of the Government can access this data with the due authorization. For example, the Income Tax department can use the value of the total transaction in a year to verify the income declared by the citizen in his Income tax return. Police can trace an absconder from the data warehouse. The Banks and the Revenue Departments can trace the defaulters.
- A citizen can use this card to vote at time election from any place, because once the card is unique and its record is stored in central database then at the time of election government can make e-voting by creating virtual polling booths. These booths can be a bank's ATM center or can be a government undertaken cyber-cafe or government institution, which are capable to provide Internet connectivity. In this case citizen can vote at any place and his authentication will be done using citizen (smart) card as well as biometric authentication with central database server.

3.2 Smart Card Technology

Smart card technology has been around for more than 20 years. The technology has its historical origin in the seventies when inventors in Germany, Japan, and France filed the original patents. While inventors in the U.S., Japan and Austria, were issued patents, it was the French who put up big money to push the technology. Since its first introduction into the market, its main application is for the payphone system. As card manufacturing cost decreases, smart card usage has expanded.

The smart card expected to be used in many applications and especially in personal security related applications such as access control, computer logon, secure email sending and retrieving services. The reason for this growth lies in the smart card's portability and security characteristics. In addition, as the recent growth of palmtop computers shows, people are looking for smaller and smaller devices for carrying their data with them.

Many applications have already been implemented, such as prepayment for services, credit and debit card, loyalty card, and access control card. The most commonly known example is the prepayment services cards, namely, prepaid phone cards, transportation cards and parking cards. Based on the e-purse card, people could perform bank transaction from ATM machines at home or in the bank. With the use of loyalty cards,

companies could store discount information and shopping preferences of their customers. Using these shopping preferences, companies could design new strategies for the users. Access control systems to buildings, computers or other secure areas will soon be handled by a single smart card.

3.2.1 Smart Card – Introduction

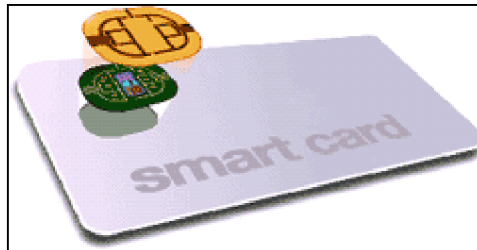


Figure: 3.1 Smart Card

A smart card is a plastic card with an integrated circuit embedded in it, which makes it 'smart'. It provides not only memory capacity, but computational capability as well and thus the chip is capable of processing data. It has gold contacts that allow other devices to communicate with it. This chip holds a variety of information, from stored (monetary) value used for retail and vending machines to secure information and applications for higher-end operations such as medical/healthcare records. New information and applications can be added depending on the chip capabilities. Smart Cards can store several hundred times more data than a conventional card with a magnetic stripe and can be programmed to reveal only the relevant information. For example, it could tell a device in a store that there is sufficient balance in an account to pay for a transaction without revealing the balance amount. The marriage between a convenient plastic card and a microprocessor allows information to be stored, accessed and processed either online or offline. Therefore, unlike the read-

only plastic card, the processing power of Smart Cards gives them the versatility needed to make payments, to configure your cell phones, TVs and video players and to connect to your computers via telephone, satellite or the Internet anytime, anywhere in the world.

- Smart card – Manufacturing

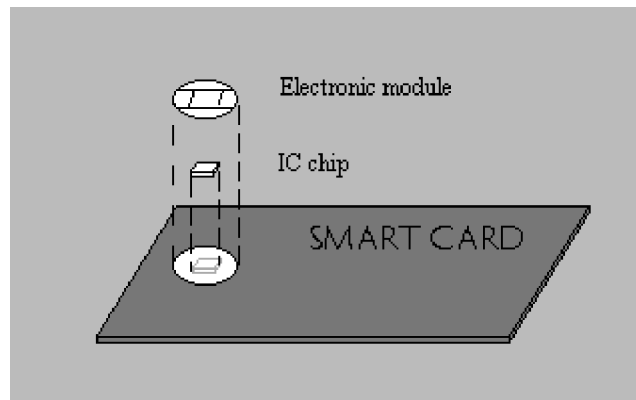


Figure 3.2 Smart Card Manufacturing

Manufacturing a smart card involves much more than just sticking a chip on plastic. The plastic used is usually PVC (Poly Vinyl Chloride), but other substitutes like PC (Poly-Carbonate) is also used. The chip, also known as micro module, (which contains the integrated circuit) is very thin and is embedded into the plastic substrate or card. To do this, a cavity is formed or milled into the plastic card. Then, either a cold or hot glue process bonds the micro module to the card.

3.2.2 Smart Card – Need and Advantages

Smart cards greatly improve the convenience and security of any transaction. They provide tamper-proof storage of user and account identity. Smart cards also provide vital components of system security for the exchange of data throughout virtually any type of network. They protect against a full range of security threats, from careless storage of user passwords to sophisticated system hacks. Multifunction cards can also serve as network system access and store value and other data.

Large storage capacity is one of the advantages in using smart card, but the single-most important feature of smart card consists of the fact that their stored data can be protected against unauthorized access and tampering. Inside a smart card, access to the memory content is controlled by a secure logic circuit within the chip. As access to data can only be performed via a serial interface supervised by the operating system and the secure logic system, confidential data written onto the card is prevented from unauthorized external access. This secret data can only be processed internally by the microprocessor.

Due to the high security level of smart cards and its off-line nature, it is extremely difficult to "hack" the value off a card, or otherwise put unauthorized information on the card. Because it is hard to get the data without authorization, and because it fits in one's pocket, a smart card is uniquely appropriate for

secure and convenient data storage. Without permission of the cardholder, data could not be captured or modified. Therefore, smart card could further enhance the data privacy of citizen.

Smart cards are a point of convergence for public key certificates and associated keys because they:

- Provide tamper-resistant storage for protecting private keys and other forms of personal information.
- Isolate security-critical computations, involving authentication, digital signatures, and key exchange from other parts of the system that don't have a need to know.
- Enable portability of credentials and other private information between computers at work, at home, or on the road.

The key advantages of smart card technology include:

- The capacity provided by the on-board microprocessor and data capacity for highly secure, off-line processing.
- Adherence to international standards, ensuring multiple vendor sources and competitive prices.
- Established track record in real world applications.
- Durability and long expected life span (guaranteed by vendor for up to 10,000 read/writes before failure).
- Chip Operating Systems that support multiple applications and secure independent data storage on one single card.

Therefore, smart card is not only a data store, but also programmable, portable, tamper-resistant memory storage.

People worldwide are now using smart cards for a wide variety of daily tasks, these include:

- Multiple Services on a Single Card

As mentioned earlier, the subscriber realizes maximum value when multiple applications are stored on a single card. A multi-application smart card could provide access to airline reservation and ticketing systems and information networks, as well as a mobile telephone service. Considering the many cards that the average person carries these days (i.e., numerous credit cards, debit cards, employee ID cards), integrating more applications into a single card (or at least fewer cards) has obvious appeal and benefits. It is important to note that there is clear interest on the part other industries to package their services with mobile telephony. For example, research by Citibank indicates clearly that a substantial percentage of the company's customers would like to be able to conduct its banking on a variety of platforms, including wireless. Such services are already available using a standardized toolbox for smart-card application creation.

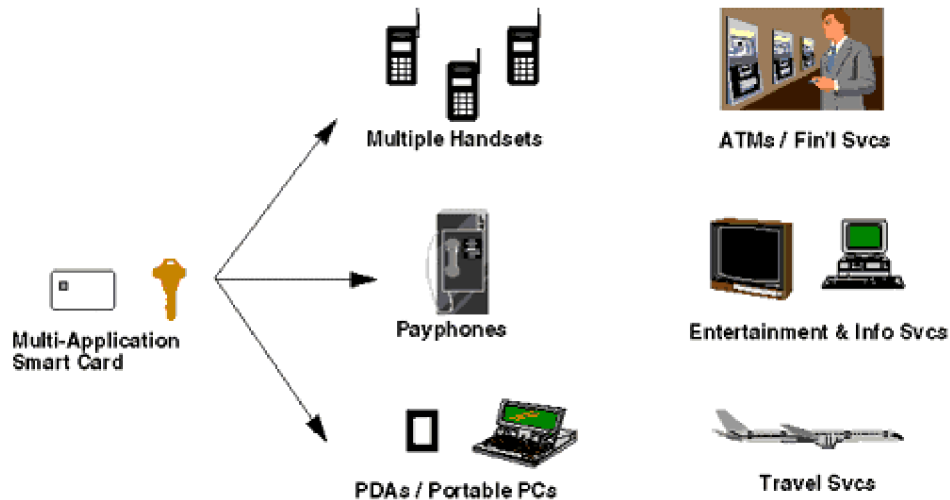


Figure: 3.3 Smart Card—A Key to Information Services

- Loyalty and Stored Value

A primary use of smart cards is stored value, particularly loyalty programs that track and incentives repeat customers. Stored value is more convenient and safer than cash. For issuers, float is realized on unspent balances and residuals on balances that are never used.

For multi-chain retailers that administer loyalty programs across many different businesses and Point of sale systems, smart cards can centrally locate and track all data. The applications are numerous, from parking and laundry to gaming, as well as all retail and entertainment uses.

- Securing Information and Physical Assets

In addition to information security, smart cards achieve greater physical security of services and equipment, because the card

restricts access to all but the authorized user(s). E-mail and PCs are being locked-down with smart cards. Information and entertainment is being delivered via to the home or PC. Home delivery of service is encrypted and decrypted per subscriber access. Digital video broadcasts accept smart cards as electronic keys for protection. Smart cards can also act as keys to machine settings for sensitive laboratory equipment and dispensers for drugs, tools, library cards, health club equipment etc.

- E-Commerce

E-commerce means different things to different people. Some people, for example, limit the meaning of e-commerce to commerce conducted over the Internet and the Web. For the purposes of this chapter, we're going to use the term more widely. So, by e-commerce, we mean everything from electronic business-to-business traffic (for example, Electronic Data Interchange), through Internet-based systems, to any system in which money is represented as bits. Under this admittedly overly broad definition, some aspect of e-commerce touches almost the entire economy. We're intentionally invoking this broad definition to emphasize the utility of smart cards for transacting business.

Smart cards are seemingly an excellent medium for carrying password-protected personal data. Private information such as medical records or secret crypto keys can be stored on a card in a form accessible only to the card carrier (or at least

someone who knows the right secrets). In addition, smart cards can store value. Card carriers can decide with whom to share data and with whom to transact business and use their cards only with those vendors they choose to trust.

The most common form of smart card for commerce is the register-based, stored-value card. Somewhat ironically, one of the most unfortunate consequences of this kind of smart card is that secret keys on the card are known only to the issuing bank and must remain secret from the owner. If the card owner can somehow retrieve a secret key, then he or she can mint electronic cash. In light of the physical attacks sketched earlier in the chapter, this is a serious problem.

Multiple-application smart cards like the Java Card should directly impact the marketability of smart card technology for e-commerce. When a single card can replace the many cards most consumers carry around today, people are likely to want it. Imagine a single card that both holds personal information (such as driver's license, social security, medical information, auto insurance, voter registration, workplace ID, Web site passwords, keys for making digital signatures and encrypting data) and also provides multiple functions (working as a phone card, a charge card for a store, a video rental credit tracker, a credit card, a debit card, and an electronic cash repository).

Leading Web vendors like Netscape are developing APIs for smart card interfaces. The idea is to use a smart card to store cryptographic data for use with existing protocols such as SSL. This will allow Netscape users to interact over the Web with a

well-understood (and widely accepted) protocol. Microsoft is also building smart card interfaces into its products.

The first use of smart cards for e-commerce is likely to be as a key/identity repository. In this case, smart cards act as highly portable hardware tokens that can be uniquely identified. Smart cards can store personal digital certificates for use with the SET protocol and other authentication-based protocols. This could make it possible to carry out Web-based commerce on Internet kiosk systems of the sort occasionally found in airports and coffee shops.

Smart cards make it easy for consumers to securely store information and cash for purchasing. The advantages they offer consumers are:

- The card can carry personal account, credit and buying preference information that can be accessed with a mouse click instead of filling out forms.
- Cards can manage and control expenditures with automatic limits and reporting.
- Internet loyalty programs can be deployed across multiple vendors with disparate POS systems and the card acts as a secure central depository for points or rewards.
- Micro Payments - paying nominal costs without transaction fees associated with credit cards or for amounts too small for cash, like reprint charges.

- Personal Finance

As banks enter competition in newly opened markets such as investment brokerages, they are securing transactions via smart cards at an increased rate. This means:

- Smart cards increase trust through improved security. Two-Factor Authentication insures protection of data and value across the Internet. Threats such as the "Man in the middle" and "Trojan Horses" that replay a user name and password are eliminated
- This will improve customer service. Customers can use secure smart cards for fast, 24-hour electronic funds transfers over the internet
- Costs are reduced: transactions that normally would require a bank employee's time and paperwork can be managed electronically by the customer with a smart card.

- Health Care

The explosion of health care data brings up new challenges to the efficiency of patient care and privacy safeguards. Smart cards solve both challenges with secure storage and distribution of everything from emergency data to benefits status.

- Rapid identification of patients; improved treatment

- A convenient way to carry data between systems or to sites without systems
- Reduction of records maintenance costs
- Network Security

Business to business Intranets and Virtual Private Networks “VPNs” are enhanced by the use of smart cards. Users can be authenticated and authorized to have access to specific information based on preset privileges. Additional applications range from secure email to electronic commerce.

- Physical Access

Businesses and universities of all types need simple identity cards for all employees and students. Most of these people are also granted access to certain data, equipment and departments according to their status. Multifunction, microprocessor-based smart cards incorporate identity with access privileges and also store value for use in various locations, such as cafeterias and stores.

3.2.3 Types of Smart Card

The term Smart Card is loosely used to describe any card with a capability to relate information to a particular application such as magnetic stripe, optical, memory, and microprocessor cards. It is more precise, however to refer to memory and microprocessor cards as smart cards.

- A magnetic stripe card has a strip of magnetic tape material attached to its surface. This is the standard technology used for bank cards.
- Optical cards are bank card-size, plastic cards that use some form of laser to write and read the card.
- Memory cards can store a variety of data, including financial, personal, and specialized information; but cannot process information.

Smart cards with a microprocessor look like standard plastic cards, but are equipped with an embedded Integrated Circuit (IC) chip. Microprocessor cards can store information, carry out local processing on the data stored, and perform complex calculations. These cards take the form of either "contact" cards, which require a card reader, or "contact less" cards which use radio frequency signals to operate.

Microprocessor based Smart cards are defined according to

- a) How the card data is read and written
- b) The type of chip implanted within the card and its capabilities.

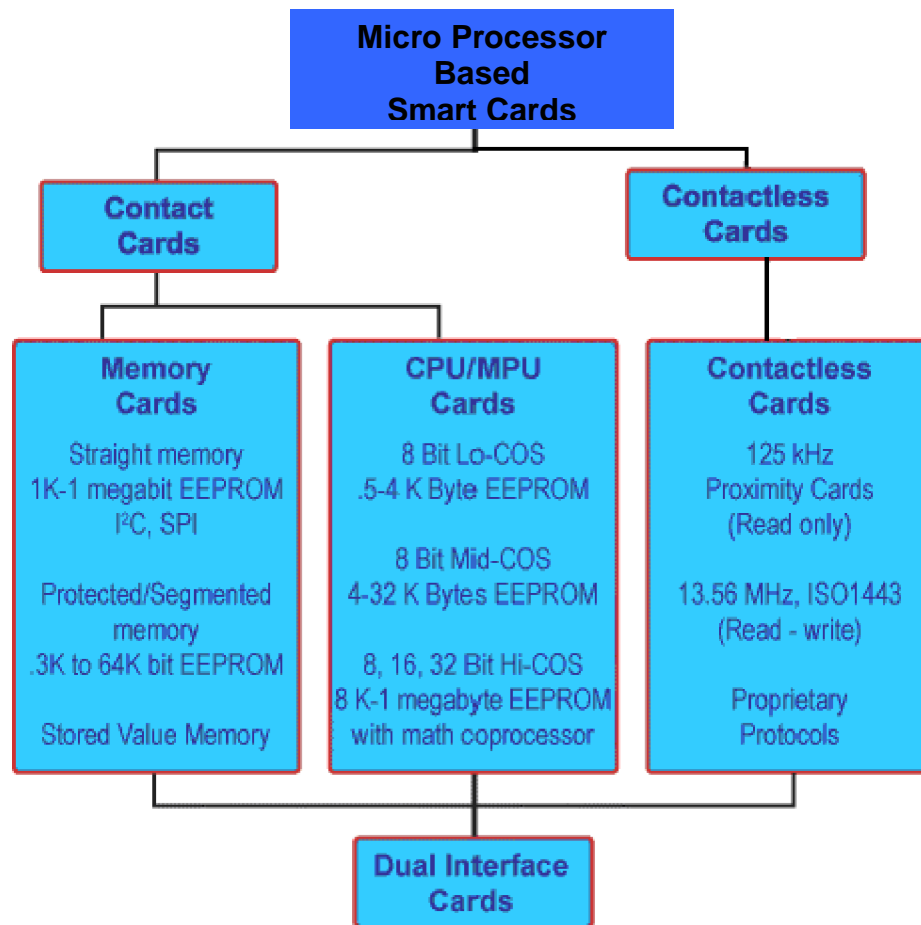


Figure: 3.4 Microprocessor based Smart Card Types

3.2.3.1 Contact Cards

It is the most common type of smart card. Electrical contacts located on the outside of the card connect to a card reader when the card is inserted.

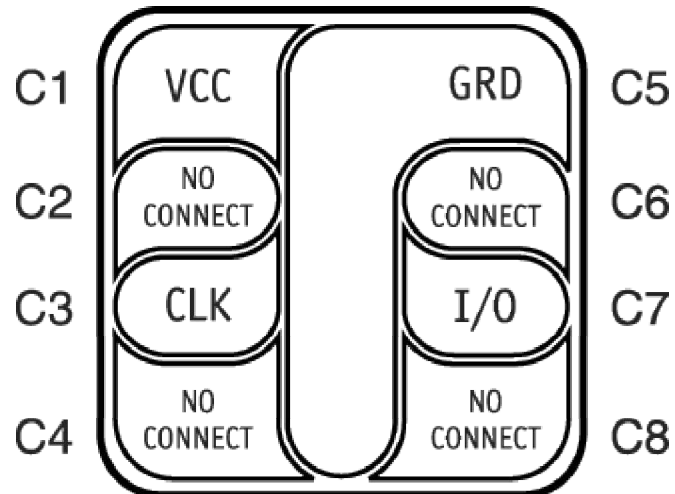
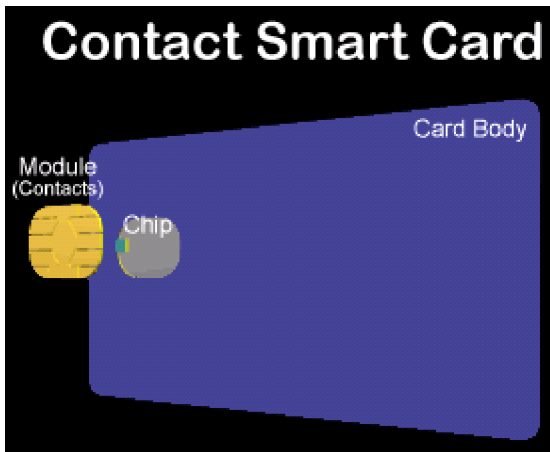


Figure: 3.5 Contact Cards

Increased levels of processing power, flexibility and memory add cost. Single function cards are often the most cost-effective solution. Choose the right type of smart card for an application by evaluating cost versus functionality and determine the required level of security. All of these variables should be weighted against the expected lifecycle of the card.

- Memory Cards

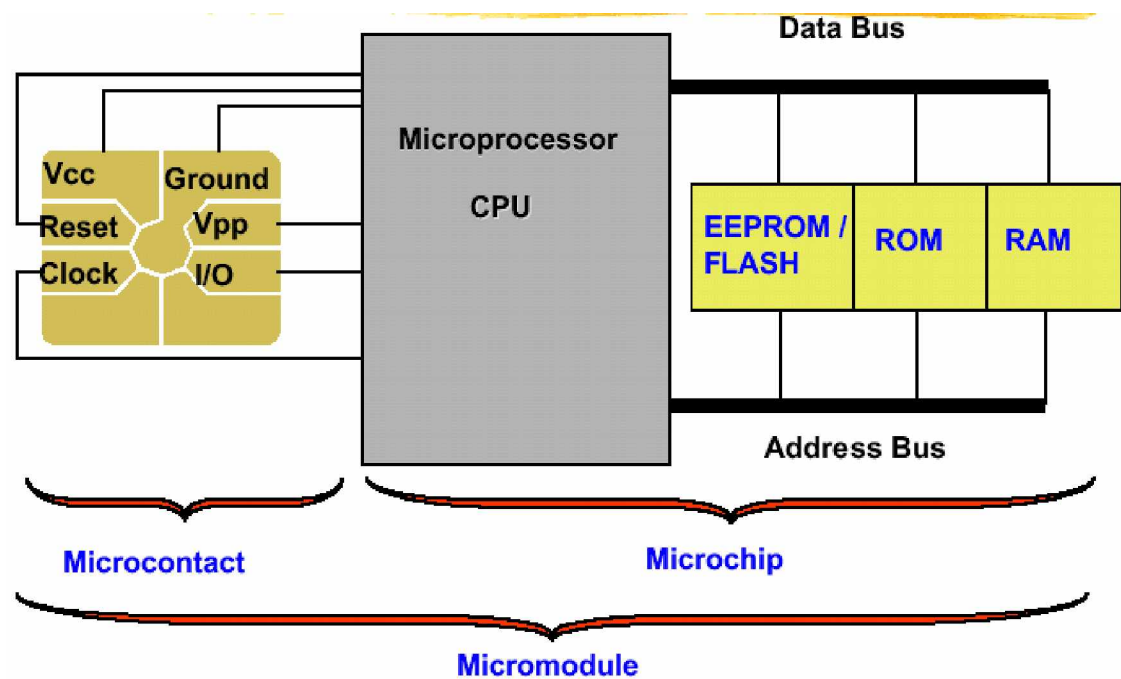


Figure: 3.6 Memory Architecture in Card

Memory cards have no sophisticated processing power and cannot manage files dynamically. All memory cards communicate to readers through synchronous protocols. In all

memory cards we can read and write to a fixed address on the card.

There are three primary types of memory cards:

- a. Straight
- b. Protected
- c. Stored Value

a. Straight Memory Cards

These cards just store data and have no data processing capabilities. These cards are the lowest cost per bit for user memory. They should be regarded as floppy disks of varying sizes without the lock mechanism. These cards cannot identify themselves to the reader, so the host system has to know what type of card is being inserted into a reader. These cards are easily duplicated and cannot be tracked by on-card identifiers.

b. Protected / Segmented Memory Cards

These cards have built-in logic to control the access to the memory of the card. Sometimes referred to as Intelligent Memory cards, these devices can be set to write protect some or all of the memory array. Some of these cards can be configured to restrict access to both reading and writing. This is usually done through a password or system key. Segmented memory cards can be divided into logical sections for planned multi-functionality. These cards are not easily duplicated but

can possibly be impersonated by hackers. An on-card identifier typically can track them.

c. Stored Value Memory Cards

These cards are designed for the specific purpose of storing value or tokens. The cards are either disposable or rechargeable. Most cards of this type incorporate permanent security measures at the point of manufacture. These measures can include password keys and logic that are hard-coded into the chip by the manufacturer. The memory arrays on these devices are set-up as decrements or counters. There is little or no memory left for any other function. For simple applications such as a telephone card the chip has 60 or 12 memory cells, one for each telephone unit. A memory cell is cleared each time a telephone unit is used. Once all the memory units are used, the card becomes useless and is thrown away. This process can be reversed in the case of rechargeable cards.

- CPU/MPU Microprocessor Multifunction Cards

These cards have on-card dynamic data processing capabilities. Multifunction smart cards allocate card memory into independent sections or files assigned to a specific function or application. Within the card is a microprocessor or micro controller chip that manages this memory allocation and file access. This type of chip is similar to those found inside all personal computers and when implanted in a smart card, manages data in organized file structures, via a card operating

system. Unlike other operating systems, this software controls access to the on-card user memory. This capability permits different and multiple functions and/or different applications to reside on the card, allowing businesses to issue and maintain a diversity of 'products' through the card. One example of this is a debit card that also enables building access on a college campus.

Multifunction cards benefit issuers by enabling them to market their products and services via state-of-the-art transaction and encryption technology. Specifically, the technology enables secure identification of users and permits information updates without replacement of the installed base of cards, simplifying program changes and reducing costs. For the card user, multifunction means greater convenience and security, and ultimately, consolidation of multiple cards down to a select few that serve many purposes.

There are many configurations of chips in this category including chips that support cryptographic PKI functions with on board math co-processors or Java virtual machine hardware blocks. As a rule of thumb - the more functions the higher the cost.

3.2.3.2 Contactless Cards

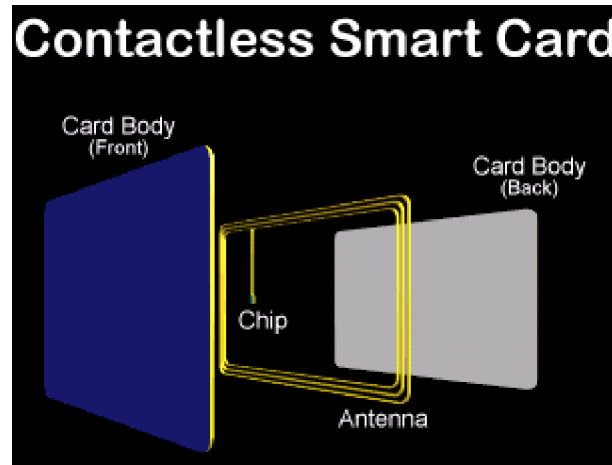


Figure: 3.7 Contactless Smart Card

These are smart cards that employ a radio frequency (RFID) between card and reader without physical insertion of the card. Instead the card is passed along the exterior of the reader and read. Types include proximity cards, which are implemented as a read-only technology for building access. These cards function with a limited memory and communicate at 125 MHz. True read & write contact less cards were first used in transportation for quick decrementing and re-loading of fare values where their lower security was not an issue. They communicate at 13.56 MHz, and conform to the ISO14443 standard. These cards are often straight memory types. They are also gaining popularity in retail stored value, since they can speed-up transactions and not lower transaction processing

revenues (i.e. VISA and MasterCard), like traditional smart cards.

Variations of the ISO14443 specification include A, B, and C, which specify chips from either specific or various manufacturers. A=Philips B=everybody else and C=Sony chips. Contact less card drawbacks include the limits of cryptographic functions and user memory versus microprocessor cards and the limited distance between card and reader required for operation.

- Prox Cards

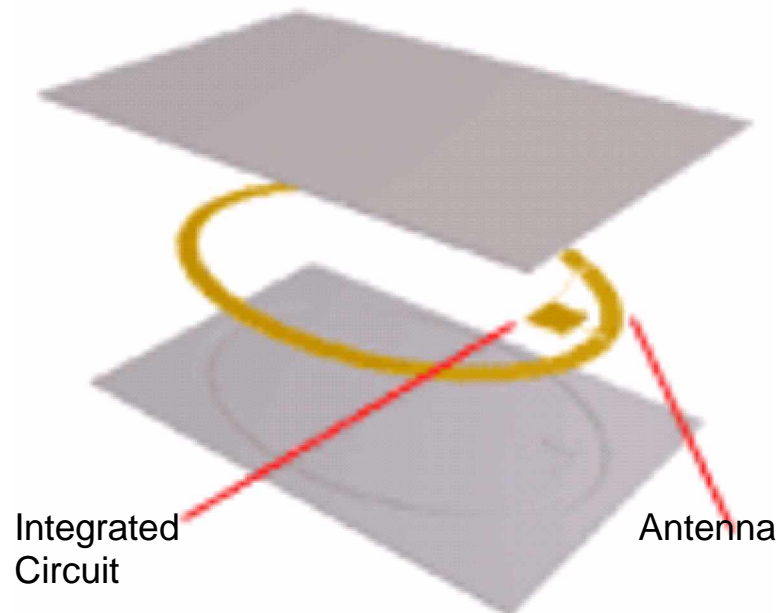


Figure: 3.8 Prox Cards

In addition to the features and functions found in contact smart cards, contact less smart cards contain an embedded antenna instead of contact pads attached to the chip for reading and

writing information contained in the chip's memory. Contactless cards do not have to be inserted into a card acceptor device. Instead, they need only be passed within range of a radio frequency acceptor to read and store information in the chip. The range of operation is typically from about 2.5" to 3.9" (63.5 mm to 99.06 mm) depending on the acceptor.

Contactless smart cards are used in many of the same applications as contact smart cards, especially where the added convenience and speed of not having to insert the card into a reader is desirable. There is a growing acceptance of this type of card for both physical and logical access control applications. Student identification, electronic passport, vending, parking and tolls are common applications for Contactless cards.

- Hybrid Cards

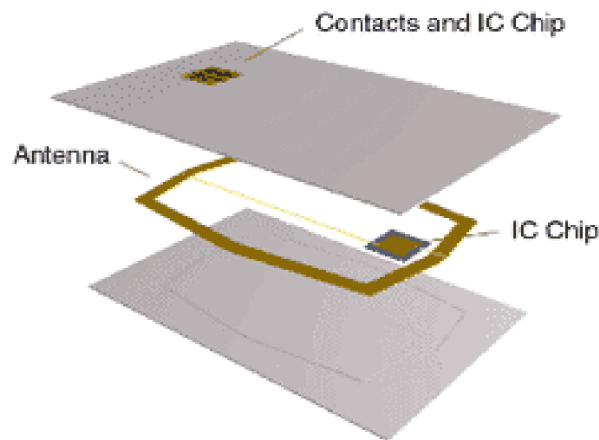


Figure: 3.9 Hybrid Cards

Hybrid card is the term given to e-cards that contain two or more embedded chip technologies such as a Contactless smart chip with its antenna, a contact smart chip with its contact

pads, and/or a proximity chip with its antenna - all in a single card. The Contactless chip is typically used for applications demanding fast transaction times, such as mass transit. The contact chip can be used in applications requiring higher levels of security. The individual electronic components are not connected to each other even though they share space in a single card.

This e-card allows user to accommodate the infrastructure and card technology of a legacy system while adding new applications and e-card technologies - all in a single ID card.

3.2.3.3 Combination Cards

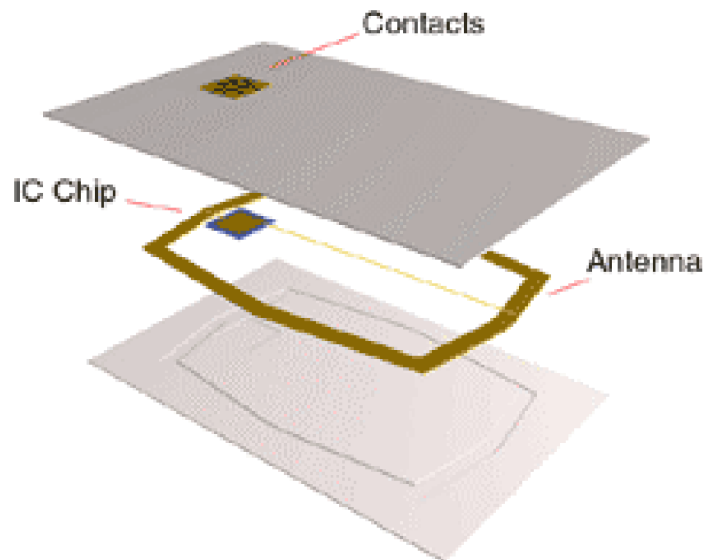


Figure: 3.10 Combi Cards

Contact and Contactless smart cards are using two different communication protocols and development processes. Both

cards have their advantages and disadvantages. Contact smart cards have higher level of security and readily available infrastructure, while Contactless smart cards provide a more efficient and convenient transaction environment. In order to provide customers with the advantages of these two cards, two methods could be employed. The first method is to build a hybrid card reader, which could understand the protocols of both types of cards. The second method is to create a card that combines the contact functions with the Contactless functions. Because the manufacturing cost of the hybrid reader is very expensive, the later solution is usually chosen.

In the hybrid card, the contact IC chip and Contactless chip are separate modules. No electrical connections have been included for communications between the two chips. These two modules can be considered as separate but co-existing chips on the same card. While in the combi card, the contact and Contactless chips could communicate between themselves, thus giving the combi card the capability to talk with external environment via either the contact or Contactless method.

As the combi cards possess the advantages of both contact and Contactless cards, the only reason that is hindering its acceptance is cost. When the cost and technical obstacles are overcome, combi cards will become a popular smart card solution.

3.2.4 Smart Card Operating Systems

Every smart card has an operating system. It is the hardware-specific firmware that provides basic functionality as secure access to on-card storage, authentication and encryption. Only a few cards allow writing programs that are loaded onto the smart card - just like programs on a computer. This is a great way to extend the basic functionality of the smart card OS.

Until the emergence of multi-application smart cards, each software application representing a product or service on a card was written for a card specific operating system, which in turn was particular to a hardware (chip) or silicon platform supplier. In most cases there wasn't even an operating system between the hardware layer and the card edge.

The two primary types of smart card operating systems

- a. Fixed File Structure and
- b. Dynamic Application System

As with card types, selection of a card OS depends on the application the card is developed for. The other defining difference is in the Encryption Capabilities of the OS and the Chip. Symmetric Key and Public Key typically distinguish these. See the security section of this site for more information.

a) Fixed File Structure

This type treats the card as a secure computing and storage device. The issuer sets files and permissions in advance. These specific parameters are ideal and economical for a fixed type of card structure and functions that will not change in the near future. An example of this kind of card is a low-cost employee multi-function badge.

b) Dynamic Application System

This type of operating system, which includes the MULTOS and JAVA card varieties, enables developers to build, test, and deploy different applications securely. Because the OS and applications are more separate, updates can easily and repeatedly be made. An example card is a SIM card for mobile GSM where updates and security are downloaded to the phone and dynamically changed.

Multi-application operating systems allow the development of multiple applications that run on one card. Ideally the on-card applications can't interfere with each other and are protected by a firewall.

3.2.4.1 Java Card OS

JavaCard OS was developed by Sun Microsystems and then promoted to JavaCard Forum. Java Card OS is popular because it gives independence to the programmers over architecture. And Java OS based applications could be used on any vendor of smart card that supports JavaCard OS.

Java Card has changed the smart card proposition for both issuers and cardholders. Java cards provide increased convenience and flexibility for users while delivering savings and a wealth of opportunities for issuers across all business sectors.

Java Card allows applications to be loaded on the fly. This means that a card with the Java Card operating system on it can change features during its lifetime. For example a student, who has been issued a smart card with Java Card on it, can load applications (java applets) over the Internet. Of course this would require the correct authorization. But the interesting part is that this can happen securely over insecure networks. This way the student can change the set of available applications over the smartcard's lifetime. One day it could contain an electronic purse and a metro travel application. The next day the student will add an electronic key to get logical access the university network. This is extremely beneficial for both, the cardholder and the card issuer.

3.2.4.2 MULTOS

This multi-application operating system for smart cards for highest security needs. MULTOS is the first, open, high security, multi-application operating system for smart cards (hence 'MULT-OS'). The beauty of this system is that diverse parties can develop applications that are running on the same card and they all co-reside both independently and securely. This way applications from various vendors can be combined, all securely separated from each other.

The open nature of the MULTOS platform allows anyone to issue cards, write applications, implement the operating system on a specific chip, manufacture smart cards or provide value added products, which support MULTOS.

The MULTOS OS defines a secure environment for smart card applications, the MULTOS Virtual Machine. It also defines an Application Programming Interface for on-card applications to provide access to low-level smart card functions such as cryptography and inter-application communications. The API also provides terminals and other Interface Devices (IFD) mechanisms for loading, deleting and executing on-card applications. The specification includes requirements for the security of the micro-controllers and the safe implementation of cryptography as well as requirements for security assurance of the highest level achievable.

3.2.5 Smart Card Readers/Terminals

"The term 'reader' is used to describe a unit that interfaces with a PC for the majority of its processing requirements. In contrast a 'terminal' is a self-contained processing device."

Both readers and terminals read and write to smart cards. Readers come in many form factors and in a wide variety of capabilities. The easiest way to describe a reader is by the method of its interface to a PC. Smart card readers are available that interface to RS232 serial ports, USB ports, PCMCIA slots, floppy disk slots, parallel ports, infrared IRDA ports and keyboards and keyboard wedge readers.

Another difference in reader types is the on-board intelligence and capabilities. Extensive price and performance differences exist between an industrial strength intelligent reader that supports a wide variety of card protocols and a home style win-card reader that only works with microprocessor cards and performs all processing of the data in the PC.

The options in terminal choices are just as wide. Most units have their own operating systems and development tools. They typically support other functions such as magnetic-stripe reading, modem functions and transaction printing.

3.2.6 Smart Card Standards

Standardization in smart cards technologies are required to make sure that cards and card-accepting devices are made to identical specifications. This ensured that a device in another part of the world could acknowledge cards manufactured in one part of the world.

Over the past several years, industry groups implementing smart cards have developed a number of standards and specifications. These standards are voluntary, but are generally adhered to in the interest of achieving conformity and interoperability. Organizations implementing smart card-based systems should review the standards and specifications that are relevant to the applications being implemented and determine where compliance is needed.

Smart card usage and system design standards should significantly enhance the ability to achieve the following:

- Providing a clear and concise definition of terms so that all agencies have a common understanding and common criteria for evaluation.
- Providing the standards and specifications that are required for a trusted multi-agency credential and for credential information to be used across a defined infrastructure.
- Driving requirements and recognition of the total cost of ownership of a complete ID system architecture.

- Allowing convergence of disparate identity and authentication media (e.g., cards) to a common credential token that can be used and trusted across the defined enterprise.
- Providing the flexibility to meet additional agency needs to use legacy tokens, as well as safeguarding the individual's right to privacy.

A brief synopsis of the various smart card standards and specifications is presented below to illustrate the progress that has been made in standardizing smart card technology and usage. Additional information can be found in the body of work referenced with each smart card standard or specification.

3.2.6.1 ISO – Standards

ISO stands for International Standards Organization. This organization facilitates the creation of voluntary standards through a process that is open to all parties. ISO 7816 is the international standard for integrated-circuit cards (commonly known as smart cards) that use electrical contacts on the card, as well as cards that communicate with readers and terminals without contacts, as with radio frequency (RF/Contactless) technology.

3.2.6.2 FIPS (Federal Information Processing Standards)

Developed by the Computer Security Division within National Institute of Standards and Technology (NIST), USA. FIPS standards are designed to protect federal assets including computer and telecommunications systems. The following FIPS standards apply to smart card technology and pertain to digital signature standards, advanced encryption standards, and security requirements for cryptographic modules.

- FIPS 140 (1-3)

The security requirements contained in FIPS 140 (1-3) pertain to areas related to the secure design and implementation of a cryptographic module, specifically: cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

3.2.6.3 EMV Standards

Europay, MasterCard and Visa formed EMV Company, LLC and created the "Integrated Circuit Card Specifications for Payment Systems". These specifications are related to ISO7816 and

create a common technical basis for card and system implementation of a stored value system. Integrated Circuit Card Specifications for Payment Systems can be obtained from a Visa, MasterCard or Euro pay member bank.

3.2.6.4 PC/SC Standards

A Microsoft proposed and implemented standard for cards and readers, called the PC/SC specification. This proposal only applies to CPU cards. They have also built into their CryptoAPI a framework that supports many security mechanisms for cards and systems. PC/SC is now a fairly common middleware interface for PC logon applications. The standard is a highly abstracted set of middleware components that allow for the most common reader card interactions.

3.2.6.5 CEN

Committee of European for Normalization and ETSI (European Telecommunications Standards Institute) is focused on telecommunications, as with the GSM SIM for cellular telephones. GSM 11.11 and ETSI300045.

3.3.6.6 HIPAA

The Health Insurance Portability and Accountability Act adopts national standards for implementing a secure electronic health transaction system in the U.S. Example transactions affected

by this include claims, enrollment, eligibility, payment and coordination of benefits. Smart cards are governed by the requirements of HIPAA pertaining to data security and patient privacy.

3.2.7 Smart Card Security

Smart cards provide computing and business systems the enormous benefit of portable and secure storage of data and value. At the same time, the integration of smart cards into the system introduces its own security management issues, as people access card data far and wide in a variety of applications.

- Data Integrity

This is the function that verifies the characteristics of a document and a transaction. Characteristics of both are inspected and confirmed for content and correct authorization.

Data Integrity is achieved with electronic cryptography that assigns a unique identity to data like a fingerprint. Any attempt to change this identity signals the change and flags any tampering.

- Authentication

This inspects, and then confirms, the proper identity of people involved in a transaction of data or value. In authentication systems, authentication is measured by assessing the mechanisms strength and how many factors are used to confirm the identity. In a PKI system a Digital Signature verifies data at its origination by producing an identity that can be mutually verified by all parties involved in the transaction. A cryptographic hash algorithm produces a Digital Signature.

- Non-Repudiation

This eliminates the possibility of a transaction being repudiated, or invalidated by incorporating a Digital Signature that a third party can verify as correct. Similar in concept to registered mail, the recipient of data re-hashes it, verifies the Digital Signature, and compares the two to see that they match.

- Authorization and Delegation

Authorization is the processes of allowing access to specific data within a system. Delegation is the utilization of a third party to manage and certify each of the users of the system (Certificate Authorities).

- Auditing and Logging

This is the independent examination and recording of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

- Management

Is the oversight and design of the elements and mechanisms discussed above and below. Card management also requires the management of card issuance; replacement and retirement as well as policies that govern a system.

- Cryptography/Confidentiality

Confidentiality is the use of encryption to protect information from unauthorized disclosure. Plain text is turned into cipher text via an algorithm, and then decrypted back into plain text using the same method.

Cryptography is the method of converting data from a human readable form to a modified form, and then backs to its original readable form, to make unauthorized access difficult. Cryptography is used in the following ways:

- Ensure data privacy, by encrypting data
- Ensures data integrity, by recognizing if data has been manipulated in an unauthorized way

- Ensures data uniqueness by checking that data is "original", and not a "copy" of the "original". The sender attaches a unique identifier to the "original" data. The receiver of the data then checks this unique identifier.

The original data may be in a human-readable form, such as a text file, or it may be in a computer-readable form, such as a database, spreadsheet or graphics file. The original data is called unencrypted data or plain text. The modified data is called encrypted data or cipher text. The process of converting the unencrypted data is called encryption. The process of converting encrypted data to unencrypted data is called decryption.

As the card issuer, we must define all of the parameters for card and data security.

There are two methods of using cards for data system security,

- a) Host-based and
- b) Card-based.

a) Host-Based System Security

A host-based system treats a card as a simple data carrier. Because of this, straight memory cards can be used very cost-effectively for many systems. All protection of the data is done from the host computer. The card data may be encrypted but the transmission to the host can be vulnerable to attack. A

common method of increasing the security is to write in the clear (not encrypted) a key that usually contains a date and/or time along with a secret reference to a set of keys on the host. Each time the card is re-written the host can write a reference to the keys.

This way each transmission is different. But parts of the keys are in the clear for hackers to analyze. This security can be increased by the use of smart memory cards that employ a password mechanism to prevent unauthorized reading of the data. Unfortunately the passwords can be sniffed in the clear. Access is then possible to the main memory.

These methodologies are often used when a network can batch up the data regularly and compare values and card usage and generate a problem card list.

b) Card-Based System Security

These systems are typically microprocessor card-based. A card, or token-based system treats a card as an active computing device. The Interaction between the host and the card can be a series of steps to determine if the card is authorized to be used in the system. The process also checks if the user can be identified, authenticated and if the card will present the appropriate credentials to conduct a transaction. The card itself can also demand the same from the host before proceeding with a transaction.

3.3 Smart Card as a unique identity Citizen Card

In present there are many cards or identity/address proofs with citizen given by our state/central government Ration Card, Election Photo I-Card, Passport, Driving License, PAN Card.

We can deploy all this proofs in to one Smart Card. For that we have to choose a smart card with maximum storage capacity. Which can store all the identity proofs including citizens fingerprint image. The probable design of Unique Identity Smart Citizen Card can be made as under:

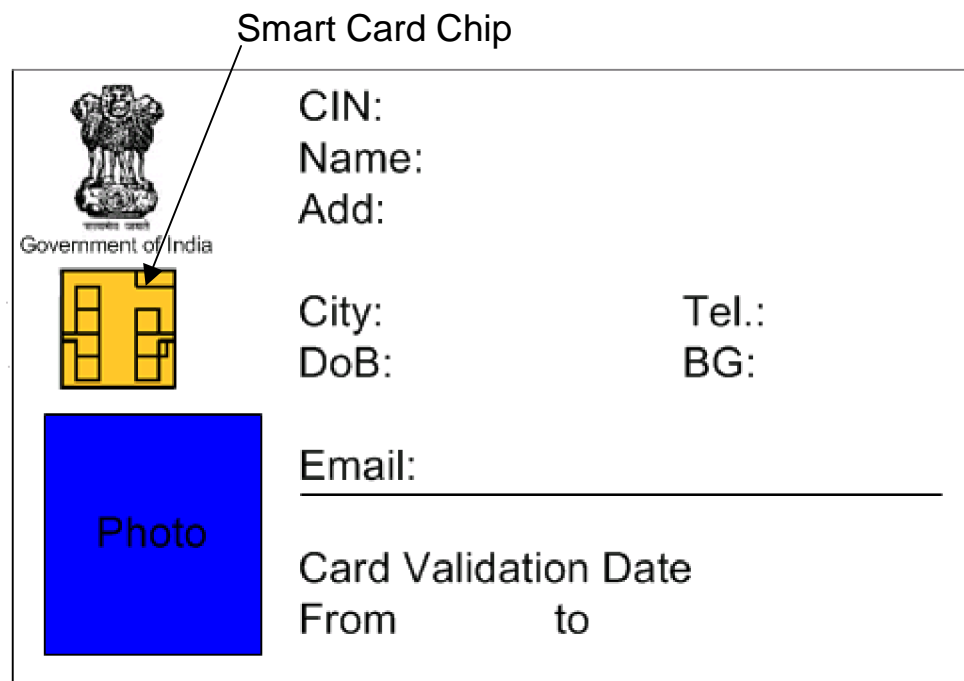


Figure: 3.11 Front Side View of Smart Citizen Card

Where:

CIN = Citizen Identity Number

DoB = Date of Birth

BG = Blood Group

License Detail :
PAN Detail :
Service / Business Detail (Optional)

Figure: 3.12 Back Side View of Smart Citizen Card

Where:

PAN: Personal Account Number

Citizen can use this smart card in any government office or in any governmental process as his/her unique identity and proof. But there may be main drawback of this card that it might be produced illegally for duplication purpose. This threat can be removed by biometric authentication. Because of biometric authentication can never be produced illegally, so at every government office, government can authenticate a citizen with his/her unique biometric identity that is stored in central server.

Main use of biometric authentication will be in election process so that very secure elections can be made.

3.4 Central Database for the card

The card is to act as a personal profile for the citizen as well for the government. Therefore the record of every citizen must be stored at central level. Then the entire database can be distributed online to related departments like police, income tax, banks etc.

3.4.1 Citizen Identity Number (CIN)

The Citizen Card to be issued to a Citizen must contain unique number called CIN (Citizen Identity Number).

The format of the number can be as follow:

First six digits of the

Pin code of the city/village* : 360005

Last nine digits as per the card issue no : 000000001

Which makes up a

Citizen Identity Number (CIN) : 3600051000000001

* If any village doesn't have pin code then its relative taluka's pin code can be used to generate the CIN.

3.4.2 Database design for the Citizen Card

The central database for the Citizen Card could be designed to store the following details of citizen

- Citizen Identity Number (CIN)
- Citizen's Full Name
- Citizen's Full Address including City, Pincode, Taluka, District and State
- Citizen's Date of Birth
- Citizen's Phone
- Citizen's Mobile
- Citizen's Email – Id
- Citizen's Blood Group
- Citizen's Sex Identity
- Citizen's photo image

Government can be suggested to launch a web portal for citizen as well as its various departments. The portal like www.indiancitizen.gov.in should have web presence and from this portal government can provide email-id for every citizen. The email-id for a citizen will include CIN & form email-id as CIN@indiancitizen.gov.in.

Through this portal government can provide the necessary information to related departments, banks or private sector to get information about a particular citizen.

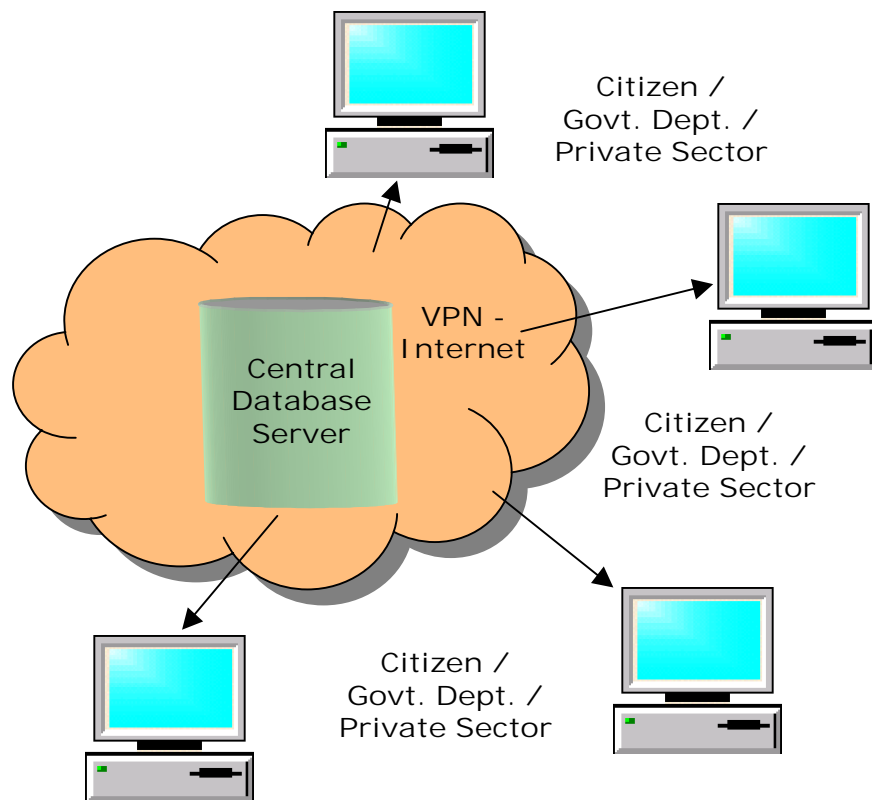


Figure: 3.13 Accessibility of information

The process of integration with the development of the system for Citizen Card, Some issues are of concerns.

- Passport offices, Airline, Railway etc must intimate the CIN to the Government.
- All FIRs in the Police Stations and all accused of the Courts must contain CIN.
- All Hotels must verify and quote the CIN before allowing entry in the Hotels.

- The retailers/ banks must ask the customers to quote the CIN if the transaction is above a specified value.
- The CIN of all tax/ bank loan defaulters must be shared by the law enforcement agencies.

All the government departments / private sectors are to be advised to design (or alter the existing) their databases with according to CIN to make the system more flexible.

Every governmental office can be provided limited server access for a particular transaction with citizen. For example R.T.O. can only access the server to alter the portion of the database record related to citizen's driving license.

Footnote Reference:

- www.smartcardalliance.org
- www.smartcardforum.org
- www.cardtechnology.com
- www.pcquest.com
- www.bioenabletech.com
- www.itl.nist.gov
- www.javacardforum.org

Chapter – 4

Integration of Biometric Technology with Smart Card

- 4.1 Biometric Technologies – an Overview
- 4.2 Biometrics in Model Identification Systems
- 4.3 Fingerprint based Identification System
- 4.4 Identification System with Integration of Fingerprint and Smart card

4.1 Biometric Technologies – an Overview

Primitive biometrics such as height, special body marks had been in use to identify people since the time of the ancient Egyptians. Fingerprints have been used for many years by police departments for criminal identification around the world. With the current ever improving biometrics technology has opened a window of possibilities. Today, biometric technology is not only being used for access to high security areas, but also for network security.

Biometrics refers to the automatic identification of a person based on his/her physiological or behavioral characteristics. This method of identification is preferred over traditional methods involving passwords and PIN numbers for various reasons:

- (a) The person to be identified is required to be physically present at the point-of-identification.
- (b) Identification based on biometric techniques obviates the need to remember a password or carry a token.

With the increased use of computers as vehicles of information technology, it is necessary to restrict access to sensitive/personal data. By replacing PINs (Personal Identification Number), biometric techniques can potentially prevent unauthorized access to or fraudulent use of ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. PINs and passwords may be forgotten, and token-based methods of identification like passports and

driving licenses may be forged, stolen, or lost. That is why biometric based systems of identification are receiving considerable interest. Various types of biometric systems are being used for identification in real time mode.

A biometric technology is essentially a pattern recognition system, which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. An important issue in designing a practically working system is to determine how an individual is identified. Depending on the context, a biometric system can be either a verification (authentication) system or an identification system.

- Access Control

Biometrics has proven to be an effective solution for high-security access control, ensuring that only authorized individuals can access protected or secure areas. Biometric systems require controlled and accurate enrollment processes, careful monitoring of security settings to ensure that the risk of unauthorized entry is low and well-designed interfaces to ensure rapid acquisition and matching. Poor system design and implementation can slow down the authentication process and can expose new vulnerabilities.

Complex access control installations require independent expertise to ensure that security levels, ingress and egress processes, and system administration capabilities meet

deployed expectations. In access control primary biometric technologies in use are palmprint, fingerprint, and iris-scan.

- IT/Network Security

As more and more valuable information is made accessible to users via LAN and WAN, the risks associated with unauthorized access to sensitive data grow larger. Protecting every network with passwords is not safe, as passwords are easily compromised, lost, or inappropriately shared. Whether driven by security, convenience, or cost-reduction, biometrics is proving to be an effective solution for IT/Network Security. Major challenges in deploying biometrics include accuracy and performance, integrating biometric match decisions with existing systems, interoperability across proprietary technologies, and secure storage and transmission of biometric data.

Biometrics' core capabilities in IT/Network Security include the following:

- Evaluation and testing of leading biometric solutions for IT/Network Security
- Integration of biometric solutions into legacy applications
- Flexible, vendor-independent system design
- Adherence to emerging biometric standards
- Application development
- Multiple device integration

- Encryption of biometric data and match decisions
- Custom reporting and auditing systems
- Specific vendor strengths and weaknesses

Biometrics is being positioned as a solution for e-Commerce and Internet security, designed to ensure that only authorized individuals could access sensitive data or execute transactions. From the perspective of commercial or government institutions, however, building effective e-Commerce and Internet solutions is more complicated than replacing a password dialog with a biometric interface.

Whether authenticating customers, employees, or citizens, we must consider the following factors:

- Providing compatibility across the range of incompatible fingerprint technologies deployed at the desktop level
- Accommodating individuals who cannot enroll or verify successfully, requiring fallback procedures
- Integrating biometric match decisions into payment and clearance systems
- Defining accuracy requirements for biometric systems
- Location of biometric data storage and processing for maximum availability
- Integrating biometric acquisition processes into existing interfaces
- Administrative and auditing functionality to manage biometric accounts and transactions
- Secure transmission of biometric information

- Compatibility with Windows and Unix web servers
- Processes for verifying initial identity claims
- Incorporating iris-scan, voice recognition, and other biometric technologies for account access

4.1.1 Types of Biometrics Technologies

Biometrics are the best defined as measurable physiological and / or behavioral characteristics that can be utilized to verify the identity of an individual. They are of interest in any area where it is important to verify the true identity of an individual. Initially, these techniques were employed primarily in specialist high security applications; however we are now seeing their use and proposed use in a much broader range of public facing situations.

Following are the main types of biometrics

1. Iris/Retinal Scan
2. Vein check
3. Face Recognition
4. Fingerprint Verification
5. Voice Verification
6. Signature Verification

4.1.1.1 Iris/Retinal Scan

There are two main types of iris/retinal scans technology available today.

Iris scanning is undoubtedly the less intrusive of the eye related biometrics. It utilizes a fairly conventional CCD camera element and requires no intimate contact between user and reader. In addition it has the potential for higher than average template matching performance. As a technology it has attracted the attention of various third party integrators and one would expect to see additional products launched in due course as a result. It has been demonstrated to work with spectacles in place and with a variety of ethnic groups and is one of the few devices, which can work well in identification mode. Ease of use and system integration has not traditionally been strong points with the iris scanning devices, but we can expect to see improvements in these areas as new products are introduced.

For retinal scan infrared scanning is necessary. Infrared Scanning requires use of infrared light beams. The eye's inherent isolation and protection from the external environment as an internal organ of the body (as opposed to fingerprint) is a benefit.

The eye's physiological response to light and natural pupillary oscillation prevents substitution of a photograph or some other imitation for living tissue. This reliability of uniqueness ensures

that even (monozygotic) twins have iris patterns as distinct in their mathematical detail as those of unrelated persons.

- Benefits:
 - Low error incidence
 - Employees know that their employers mean business when this type of security is implemented
- Drawbacks:
 - Infrared iris scanning is perceived as intrusive
 - Portability issues arise with remote (laptop) users
 - Video cameras are being used, and employees may fear being 'spied' upon.

4.1.1.2 Vein check

The Vein check principle is a non-invasive, computerized comparison of subcutaneous blood vessel structures (the veins) in the back of a palm to verify the identity of individuals for access control or cardholder ID. Vein check measures the shape and size of veins in the back of the palm. The vein pattern is best defined when the skin on the back of the palm is taut - when the fist is clenched.

The skeleton of the palm then holds the vein "tree" rigid. Non-harmful, near infrared lighting is employed. The vein "tree" pattern is picked up by a video camera, and converted by a computer into a vector pattern or into a string of numbers. This pattern of the vein "tree" is sufficiently idiosyncratic to function as a personal bar code, or PIN equivalent, that is extremely difficult to duplicate or discover.

- Benefits:
 - Non-invasive, socially acceptable alternative to fingerprinting and retinal scanning
 - Fast, easy-to-use, and discreet
 - Very low false reject rate
 - Compact reference pattern (400 bits)
 - Inaccessible to masqueraders
- Drawback:
 - Uses camera equipment, which for now is less portable than other technologies.

4.1.1.3 Face Recognition

Another exciting biometric technology emerging today is planar face recognition. A video or static image is taken of a subject and broken down into facial planes which are unique to an individual. Examples of the applications of face recognition technology include; Computers that will only unlock when they see user's face and will close up when they can no longer see their user, taking pictures of people who come into private work space, terrorist surveillance at airports, time and attendance validation, providing secure access to employee and medical records, locking and unlocking doors.

When a computer recognizes who is looking at it, it is not only able to customize its offerings to the individual but it is able to adapt to the individual voice, gesture and other habits allowing for more effective interaction. This technology can secure a computer from unauthorized access by using faces as user's passwords.

Another face identification technology uses infrared heat scans to identify facial characteristics. Facial thermo gram technology was developed on the demonstrated premise that an infrared camera can capture individual facial heat emission patterns.

- Non-intrusive, can also be used in low light and without light.
- The technology is light independent. An infrared camera can capture facial images in low light or in the absence of light.

- The technology is not vulnerable to disguises. Even plastic surgery, which does not reroute the flow of blood through the veins, cannot penetrate the system.
- The technology delivers greater accuracy, speed and reliability.
- Storage requirements are minimal, since the system only needs a portion of the face for recognition. (2-4KB)

- Benefits:
 - Can recognize when user leaves PC
 - Easy to use
 - Equipment can be used for video conferencing as well as security
 - Uses a 3 dimensional picture and will not accept 2 dimensional substitutes
- Drawback:
 - Constant camera surveillance may intimidate users

4.1.1.4 Fingerprint / Palmprint Verification

There are a variety of approaches to fingerprint verification. Some of them try to emulate the traditional police method of matching minutiae, others are straight pattern matching devices, and some adopt a unique approach all of their own. Some of them can detect when a live finger is presented, some cannot. There are a greater variety of fingerprint devices available than any other biometric at present.

Potentially capable of good accuracy (low instances of false acceptance) fingerprint devices can also suffer from usage errors among insufficiently disciplined users (higher instances of false rejection) such as might be the case with large user bases. One must also consider the transducer / user interface and how this would be affected by large scale usage in a variety of environments. Fingerprint verification may be a good choice for in house systems where adequate explanation and training can be provided to users and where the system is operated within a controlled environment. It is not surprising that the workstation access application area seems to be based almost exclusively around fingerprints, due to the relatively low cost, small size (easily integrated into keyboards) and ease of integration.

As the name suggests, palmprint is concerned with measuring the physical characteristics of the users' palm and fingers, from a three-dimensional perspective in the case of the leading product. One of the most established methodologies; Palmprint

offers a good balance of performance characteristics and is relatively easy to use.

This methodology may be suitable where we have larger user bases or users who may access the system infrequently and may therefore be less disciplined in their approach to the system. Accuracy can be very high if desired, whilst flexible performance tuning and configuration can accommodate a wide range of applications. Palmprint readers are deployed in a wide range of scenarios, including time and attendance recording where they have proved extremely popular. Ease of integration into other systems and processes, coupled to ease of use makes palmprint an obvious first step for many biometric projects.

- Benefits:
 - Non-intrusive and Low level of error rates
 - Fraud deterrent documentation capabilities - May be programmed to capture and record the original print of an unauthorized user. Fraudulent attempts are discouraged for fear of leaving prints at the "scene of the crime".
 - Adjustable precision - The system operator can set the tolerances for the desired level of security. Therefore, appropriate false acceptance and false rejection rates can be achieved for a particular application.

- Drawback:
 - Since fingers experience so much wear and tear from cuts and burns, software must be able to do image rebuilding.

4.1.1.5 Voice Verification

A potentially interesting technique bearing in mind how much voice communication takes place with regard to everyday business transactions. Some designs have concentrated on wall-mounted readers whilst others have sought to integrate voice verification into conventional telephone handsets.

Whilst there have been a number of voice verification products introduced to the market, many of them have suffered in practice due to the variability of both transducers and local acoustics. In addition, the enrolment procedure has often been more complicated than with other biometrics leading to the perception of voice verification as unfriendly in some quarters. However, much work has been and continues to be undertaken in this context and it will be interesting to monitor progress accordingly.

Benefits:

- Low in cost
- Non-intrusive
- Equipment is already built into most PC's and workstations.
- Drawback:
 - Voice pattern fluctuations due to illness, physical exertion, etc. could affect recognition software.

4.1.1.6 Signature Verification

Using Acoustic Emissions, a system can automatically verify signatures by analyzing the acoustic emissions that are generated as a person signs his or her name. This biometric technology captures data from the dynamic process of the movement of a pen tip over the paper. These acoustic emissions are transmitted in the form of stress waves within the material of a writing block beneath the document being signed.

A Signature Verification using acoustic emissions captures data from the dynamic process of writing a signature or some other sample of handwriting. As the user writes on the surface of the paper, the movement of the pen tip over the paper fibers generates acoustic emissions that are transmitted in the form of stress waves within the material of a writing block beneath the document being signed.

The structure-borne elastic waves behave in materials in a similar way to sound waves in air and can be detected by a hidden sensor attached to the writing block. The acoustic-emission sound sequence generated by the signing process constitutes a pattern that is unique to the individual's signing style. The pattern contains extensive information about the way in which the signature was executed.

- Benefits:
 - Fast and easy to use

- Any pen that produces reasonably fine lines can be used
- Easily integrated into existing equipment
- Acceptability in the marketplace (people are already becoming accustomed to using the new credit card signature capture technology).
- Drawback:
 - Lower levels of performance and reliability, possible problems with portability for remote users.

Whichever type of biometric technologies is used, the basic concept of verification remains the same. The characteristic is evaluated and compared with a stored copy in a database or stored on a smart card. Comparison against card-stored or centrally recorded reference patterns can be carried out automatically using software with high-speed algorithms on a standard personal computer. If there is a match, access is granted.

4.2 Biometrics in Model Identification Systems

Biometrics is increasingly integrated into large-scale systems for drivers' licensing, surveillance, health and identity cards, and benefits issuance. The need for singular identification and transactional verification has emerged in various public and private sector environments.

Identification systems based on biometrics are capable of identifying persons on the basis either physical or behavioral characteristics. Currently, there are over ten different techniques available to identify a person based on biometrics. The following technologies are applied within the two main categories

- Behavioral characteristics
 - Voice verification
 - Signature verification
- Physical characteristics
 - Iris recognition
 - Retina recognition
 - Vein recognition
 - Face recognition
 - Fingerprint / Palmprint verification

Identification Systems include the following:

- Smart Card integration
- Interfaces between 1:1 and 1:N systems
- Vendor-neutral system design

- Multiple device integration
- Ensuring accurate enrollment processes
- Integration of biometric systems and decisions into legacy systems
- Privacy-sympathetic system design
- Image processing and optimization
- Encryption of biometric data and match decisions

Identification systems are among the most complex biometric systems, with detailed requirements for acquisition devices, matching algorithms, fallback procedures, and privacy-sympathetic design. At its most simple level, biometric systems operate on a three-step process.

- A sensor takes an observation. The type of sensor and its observation will vary by biometric type. For face recognition, the sensor is usually a camera and the observation is a picture of an individual's face.
- Second, the biometric system develops a way to describe the observation mathematically; a biometric signature. The method will again vary by biometric type, but also from vendor to vendor.
- Third, the computer system inputs the biometric signature into a comparison algorithm and compares it to one or more biometric signatures previously stored in its database. Other system components, or human operator,

then use these result(s) for other actions such as allowing computer access, sounding an alarm, etc.

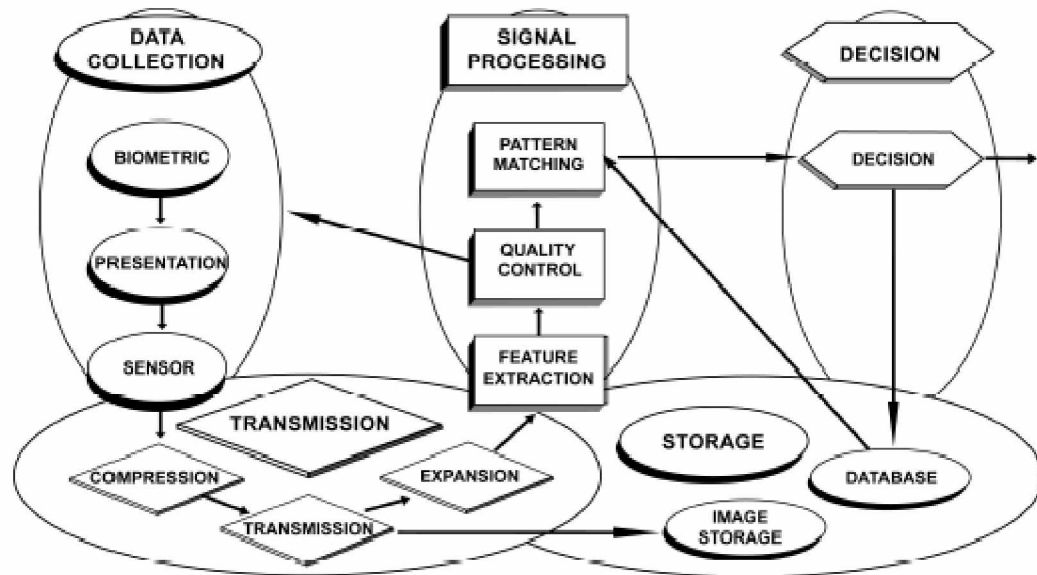


Figure: 4.1 Generic Biometric Systems

Although understanding the three-step biometric process is sufficient for most users, biometric systems are in reality much more complicated.

4.2.1 Verification and Identification

Perhaps the most fundamental distinction in biometrics is between verification and identification. Nearly all aspects of biometric-performance, benefits and risks of deployment, privacy impart, cost- differ when moving between these two types of systems.

Verification systems answer the question, "Am I who I claim to be?" by requiring that a user claim an identity in order for a biometric comparison to be performed. After a user claims an identity, he or she provides biometric data, which is then compared against his or her enrolled biometric data. Depending on the type of biometric system, the identity that a user claims might be a Windows username, a given name, or an ID number; the answer returned by the system is match or no match. Verification systems can contain dozens, thousands, or millions of biometric records, but are always predicated on a user's biometric data being matched against only his or her own enrolled biometric data. Verification is often referred to as 1:1 {one to one}. The process of providing a username and biometric data is referred to as authentication.

Identification systems answer the question, "who am I?" and do not require that a user claim an identity before biometric comparisons take place. The user provides his or her biometric data, which is compared to data from a number of users in order to find a match. The answer returned by the system is an identity such as a name or ID number. Identification is often referred to as 1:N {one-to N or one-to-many}, because a person's biometric information is compared against multiple {N} records.

Within identification systems there is a further distinction between positive and negative. Positive identification systems are designed to find a match for a user's biometric information in a database of biometric information. A typical positive

identification system would be a prison release program where individuals do not enter an ID number or use a card, but provide biometric data and are located within an inmate database. The anticipated result of a search in a positive identification system is a match. Negative identification systems, by contrast, are designed to ensure that a person's biometric information is not present in a database. This prevents people from enrolling twice in a system and is often used in large-scale public benefits programs in which users attempt to enroll multiple times to gain benefits under different names. Although the underlying biometric matching technology may be very similar to that of positive identification, the anticipated result of a search in a negative identification system is a non-match.

Identification systems with more than approximately 100,000 users are considered large-scale identification systems. Large-scale identification systems generally differ substantially from smaller-scale identification systems, especially in accuracy and response time, to the point where they effectively become qualitatively different types of biometric technology. Only certain biometric technologies are capable of performing identification, including finger-scan, iris-scan, retina-scan, and to a lesser degree facial-scan. Signature-scan, voice-scan, and palm-scan are incapable of identification, because the physiological and behavioral characteristics upon which they are based are not sufficient distinctive.

4.2.2 Appropriate need of both Verification and Identification

It is rare that an organization facing a specific problem will find itself deciding whether to deploy identification or a verification system. Instead, certain applications naturally lead themselves to verification, and others require identification. PC and network security generally employ verification systems; access to buildings and rooms can be effective with either identification or verification systems, though verification is predominant; and large-scale public benefits programs generally utilize identification systems, to deploy an effective biometric system, we must understand and be prepared to evaluate the strengths and weaknesses of each system types in relation to business and security needs.

Verification systems are generally faster and more accurate than identification systems. Instead of performing hundreds of comparisons against enrolled users, they need only match a person's data against his or her existing data. This requires less computing power and decreases the likelihood that the system will match an unauthorized user. Nearly all verification systems can render a match/ no-match decision within less than one-second. Verification systems, of course, cannot determine whether a given person is present in a database more than once.

Identification systems require more computational power than verification systems, because more comparisons take place

before a match occurs-in some cases, millions of matches. In addition, there are opportunities for an identification system to err, because many more matches must be conducted. As a rule, identification systems are deployed when verification simply does not make sense {to eliminate duplicate enrollments, for example}. Although the idea of performing identification in desktop environment may be appealing, the association reduction in speed and accuracy generally outweigh these modest benefits of eliminating a username or ID.

4.2.3 Logical versus physical access

Once a biometric system has determined or verified an identity, what happens? The answer depends on the purpose for which the system is deployed. Biometric systems, and in many ways the entire biometric industry, can be segmented according to the purposes for which verification and identification are being performed. The two primary users for a biometric system are physical access and logical access.

Physical access systems monitor, restrict, or grant movement of a person or object into or out of a specific area. Most physical access implementations involve entry into a room or building: bank vaults, server rooms' control towers, or any location to which access is restricted. Time and attendance are a common physical access application, combining access to a location with an audit of when the authentication occurred. Physical access can also entail accessing equipment or material, such as opening a safe or starting an automobile, although most of the applications are still speculation. When used in physical access systems biometrics replace or complement keys, access cards, PIN cords, and security guards.

Logical access systems monitor, restrict, or grant access to data or information. Logging into a PC, accessing data stored on a network, accessing an account, or authenticating a transaction are examples of logical access. Biometrics replaces or complements password, PINs, and tokens in logical access

systems. The core biometric functionality- acquiring and comparing biometric data- is often identical in physical and logical access systems. The same finger-scan algorithm and reader, for example, can be used for both desktop and doorway applications. What changes between the two is the external system into which the biometric functionality is integrated into a larger system {be it a door control system, for example, or an operating system}. The biometric match affects a result such as at the opening of a door or access to an operating system.

Because of the value of information stored on corporate networks and the transaction value of business-to business (B2B) and business-to consumer (B2C) e-commerce. The number of times an individual needs to provide authentication to a PC in a given day might be 20 or 30, while the instances of physical access authentication are less frequent and generally entail less value. The value of information and other intangible assets continually the potential value of biometric authentication as a logical access solution. However, biometric have proven very valuable in both types of applications.

Not every system fits neatly into the physical/ logical classification. Some identification systems, especially large-scale systems, are difficult to classify because the result of a match may be to investigate further- there is no resultant access to data or a physical object, but does so by allowing a user logical access to his or her data. Even allowing for difficult-to-classify applications, the differences between logical

and physical access systems are generally very pronounced: the distinction between the two is a valuable tool in understanding biometrics. Key criteria such as accuracy, response time, fallback procedures, privacy requirements, cost, and complexity of integration vary substantially when moving from logical to physical access.

4.2.4 Biometrics System Process

Whilst individual biometric devices and systems have their own operating methodology, there are some generalizations one can make as to what typically happens within a biometric systems implementation.

The following figure depicts the process pictorially and the accompanying notes provide a more detailed explanation.

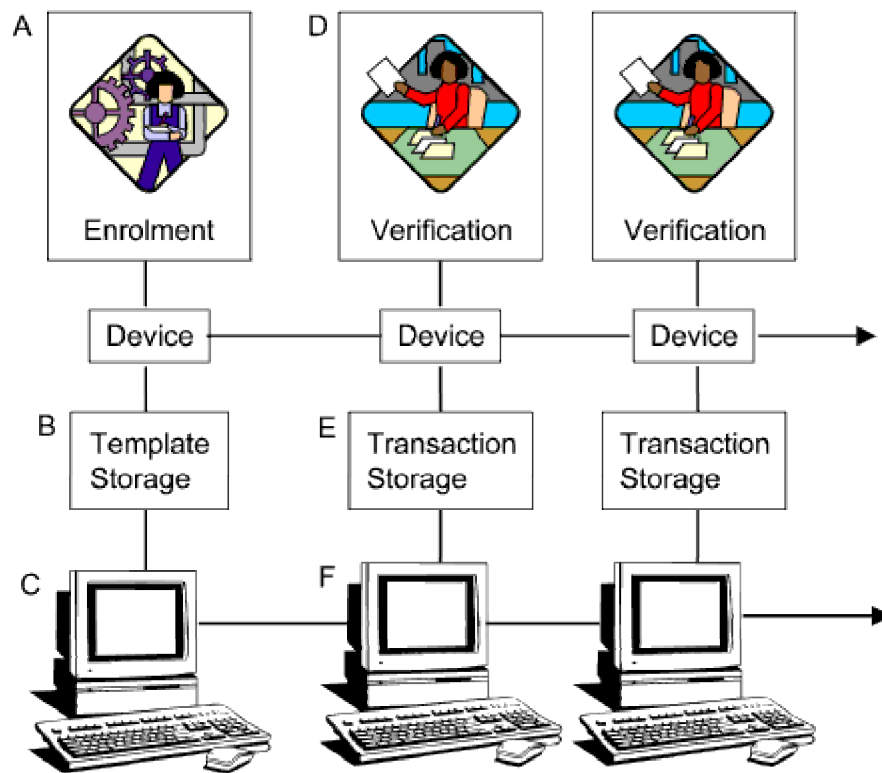


Figure: 4.2 Biometric System Process

From the figure 4.2

[A]

Before we verify an individual's identity via a biometric we must first capture a sample of the chosen biometric. This 'sample' is referred to as a biometric template and is the reference data against which subsequent samples provided at verification time are compared. A number of samples are usually captured during enrolment (typically three) in order to arrive at a truly representative template via an averaging process. The template is then referenced against an identifier (typically a PIN or card number if used in conjunction with existing access control tokens) in order to recall it ready for comparison with a live sample at the transaction point. The enrolment procedure and quality of the resultant template are critical factors in the overall success of a biometric application. A poor quality template will often cause considerable problems for the user, often resulting in a re-enrolment.

[B]

Template storage is an area of interest, particularly with large-scale applications, which may accommodate many thousands of individuals. The possible options are as follows:

- 1) Store the template within the biometric reader device.
- 2) Store the template remotely in a central repository.
- 3) Store the template on a portable token such as a chip card.

1)

Storing the template within the biometric device has both advantages and disadvantages depending on exactly how it is implemented. The advantage is potentially fast operation as a relatively small number of templates may be stored and manipulated efficiently within the device. In addition, we cannot rely on an external process or data link in order to access the template. In some cases, where devices may be networked together directly, it is possible to share templates across the network.

The potential disadvantage is that the templates are somewhat vulnerable and dependent upon the device being both present and functioning correctly. If anything happens to the device, we may need to re-install the template database or possibly re-enroll the user base.

2)

Storing the templates in a central repository is the option, which will naturally occur to IT systems engineers. This may work well in a secure networked environment where there is sufficient operational speed for template retrieval to be invisible to the user. However, we must bear in mind that with a large number of readers working simultaneously there could be significant data traffic, especially if users are impatient and submit multiple verification attempts. The size of the biometric template itself will have some impact on this, with popular

methodologies varying between 9 bytes and 1.5k. Another aspect to consider is that if the network fails, the system effectively stops unless there is some sort of additional local storage. This may be possible to implement with some devices, using the internal storage for recent users and instructing the system to search the central repository if the template cannot be found locally.

3)

Storing the template on a token. This is an attractive option for two reasons. Firstly, it requires no local or central storage of templates (unless we wish to) and secondly, the user carries their template with them and uses it at any authorized reader position.

If the user is attracted to the scheme because he believes he has effective control and ownership of his own template (a strong selling point in some cases) then we cannot additionally store his template elsewhere in the system. If he subsequently loses or damages his token, then he will need to re-enroll. Another consideration may be unit cost and system complexity if we need to combine chip card readers and biometric readers at each enrolment and verification position.

If the user base has no objection, we may wish to consider both on token and central storage of templates (options 2 and 3) this could provide fast local operation with a fallback position if the chip card reading process

fails for any reason or if a genuine user loses their token and it is to provide suitable identity information. Our choice of template storage may be dictated to some extent by our choice of biometric device. Some devices offer greater flexibility than others in this respect.

[C]

There are possible variations on a theme with regard to networks. Some devices have integral networking functionality, often via RS485 or RS422 with a proprietary protocol. This may enable us to network a number of devices together with no additional equipment involved, or maybe with a monitoring PC connected at one end of the network. In such a case, we will almost certainly be relying on the vendor's systems design and message functionality, together with their own software.

Alternatively we may design the networking, message passing and monitoring system ourselves, taking advantage of the recent generic biometric API's and accessing the reader functions directly. This will give us absolute flexibility and control over systems design, providing the chosen device supports this.

[D]

The verification process requires the user to claim an identity by either entering a PIN or presenting a token, and then verify this claim by providing a live biometric to be compared against the claimed reference template. There will be a resulting match

or no match accordingly (the parameters involved will be discussed later under performance measures). A record of this transaction will then be generated and stored, either locally within the device or remotely via a network and host (or indeed both).

With certain devices, we may allow the user a number of attempts at verification before finally rejecting them if the templates do not match. Setting this parameter requires some thought. On the one hand, we want to provide every opportunity for a valid user (who may be having difficulty using the system) to be recognized. On the other hand, we do not want impostors to have too much opportunity to experiment.

With some systems, the reference template is automatically updated upon each valid transaction. This allows the system to accommodate minor changes to the users live sample as a result of ageing, local abrasions etc. and may be a useful feature when dealing with large user bases.

[E]

Transaction storage is an important area, as we will certainly wish to have some sort of secure audit trail with respect to the use of our system. Some devices will store a limited number of transactions internally, scrolling over as new transactions are received. This is fine as long as we are confident of retrieving all such transactions before the buffer fills up and we start losing them. In practice, this is unlikely to be a problem unless we have severe network errors. In some cases, we may wish to

have each biometric device connected directly to a local PC, which may in turn be polled periodically (over night for example) in order to download transactions to a central point. In either case, we will probably wish to adopt a local procedure to deal with error and exceptional conditions, which will in turn require some sort of local messaging. This may be as simple as a relay closure in the event of a failed transaction activating an annunciator of some description.

What we do with this transaction data is another matter. We may wish to analyze it via an existing reporting tool (if it is in a suitable format) or perhaps write a custom application in order to show transactions in real time as well as write them to a central database.

[F]

How the network handles transactions may be of critical importance in some applications. For example, we may have multiple terminals distributed within a large facility, each of which requires a real time display of information. This will require fast and reliable message transmission. Each terminal user may wish to 'hold' a displayed transaction until a response has been initiated. This will require a separate local message buffer and possibly a message prioritization methodology to ensure that critical messages are dealt with promptly.

We may require variations on terminal / host software according to the user and core function. All of this will need to be accommodated within the overall network in a secure and

efficient manner. There are many potential issues to consider in this respect and overall system design should reflect this.

4.3 Fingerprint based Identification System

The biometric solutions such as the retina or facial recognition are not so mature and their costs are still too high for a widespread use.

The fingerprint has had a long history of use in police forensic science. Because of this, the authentication by fingerprint is the most convenient biometric element to identify a person. A large variety of solutions are already available and the technology is mature.

With the progress of the technology, the fingerprint is currently to be processed automatically and authenticate a person with a fingerprint reference template. The diversity of applications grows in several fields like the identity card, the driver's license, the security access, etc.

4.3.1 The Fingerprint features

A fingerprint is composed of valley and ridgelines. They follow a pattern. The general shape of this pattern may be classified according to 5 classes:

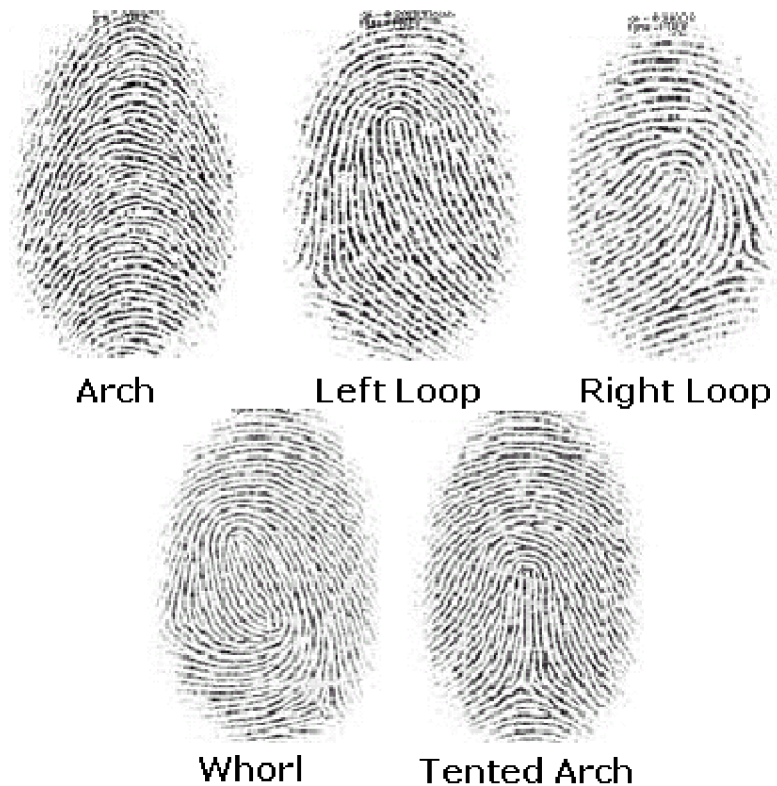


Figure: 4.3 The Classes of Fingerprint Patterns

The second features are the cores and deltas. The core is located by a square while the delta is located by a triangle on the following image. Fingers are then to be sorted in the pattern classification after computing the core and the delta.

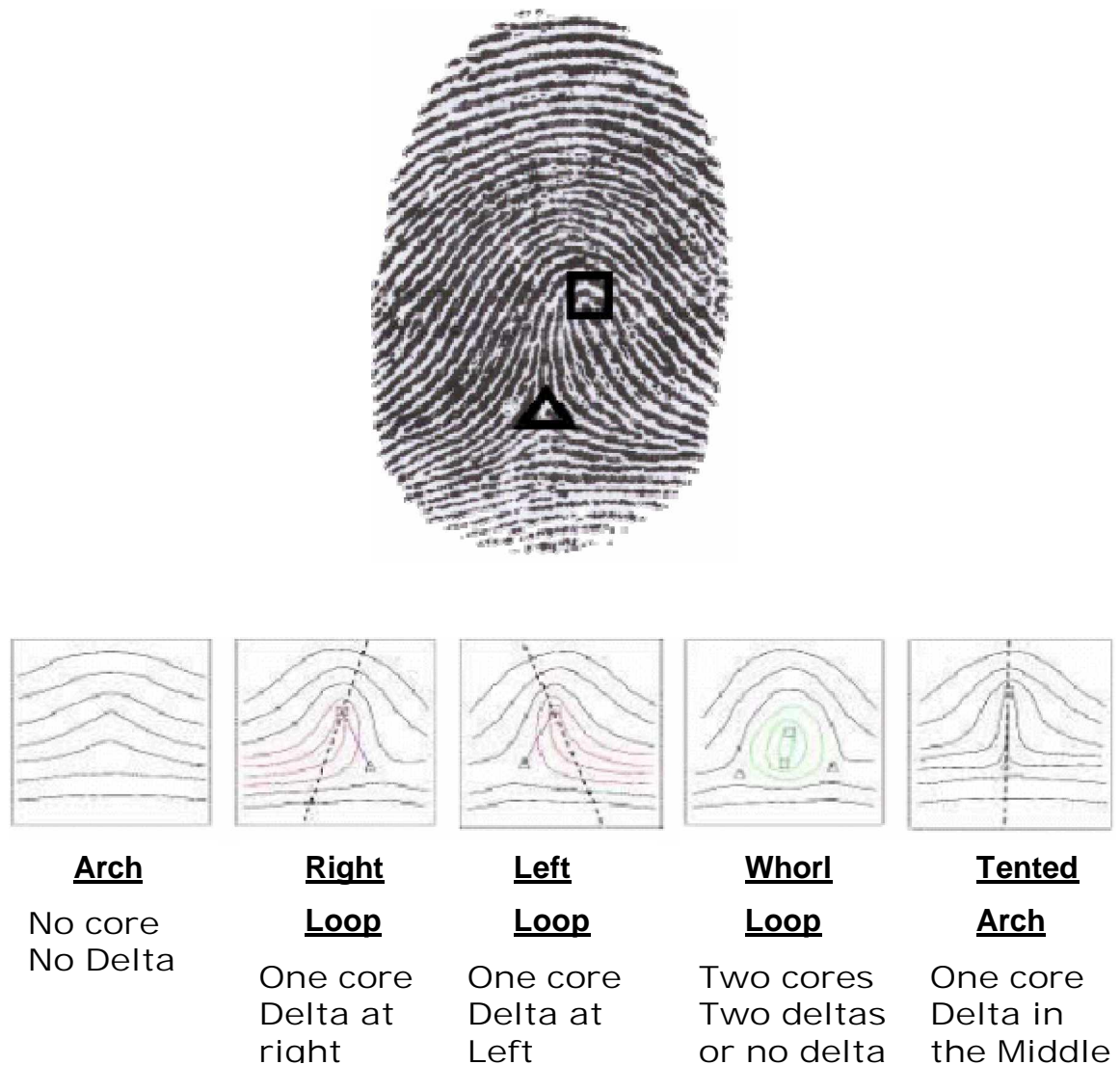


Figure: 4.4 Fingerprint Pattern Classification

The features, which give guarantee and uniqueness of a fingerprint, are the minutiae. These points are the ending ridges and the bifurcation when one ridge splits up in two ridges.

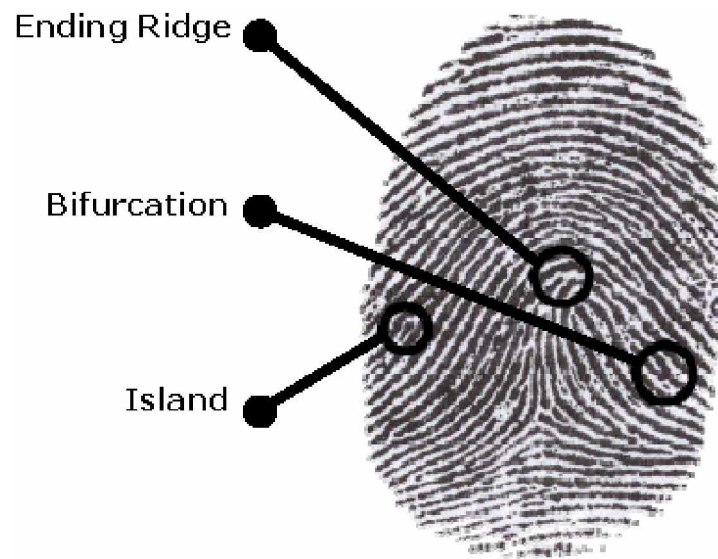


Figure: 4.5 Fingerprint Ridges, Bifurcation and Island

Ridge ending - where a line just stops.

Bifurcation – where a line splits into two.

Enclosure – where the lines make a little island

Island (Ridge dot) – a small dot

The minutiae are characterized by both their X-Y coordinates and the angle of the general direction of the ridge in this point characterize the minutia. Some minutiae are shown on the following fingerprint:

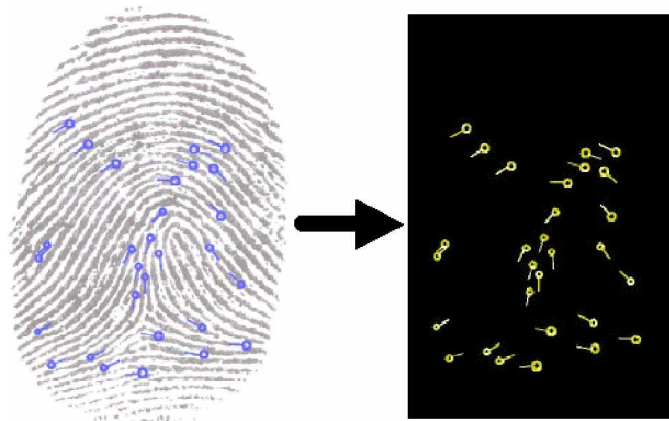


Figure: 4.6 Fingerprint Minutiae

This set of minutiae could be the minimum fingerprint template for recognition. In order to increase the performance of this electronic recognition. Each minutia is related to a vector, which describes the frequencies of the ridge, in few directions around the minutia. This vector is used when the number of minutiae is too low. This insures a better matching process. Some other features may be used like the topological configuration between the minutiae, the direction matrix or the general texture vector. These features are used to achieve a better fingerprint classification than the one based on patterns (Arch, Left Loop, Right Loop, whorl, tented arch).

4.3.2 Fingerprint Image enhancement

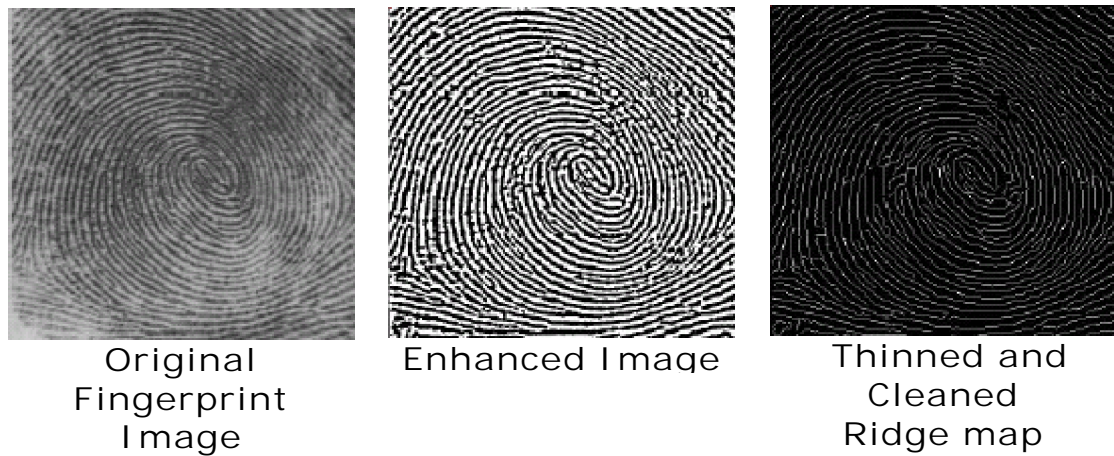


Figure: 4.7 Fingerprint Imaging

When capturing a fingerprint image, the image scan quality can usually significantly affect the performance of an electronic fingerprint system. In order to ensure that the performance of the system will be robust, with respect to the quality of the fingerprint images, it is essential to incorporate a fingerprint enhancement algorithm to filter out image noise and reliably extract ridge and minutiae from the fingerprint image.

Image noise is any condition that prohibits the accurate extraction of ridge and minutiae from the fingerprint image. This noise can come from many conditions, like having dry or wet fingerprints as an example. Dry fingerprints are from the insufficient natural moisture in the skin causing the fingerprint image to appear broken or incomplete. Wet fingerprints are from the excessive moisture in the skin causing the fingerprint image features to blend together.

Problems with scars, too dry or too moist fingers, or incorrect pressure must also be overcome to get an acceptable image. Therefore, a number of filters, some of which will be described below, are applied to the image.

- Normalization

By normalizing an image, the colors of the image are spread evenly throughout the gray scale. A normalized image is much easier to compare with other images, and the quality of the image is easier determined.

- Binarization

Making an image binary, transforms the gray scale image into a binary image (black and white). Either a global or localized threshold value is used.

- Low pass filtering

The process of low pass filtering smoothens the image to match the pixels nearby so that no points in the image differ from its surroundings to a great extent. By low pass filtering an image, errors and in-correct data are removed, and it simplifies the acquisition process of patterns or minutiae.

- Quality markup

Redundant information needs to be removed from the image before further analysis can be performed and specific features of the fingerprint can be extracted. Therefore segmentation, i.e. separating the fingerprint image from the background, is

needed. Furthermore, any unwanted minutiae (can appear if the print is of bad quality) needs to be removed.

4.3.2 Fingerprint Feature extraction and comparison

Many algorithms have been developed to match two different fingerprints and they can be divided into the following groups:

- Minutia Matching

Every fingerprint consists of a number of ridges and valleys. Ridges are the upper skin layer segments of the finger and valleys are the lower segments. The ridges form so-called minutia points; ridge endings—where a ridge ends—and ridge bifurcations—where a ridge splits.

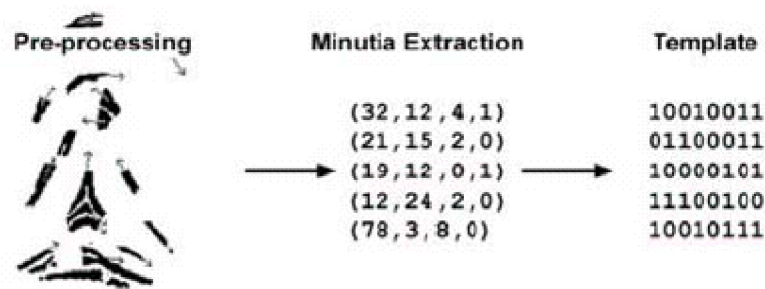


Figure: 4.8 Enrolment of minutia points

At registration—enrollment—the minutia points are located and the relative positions to each other and their directions are recorded. This data forms the template, the information later used to authenticate a person. At the matching stage, the

incoming fingerprint image is pre-processed and the minutia points are extracted. The minutia points are compared with the registered template, trying to locate as many similar points as possible within a certain boundary. The result of the matching is usually the number of matching minutiae. A threshold is then applied, determining how large this number needs to be for the fingerprint and the template to match.

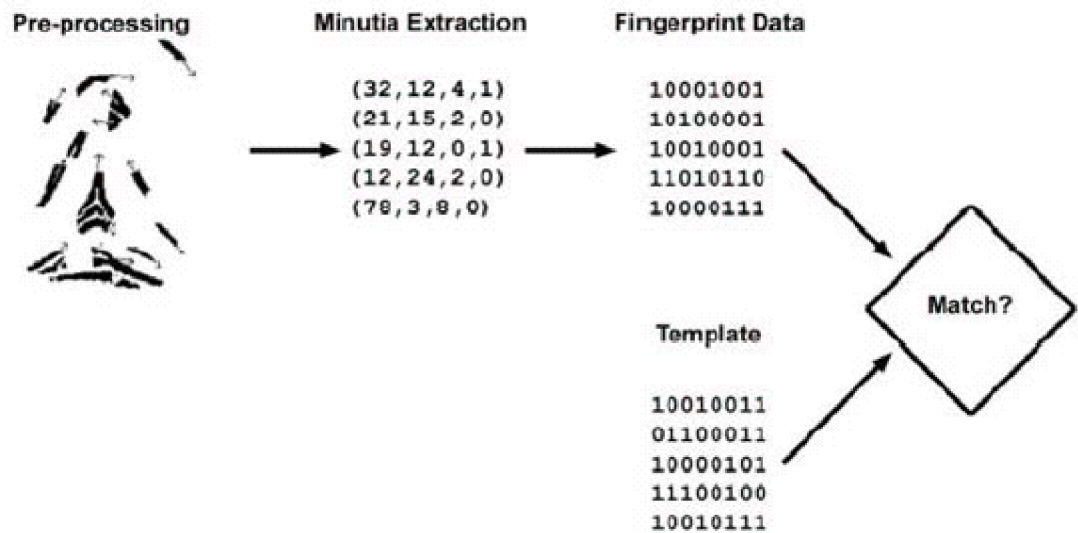


Figure: 4.9 Verification using minutia points

- **Pattern Matching**

One intrinsic property of pattern matching algorithms is that overall fingerprint characteristics are taken into account, not only individual points. Fingerprint characteristics can then include sub-areas of certain interest including ridge thickness, curvature, or density. Due to this increased depth of data a

pattern-based algorithm is less dependent on the size of the fingerprint sensor and is independent of the number of minutiae points in a fingerprint. Pattern-based algorithms do not, to the same extent as minutia-based methods, suffer from difficulties of recognizing a finger with varying fingerprint quality.

Pattern matching algorithm locates sub-areas of the fingerprint image instead of registering minutia points. Small sections of the fingerprint and their relative distances are extracted from the fingerprint (figure 4.9) in order to maximize the amount of unique information. Areas of certain interest are for example the area around a minutia point and areas with low curvature radius. The main structure and unusual combinations of ridges are also valuable data.

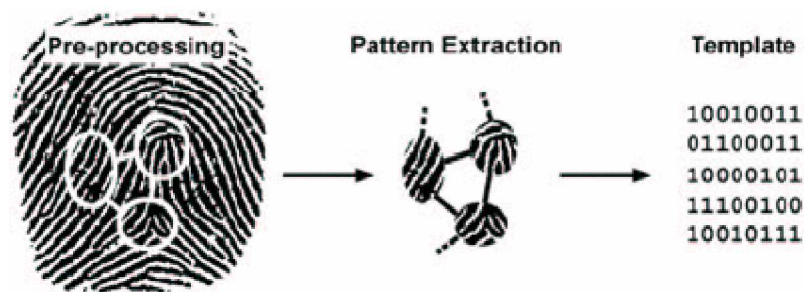


Figure: 4.10 Enrolment with pattern-based algorithm

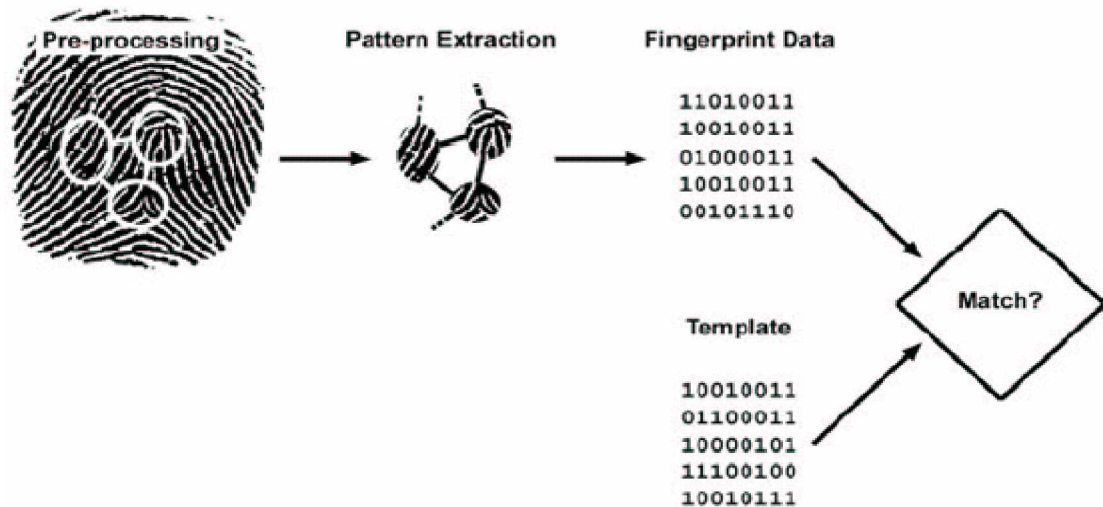


Figure: 4.11 Verification using pattern-based algorithm

The verification procedure begins with the pre-processing of the incoming fingerprint image. The registered small images from the template are then compared with the fingerprint image to determine to what degree the template matches the image. A threshold describing the smallest allowable deviation is then used to decide if the finger matches the stored template.

4.3.2 Fingerprint Scanners

A fingerprint scanner has basically two tasks; to acquire an image of a fingerprint, and to decide whether or not this image matches the image of a previously enrolled fingerprint. Extracting features from the image and then comparing these features to templates stored in a database or a smart card make decision.

The first generation fingerprint scanners appeared on the market in the mid eighties, so the technology is about fifteen years old. Over the past few years the technology for scanning fingerprints for commercial purposes has evolved a lot. While the first generation sensors used optical techniques to scan the finger, current generation sensors are based on a variety of techniques. The following techniques are deployed in commercial products that are currently available:

- Optical sensors with CCD or CMOS cameras
- Ultrasonic sensors
- Solid state electric field sensors
- Solid state capacitive sensors
- Solid state temperature sensors

The techniques will be described in greater detail in this section. The solid-state sensors are so small that they are to be built into virtually any machine. Currently a sensor is in development that will be built in a plastic card the size of a credit card, not only with respect to length and width but also with respect to thickness! It is clear that this type of sensor will give a boost to the number of applications using fingerprint technology.

- Optical Sensors

With optical sensors, the finger is placed or pushed on a plate and illuminated by a LED light source. Through a prism and a system of lenses, the image is projected on a camera. This can be either a CCD camera or, its modern successor, a CMOS

camera. Using frame grabber techniques, the image is stored and ready for analysis.

- Ultrasonic Sensors

Ultrasonic techniques were discovered when it was noticed that there is a difference in acoustic impedance of the skin (the ridges in a fingerprint) and air (in the valleys of a fingerprint). The sensors that are used in these systems are not new; they were already being deployed for many years in the medical world for making echo's. The frequency range, which these sensors use, is from 20kHz to several GigaHertz. The top frequencies are necessary to be able to make a scan of the fingerprint with a resolution of about 500 dots per inch (dpi). This resolution is required to make recognition of minutiae possible.

- Electric Field Sensors

This solid-state sensor has the size of a stamp. It creates an electric field with which an array of pixels can measure variations in the electric field, caused by the ridges and valleys in the fingerprint. According to the manufacturer the variations are detected in the conductive layer of the skin, beneath the skin surface or epidermis.

- Capacitive Sensors

Capacitive sensors are, just as the electric field sensors, the size of a stamp. When a finger is placed on the sensor an array of pixels measures the variation in capacity between the

valleys and the ridges in the fingerprint. This method is possible since there is a difference between skin-sensor and air-sensor contact in terms of capacitive values.

- Temperature Sensors

Sensors that measure the temperature of a fingerprint can be smaller than the size of a finger. Although either width or height should exceed the size of the finger, the other dimension can be fairly small since a temperature scan can be obtained by sweeping the finger over the sensor. The sensor contains an array of temperature measurement pixels, which make a distinction between the temperature of the skin (the ridges) and the temperature of the air (in the valleys).

4.3.2.1 Algorithms in fingerprint scanners

A typical fingerprint verification system consists of a scanning device (capture and enhancement), a feature extraction part, and a comparison part where an identification/verification decision is taken.

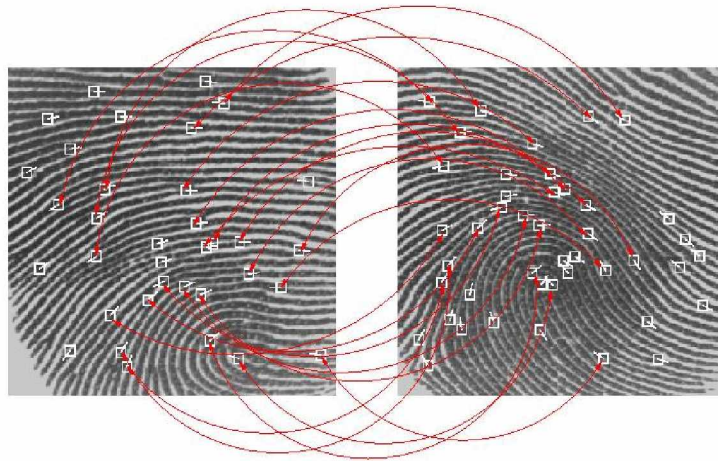


Figure: 4.12 Fingerprint Verification

For very secure applications, where we allow false rejections due to the level of security, the threshold would be set very high. In low security applications, though, we may be able to deal with a few false acceptances because whatever is being protected is of low value or may be protected.

- False Acceptance Rate (FAR)

The FAR is the frequency that a non-authorized person is accepted as authorized. Because a false acceptance often leads to damages, FAR is generally a security relevant measure. FAR is a non-stationary statistical quantity, which does not only show a personal correlation, it is to be determined for each individual feature (called personal FAR).

- False Rejection Rate (FRR)

The FRR is the frequency that an authorized person is rejected access. FRR is generally thought of as a comfort criteria,

because a false rejection is most of all annoying. FRR is a non-stationary statistical quantity, which does not only show a strong personal correlation, it can even be determined for each individual feature.

- Failure To Enroll rate (FTE or FER)

The FER is the proportion of people who fail to be enrolled successfully. FER is a non-stationary statistical quantity, which does not only show a strong personal correlation, it can even be determined for each individual feature (called personal FER).

Those who are enrolled yet are mistakenly rejected after much verification / identification attempts count for the Failure To Acquire (FTA) rate. FTA can originate through temporarily not measurable features ("bandage", non-sufficient sensor image quality, etc.). The FTA usually is considered within the FRR and need not be calculated separately.

- False Identification Rate (FIR)

The False Identification Rate is the probability in an identification that the biometric feature is falsely assigned to a reference. The exact definition depends on the assignment strategy; namely, after feature comparison, often more than one reference will exceed the decision threshold.

- False Match Rate (FMR)

The FMR is the rate which non-authorized people are falsely recognized during the feature comparison. In contrast to the FAR, attempts previously rejected due to poor (image) quality (Failure to Acquire, FTA) are not accounted for. Whether a falsely recognized feature leads to an increase in FAR or FRR depends upon the application. (There are applications that define a successful recognition as a rejection, when, for example, double release of identification cards for a person with a false identity is prevented by comparing the actual reference features with the centrally stored reference features of all cards released so far.)

- False Non-Match Rate (FNMR)

The FNMR is the rate at which authorized people are falsely not recognized during feature comparison. In contrast to the FRR, attempts previously rejected due to poor (image) quality (Failure to Acquire, FTA) are not accounted for. Whether a falsely recognized feature leads to increases in FAR or FRR depends upon the application.

- Equal error rate (EER)

The common value of the FAR and FRR when the FAR equals the FRR. This is the value where both the FAR and FRR are kept as low as possible at the same time. A low EER value indicates a high accuracy of the system.

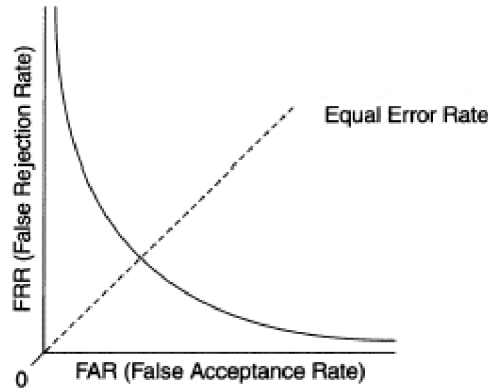


Figure: 4.13 EER Measurement

Above figure 4.12 illustrates the relationship between FRR, FAR, and EER. A big FRR often means a low FAR, and a big FAR often means a low FRR. The small EER value indicates that the security of the system is better.

The algorithm must make a speedy, automated determination of the authenticity of a fingerprint, FAR and FRR must be at or near zero. This way, authentic fingerprints are not rejected and false prints are not accepted.

4.3.3 Fingerprint Accuracy

Different technologies may be appropriate for different applications, depending on perceived user profiles, the need to interface with other systems or databases, environmental conditions, and a host of other application-specific parameters.

From the following table we can determine that the finger print verification is more accurate than any other biometrics technology for the identification system.

Characteristic	Fingerprints	Retina	Iris	Face	Signature	Voice
Ease of Use	High	Low	Medium	Medium	High	High
Error incidence	Dryness, dirt, age	Glasses	Poor Lighting	Lighting, age, glasses, hair	Changing signatures	Noise, colds, weather
Accuracy	High	Very High	Very High	High	High	High
User acceptance	Medium	Medium	Medium	Medium	Medium	High
Required security level	High	High	Very High	Medium	Medium	Medium
Long-term stability	High	High	High	Medium	Medium	Medium

Table: 4.1 Biometrics Technologies Comparison

It is important to note that fingerprint identification works on the principle of a threshold. That is, it is nearly impossible to capture the fingerprint the same way every time it is used for access.

4.4 Identification System with Integration of Fingerprint & Smart card

- Secure Identification System

The authenticity of the card and the identity of the cardholder become more important in the identification system. Especially in such case like the card is used to access corporate databases, enter into restricted areas, drive a car, or enter a country, it becomes essential that the identification process use appropriate security measures and technologies to deter both impersonation and counterfeiting and to assure the privacy of information on the card. To implement the desired security level for an application, a secure identification card system must ensure that:

- A system has been established to protect access to the cardholder's information and to prevent unauthorized viewing or tampering.
- Policies and procedures are in place for both issuing and monitoring the use of the card.
- A security control is in place to provide access to information on the card to authorized viewers.
- The identification cards are issued only by the authorized issuing organization.
- The identity of the individual applying for the card has been established.
- The person to be granted access to the privileges indicated by the card is indeed entitled to him.

To provide the highest degree of confidence in identity verification, biometric technology is considered to be essential in a secure identification system design.

Smart cards uniquely provide a single device that can function as an individual's identity card and allow the combination of several technologies to cost-effectively address varying security needs of a system.

Biometrics technologies are an authentication technology; smart cards are to be a storage, processing, and/or authentication technology. In certain applications, the two technologies compete, such that an institution may deploy smart cards instead of biometrics for access control, or vice versa. Increasingly, the two technologies are deployed in conjunction, strengthening each other's capabilities.

Typically, biometric data is stored on a smart card. Matching is to take place on a local PC or central server, on the reader itself, even within the smart card's internal memory. The result of a biometric match is to unlock a protected area of a card.



Figure: 4.14 Fingerprint Scanner with Smart card

The system may use different technologies to match fingerprints acquired by a biometric scanner with stored templates. In particular, it is possible to identify three different possibilities for the use of microcircuit or microprocessor cards within systems, which support biometric identification devices.

- **Template on Card**

This class groups those applications and systems where the biometric template is stored on a hardware security module (smartcard or USB token). In this case the template has to be retrieved and transmitted to a different system to compare the fingerprints acquired by special scanners; "memory-cards" with no operating systems and onboard applications are generally used for this purpose.

- **Match on Card**

This class groups those applications and systems where the comparison between the biometric template and the fingerprint acquired through a special scanner occur inside a hardware security module. This is typically achieved through the use of a smartcard microprocessor provided with an operating system and suitable applications and the biometric template is safely stored on the card itself.

- **System on Card**

This is an evolution of the two technologies above and is certainly the best solution in terms of security because it includes the use of hardware security modules hosting

biometric scanners where the acquisition, processing, template selection and match operations occur within a totally secure system. This type of technology is realized through the use of smartcards with piezoelectric fingerprint readers or USB tokens equipped with special fingerprint scanners. The use of USB token-based systems is preferred since they do not need a special smartcard reader but are directly connected to the host processing system.

Some systems that can provide safe access to protected data inside hardware token: the case at issue can be compared to the safe access problem concerning private asymmetrical keys stored on a cryptographic smartcard. In the proposed system, once the fingerprint (the authentication credential) has been acquired, the match occurs within an objective system such as a smartcard, which contains previously acquired (during card enrolment) safe templates.

4.4.1 Match on Card based Identification System

Integrating a fingerprint sensor with a smart card reader adds to the privacy of using the system for authentication because the fingerprint template resides on the smart card. It is to be directly matched with the scanned fingerprint rather than traveling through a network to be matched on the backend.

This match on card identification provides the citizen with a personal database, a personal firewall and a personal terminal. It secures personal information on the card, allowing the citizen to control access to that information and removing the need for central database access during identity verification.

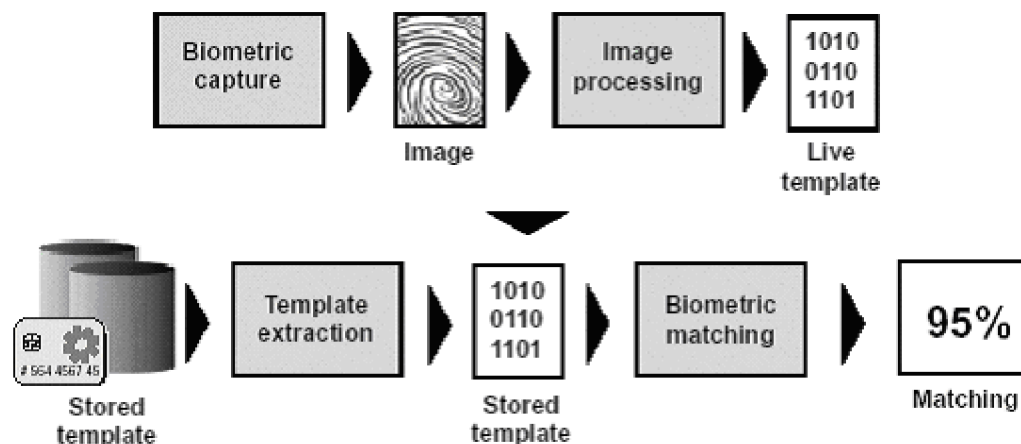


Figure: 4.15 Match on Card Technology

From the figure 4.15:

- The fingerprint reader detects the live fingerprint,
- The user's machine host system, which receives the acquired fingerprint, processes and sends it to the smartcard,
- The smartcard, after receiving the fingerprint, compares it to the template and returns an authenticated session answer to the calling user application.

This identification system has following significant security advantages.

- The fingerprint template is digitally signed and stored on the smart card at the time of enrollment and checked between the biometric capture device and the smart card it self each time the card is used.
- The template and other personal information stored on the cards are to be encrypted to improve security against external attacks.
- Cardholder authentication is performed by the smart card comparing the live template with the template stored in the card. The fingerprint template never leaves the card, protecting the information from being accessed during transmission and helping to address the user's privacy concerns.
- This card authenticates its legitimacy, and that of the reader, by creating a mutually authenticated cryptographic challenge between the card and the reader

before identity verification is started. Once that process has been accomplished, access to a specific application is to be granted. This ensures a very high level of privacy for the cardholder, prevents inappropriate disclosure of sensitive data.

- The card is also to be used to prove the digital identity of its cardholder using cryptographic keys and algorithms stored in its protected memory, making smart cards ideal for applications that need both physical and logical authentication.

With this combined biometrics & smart card technology enabled device, the security is improved further by storing the fingerprint templates inside a smart card instead of the PC. This not only provides a more secure environment but it also enhances portability and eliminates privacy concerns. It gives citizens the flexibility of being able to carry their fingerprint template with them, safe in the knowledge that no one else can use their smart card should it become lost or stolen.

Thus Smart card and fingerprint technology is to give the ultimate security to maintaining the transactions with the Citizen Card. Using this bio-smart card both citizens and government will get advantage to take and give services/information among each other.

Footnote Reference:

- Biometrics – Identity Verification in a Network World
Wiley Tech Publication, (INDIA)
- Intelligent Biometric Techniques in Fingerprint & Face
Recognition, The CRC Press, (USA)
- www.biometrics.cse.msu.edu
- www.acs.com.hk
- www.findbiometrics.com
- www.biometricgroup.com
- www.precisebiometrics.com
- www.bioapi.org

Chapter – 5

Implementation of designed Identification System on the Network Architecture and prototype generation for the entire system

- 5.1 Network Connectivity overview and requirement for the system.
- 5.2 Network Connectivity using existing network of Government of Gujarat – GSWAN for the system.
- 5.3 Internet as shared infrastructure using IPsec VPN for the system.
- 5.4 Development and implementation of the application with bio-smart card and generate the prototype that facilitates the e-Election.

5.1 Network Connectivity overview and requirement for the system.

Network connectivity requirements occur as client (voter) initiates request to the server resides in backbone network and server has to full fill the request through IP based network.

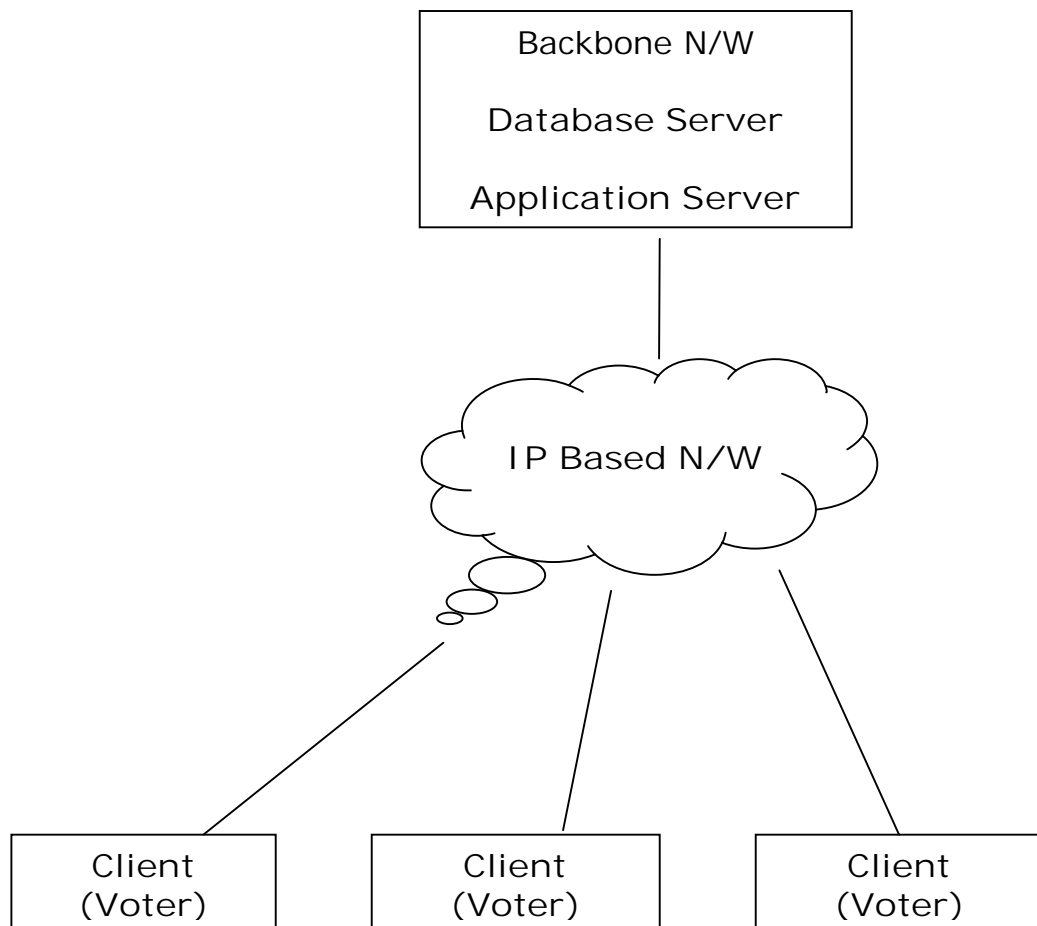


Figure: 5.1

Network connectivity requirements for the system

Entire system can be divided in to three blocks:

- a) Backbone Network
- b) IP based Network
- c) Client

a) Back bone Network

i) Application Server

An application server is a server computer in a computer network dedicated to running certain software applications. The term also refers to the software installed on such a computer to facilitate the serving (running) of other applications.

An application server is a core technology that provides key infrastructure and services to applications hosted on a system. Typical application servers include the following services:

- Resource pooling (for example, database connection pooling and object pooling)
- Distributed transaction management
- Asynchronous program communication, typically through message queuing
- A just-in-time object activation model
- Automatic XML Web Service interfaces to access business objects
- Failover and application health detection services
- Integrated security

Application Servers are referred to as middleware and provide transparency to programmers so they don't have to be concerned with the operating system or the huge array of interfaces required of a modern web based application. There has to be communication with the web in the form of HTML and XML, a link to various kinds of databases, and very likely links to systems and devices ranging from huge and irreplaceable legacy applications to small information devices which could be a link to the atomic clock or even home appliances.

Portals are a very common application server mechanism by which organizations can manage information. They provide a single point of entry for all, they can access Web services transparently from any device, and they are highly flexible. They can work inside or outside of the organization and they can attach themselves to any part of it.

Application servers are typically used for complex transaction-based applications. To support high-end needs, an application server has to have built-in redundancy, monitors for high-availability, high-performance distributed application services and support for complex database access.

In our case the application server may be designed or having such a firewall that only receive/send the request from/to the specific nodes (voting booths).

ii) Database Server

A database server is a computer program that provides database services to other computer programs or computers, as defined by the client-server model; the term may also refer to a computer dedicated to running such a program. Database management systems frequently provide database server functionality, and some DBMS's (e.g., MySQL, Oracle) rely exclusively on the client-server model for database access.

b) IP based Network

The Transmission Control Protocol (TCP) and the Internet Protocol (IP) are networked methods of data transport and generally referred to together as TCP/IP. These network protocols belong to a larger collection of protocols, or a protocol suite.

Protocols within the TCP/IP suite work together to provide data transport on the Internet. In other words, these protocols provide nearly all services available to today's Net surfer. Some of those services include

- Transmission of electronic mail
- File transfers
- Usenet news delivery
- Access to the World Wide Web

There are two classes of protocol within the TCP/IP suite, and I will address both in the following pages. Those two classes are

- The network-level protocol
- The application-level protocol

- Network-Level Protocols

Network-level protocols manage the discrete mechanics of data transfer. These protocols are typically invisible to the user and operate deep beneath the surface of the system. For example, the IP protocol provides packet delivery of the information sent between the user and remote machines. It does this based on a variety of information, most notably the IP address of the two machines. Based on this and other information, IP guarantees that the information will be routed to its intended destination. Throughout this process, IP interacts with other network-level protocols engaged in data transport. Short of using network utilities (perhaps a sniffer or other device that reads IP datagrams), the user will never see IP's work on the system.

- Application-Level Protocols

Conversely, application-level protocols are visible to the user in some measure. For example, File Transfer Protocol (FTP) is visible to the user. The user requests a connection to another machine to transfer a file, the connection is established, and the transfer begins. During the transfer, a portion of the exchange between the user's machine and the remote machine is visible (primarily error messages and status reports on the transfer itself, for example, how many bytes of the file have been transferred at any given moment).

Thus TCP/IP refers to a collection of protocols that facilitate communication between machines over the Internet (or other networks running TCP/IP).

- The OSI Model

A group called the International Standards Organization (ISO) has put together the Open Systems Interconnect (OSI) Reference Model, which is a model that describes seven layers of protocols for computer communications. These layers don't know or care what is on adjacent layers. Each layer, essentially, only sees the reciprocal layer on the other side. The sending application layer sees and talks to the application layer on the destination side. That conversation takes place irrespective of, for example, what structure exists at the physical layer, such as Ethernet or Token Ring. TCP combines the OSI model's application, presentation, and session layers into one, which is also called the application layer.

- The application layer refers to application interfaces, not programs like word processing. MHS (Message Handling Service) is such an interface and it operates at this level of the OSI model. Again, this segmentation and interface approach means that a variety of email programs can be used on an intranet so long as they conform to the MHS standard at this application interface level.
- The presentation layer typically simply provides a standard interface between the application layer and the network layers. This type of segmentation allows for the

great flexibility of the OSI model since applications can vary endlessly, but, as long as the results conform to this standard interface, the applications need not be concerned with any of the other layers.

- The session layer allows for the communication between sender and destination. These conversations avoid confusion by speaking in turn. A token is passed to control and to indicate which side is allowed to speak. This layer executes transactions, like saving a file. If something prevents it from completing the save, the session layer, which has a record of the original state, returns to the original state rather than allowing a corrupt or incomplete transaction to occur.
- The transport layer segments the data into acceptable packet sizes and is responsible for data integrity of packet segments. There are several levels of service that can be implemented at this layer, including segmenting and reassembly, error recovery, flow control, and others.
- The IP wrapper is put around the packet at the network or Internet layer. The header includes the source and destination addresses, the sequence order, and other data necessary for correct routing and rebuilding at the destination.
- The data-link layer frames the packets-for example, for use with the PPP (Point to Point). It also includes the

logical link portion of the MAC sub layer of the IEEE 802.2, 802.3 and other standards.

- Ethernet and Token Ring are the two most common physical layer protocols. They function at the MAC (Media Access Control) level and move the data over the cables based on the physical address on each NIC (Network Interface Card). The physical layer includes the physical components of the IEEE 802.3 and other specifications.

- Processing of TCP/IP Packets

Protocols such as TCP/IP determine how computers communicate with each other over networks such as the Internet. These protocols work in concert with each other, and are layered on top of one another in what is commonly referred to as a protocol stack. Each layer of the protocol is designed to accomplish a specific purpose on both the sending and receiving computers. The TCP stack combines the application, presentation, and the session layers into a single layer also called the application layer. Other than that change, it follows the OSI model. The illustration in figure 5.1 shows the wrapping process that occurs to transmit data.

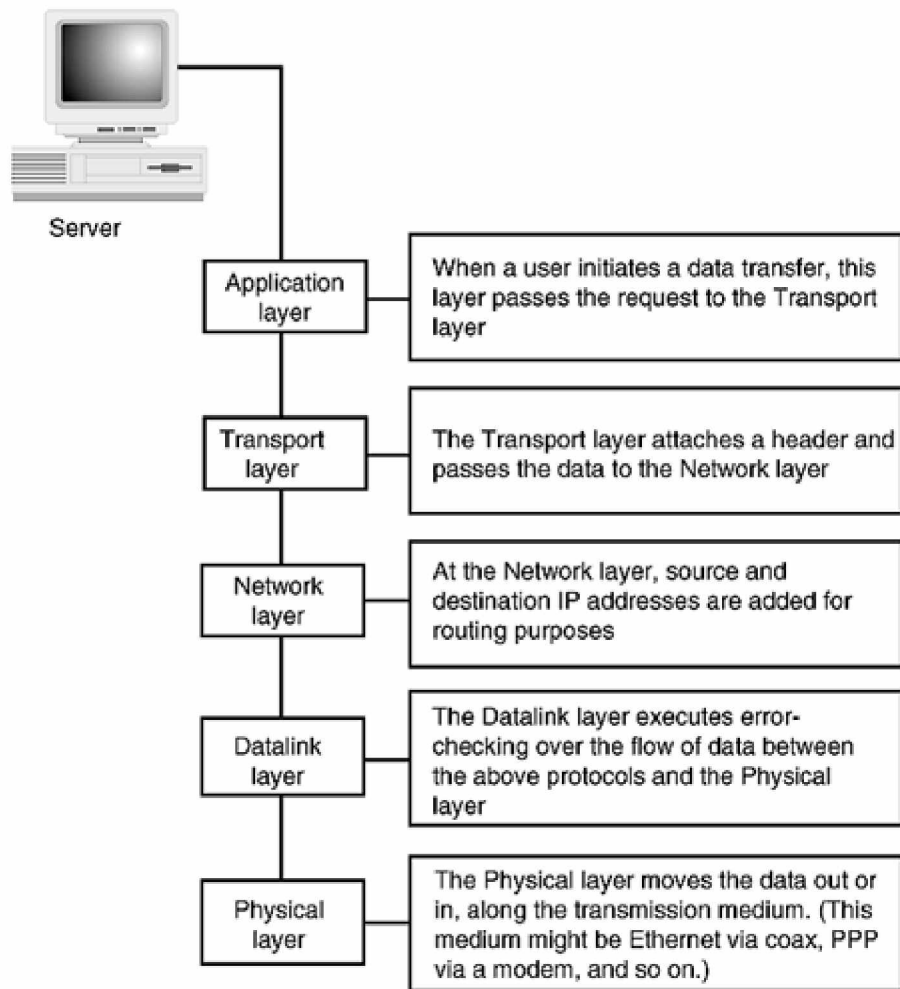


Figure: 5.2 The TCP/IP stack

After data has passed through the process illustrated in Figure 5.2, it travels to its destination on another machine or network. There, the process is executed in reverse (the data first meets the physical layer and subsequently travels its way up the stack). Throughout this process, a complex system of error checking is employed both on the originating and destination machine.

- The TCP application layer formats the data being sent so that the layer below it, the transport layer, can send the data. The TCP application layer performs the equivalent actions that the top three layers of OSI perform: the application, presentation, and session layers.
- The next layer down is the transport layer, which is responsible for transferring the data, and ensures that the data sent and the data received are in fact the same data-in other words, that there have been no errors introduced during the sending of the data. TCP divides the data it gets from the application layer into segments. It attaches a header to each segment. The header contains information that will be used on the receiving end to ensure that the data hasn't been altered en route, and that the segments can be properly recombined into their original form.
- The third layer prepares the data for delivery by putting them into IP datagrams, and determining the proper Internet address for those datagrams. The IP protocol works in the Internet layer, also called the network layer. It puts an IP wrapper with a header onto each segment. The IP header includes information such as the IP address of the sending and receiving computers, and the length of the datagram, and the sequence order of the datagram. The sequence order is added because the datagram could conceivably exceed

the size allowed for network packets, and so would need to be broken into smaller packets. Including the sequence order will allow them to be recombined properly.

- The Internet layer checks the IP header and checks to see whether the packet is a fragment. If it is, it puts together fragments back into the original datagram. It strips off the IP header, and then sends the datagram to the transport layer.
- The transport layer looks at the remaining header to decide which application layer protocol-TCP or UDP-should get the data. Then the proper protocol strips off the header and sends the data to the receiving application.
- The application layer gets the data and performs, in this case, an HTTP request.
- The next layer down, the data link layer, uses protocols such as the Point-to-Point Protocol (PPP) to put the IP datagram into a frame. This is done by putting a header-the third header, after the TCP header and the IP header-and a footer around the IP datagram to frame it. Included in the frame header is a CRC check that checks for errors in the data as the data travels over the network.

- The data-link layer ensures that the CRC for the frame is right, and that the data hasn't been altered while it was sent. It strips off the frame header and the CRC, and sends the frame to the Internet layer.
- On the receiving computer, the packet travels through the stack, but in the opposite order from which the packet was created. In other words, it starts at the bottom layer, and moves its way up through the protocol stack. As it moves up, each layer strips off the header information that was added by the TCP/IP stack of the sending computer.
- The final layer is the physical network layer, which specifies the physical characteristics of the network being used to send data. It describes the actual hardware standards, such as the Ethernet specification. The layer receives the frames from the data link layer, and translates the IP addresses there into the hardware addresses required for the specific network being used. Finally, the layer sends the frame over the network.
- The physical network layer receives the packet. It translates the hardware address of the sender and receiver into IP addresses. Then it sends the frame up to the data link layer.

TCP/IP basically comprises the Internet itself. It is a complex collection of protocols, many of which remain invisible to the user. On most Internet servers, a minimum of these protocols exist:

- Transmission Control Protocol
- Internet Protocol
- Internet Control Message Protocol
- Address Resolution Protocol
- File Transfer Protocol
- The Telnet protocol
- The Gopher protocol
- Network News Transfer Protocol
- Simple Mail Transfer Protocol
- Hypertext Transfer Protocol

With the help of this IP based network client (voter) can communicate the server and performs the online authentication from the remote voting booths. Generally voting booths are such places like schools, colleges or other governmental institutions (building), which has at least one phone line and electricity connection. With this phone line, these places can be connected to the centralized server and voter can perform the online authentication.

C) Client

From the client end the online authentication will be done with the help of biometric & smart card authentication (Bio-Smart

card) device, which is connected to the computer and that computer is, connected the central server.

The minimum requirement for the client is that it must contain window based OS (Windows-9x or higher) and the USB port so the bio-smart card device can be connected and other basic hardware/software requirement for the system is discussed later in this chapter.

Here is the brief introduction is given about the bio-smart card device.

5.1.1 Bio-Smart Card Device: AET63 BioTrustKey

The AET63 BioTrustKey is an interface for the communication between a computer (for example, a PC), a smart card and TFM (Trusted Fingerprint Module). Different types of smart cards have different commands and different communication protocols. This prevents in most cases the direct communication between a smart card and a computer. The AET63 BioTrustKey establishes a uniform interface from the computer to the smart card for a wide variety of cards. By taking care of the card specific particulars, it releases the computer software programmer of getting involved with the technical details of the smart card operation, which are in many cases not relevant for the implementation of a smart card system.

The AET63 BioTrustKey is connected to the computer through USB interface. The reader accepts commands from the computer, carries out the specified function at the smart card and returns the requested data or status information.



Figure:5.3 Bio-Smart Card Device: AET63 BioTrustKey

- ISO7816-1/2/3 compatible smart card interface
- Enrolls fingerprint, encrypts into fingerprint template and stores inside smart card
- Retrieves fingerprint template from smart card and verifies the fingerprint template inside the device.
- Supports CPU-based cards with T=0 and/or T=1 protocol
- Support PPS (Protocol and Parameters Selection) with 9600 – 96000 bps in reading and writing smart cards
- USB interface to PC with simple command structure
- Security application modules (SAM) inside the reader supporting CPU-based cards with T=0 and/or T=1 protocol (SAM Reader only)

Supported Card Types

This device can operate MCU card with T=0 and T=1 protocol. The table presented in Appendix A explains which card type selection value must be specified for the various card types supported by the reader.

Micro-controller-based smart cards (asynchronous interface)

This device supports EEPROM micro-controller-based cards with internal programming voltage (VPP) generation and the following programming parameters transmitted in the ATR:

PI1 = 0 or 5

I = 25 or 50

This device performs the Protocol and Parameters Selection (PPS) procedure as specified in ISO7816-3:1997. When the card ATR indicates the specific operation mode (TA2 present; bit b5 of TA2 must be 0) and that particular mode is not supported by the device, the reader will reset the card to set it to negotiable mode. If the card cannot be set to negotiable mode, the reader will reject the card. When the card ATR indicates the negotiable mode (TA2 not present) and communication parameters other than the default parameters, the device will execute the PPS and try to use the communication parameters that the card suggested in its ATR. If the card does not accept the PPS, the reader will use the default parameters (F=372, D=1).

Smart Card Interface

The interface between the device and the inserted smart card follows the specifications of ISO7816-3 with certain restrictions or enhancements to increase the practical functionality of the device.

Smart Card Power Supply VCC (C1)

The current consumption of the inserted card must not be higher than 50mA.

Programming Voltage VPP (C6)

According to ISO 7816-3, the smart card contact C6 (VPP) supplies the programming voltage to the smart card. Since all common smart cards in the market are EEPROM based and do not require the provision of an external programming voltage, the contact C6 (VPP) has been implemented as a normal control signal in the device. The electrical specifications of this contact are identical to those of the signal RST (at contact C2).

Card Type Selection

The controlling PC has to always select the card type through the proper command sent to the device prior to activating the inserted MCU card. For MCU-based cards the reader allows to select the preferred protocol, T=0 or T=1. However, this selection is only accepted and carried out by the reader through the PPS when the card inserted in the reader supports both protocol types. Whenever an MCU-based card supports only one protocol type, T=0 or T=1, the reader automatically

uses that protocol type, regardless of the protocol type selected by the application.

Interface for Micro-controller-based Cards

For micro-controller-based smart cards only the contacts C1 (VCC), C2 (RST), C3 (CLK), C5 (GND) and C7 (I/O) are used. A frequency of 4 MHz is applied to the CLK signal (C3).

Card Tearing Protection

This device provides a mechanism to protect the inserted card when it is suddenly withdrawn while it is powered up. The power supply to the card and the signal lines between the device and the card are immediately deactivated when the card is being removed. As a general rule, however, to avoid any electrical damage, a card should only be removed from the reader while it is powered down. The device does never by itself switch on the power supply to the inserted card. The controlling computer through the proper command sent to the reader must explicitly do this.

Power Supply

This device requires a voltage of 5V DC, 100mA, regulated, power supply. It gets the power supply from PC (through the cable supplied along with each type of reader).

Status LEDs

Green LED on the front of the reader indicates the activation status of the smart card interface:

Green LED - Indicates power supply to the smart card is switched on, i.e., the smart card is activated.

USB INTERFACE

This device is connected to a computer through a USB following the USB standard.

Communication Parameters

This device is connected to a computer through USB as specified in the USB Specification. The device is working in low speed mode, i.e. 1.5 Mbps.

USB Interface Wiring

- Pin Signal Function

1 VBUS +5V power supply for the reader

2 D- Differential signal transmits data between device and PC.

3 D+ Differential signal transmits data between device and PC.

4 GND Reference voltage level for power supply

Communication Protocol

In the normal operation, this device acts as a slave device with regard to the communication between a computer and the reader. The communication is carried out in the form of successive command-response exchanges. The computer transmits a command to the reader and receives a response from the reader after the command has been executed. A new command can be transmitted to the device only after the response to the previous command has been received.

5.2 Network Connectivity using existing network of Government of Gujarat – GSWAN for the system

Gujarat has one of the largest costal area and disasters like cyclone/flood and earthquake are frequently striking in the state. State Government has planned and augmenting a state-of-the-art state wide area network (GSWAN) to cater to the administrations internal and external communication service needs related to voice, video and data.

GSWAN planned to work in a star topology centered at Secretariat, Gandhinagar with arms extending to all districts, having further horizontal (district HQ level) and vertical downward extensions integrating multiple district level other offices and Talukas respectively with the state wide area network. Adequate dialup facilities were provisioned at all districts HQ nodes for enabling GSWAN access to the offices and units not physically integrated with the GSWAN. GSWAN was planned to be implemented in two phases with phase-I to cover district level network and Phase-II to cover total network.

The technologies selected for the GSWAN is IP and all services i.e. Video conferencing, Voice (telephony) and data services are IP based. This is unique and distinct (may be first time anywhere on such a large scale) about GSWAN that all services are IP based.



Figure 5.4 GSWAN Network

Connectivity (band width) needs were defined on the basis of traffic estimated between various network nodes. The project specifications included – bandwidth requirements, dialup connections, VSAT links (to impart mobility feature to WAN and to cover inaccessible location when required). Number of subscribers and the growth pattern were analyzed for arriving at various resources requirements on time scale. Assessment of Internet bandwidth, email service, web-hosting resources, DBM resources etc was done keeping e-Governance objectives into consideration. Web sites have been found very effective media

for mass communication, specifically information dissemination to whole world at any point of time. This was considered that each department should have their web site for dissemination of information to the public and vice -versa. Wide Area Network resources design included intra, extra and inter networking requirements.

Initially, as planned all districts HQ are linked with the Secretariat with 2 MBPS leased circuits and all Talukas (TC) linked with the District HQ (DC) with 64 KBPS leased circuits taken from Bharat Sanchar Nigam Limited (BSNL). CISCO 7513 is the central router at Secretariat with CISCO 3661 and CISCO 1751 at District and Taluka level. There are at least 20 other offices at each district HQ, in the process of integration with the district wide area node (DC) through bare copper taken from BSNL. Each DC has 10 telephone (receive only) lines from PSTN terminating on to the CISCO 3661 for dialup services. In all there are 250 dialup ports available through the state enabling units/offices/individuals to hook on to GSWAN just by making a local call, from anywhere within the state.

5.2.1 GSWAN Network Architecture and Topology

The network topology as conceived and designed for GSWAN was based on a hub-and-spoke design philosophy, with three tiers.

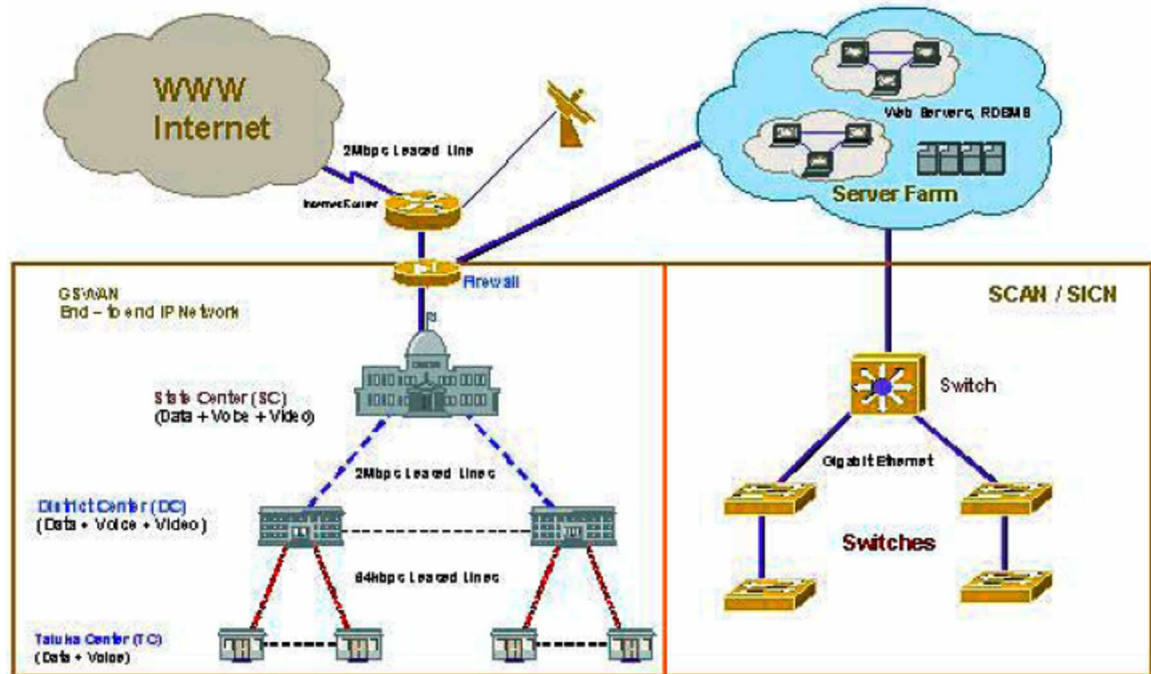


Figure: 5.5 GSWAN Network Architecture

5.2.1.2 Second Tier Architecture

District Centers, or "DC"s, located at district collector's office, and multiple district level offices connected with DC horizontally.

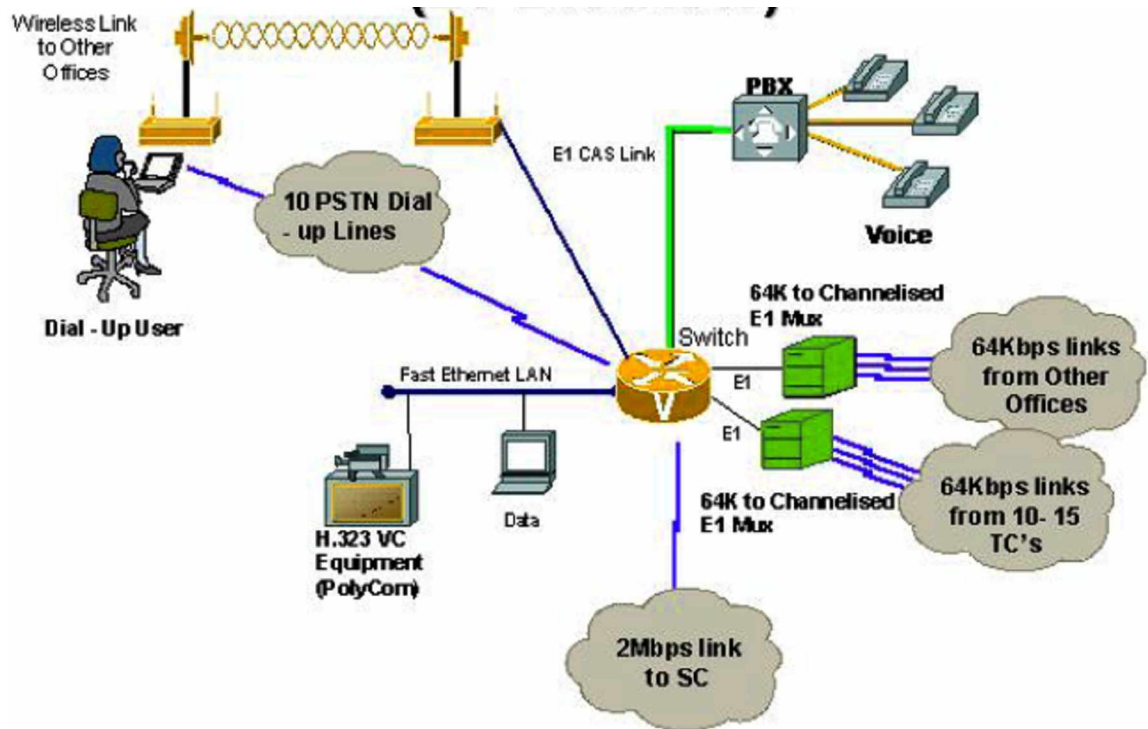


Figure: 5.7 Second tier architecture of GSWAN

5.2.1.3 Third Tier Architecture

Talukas Centers, or "TC's", located at Taluka Mamlatdar's office, and couple of Taluka level offices horizontally connected with TC. Secretariat Center (SC) at capital is marked as tier -1. This is the network hub. Secretariat Campus Area Network (SCAN) integrates with GSWAN at SC (shown in figure above). SCAN has about 7000 Ethernet I/Os at capital city, Gandhinagar and all these I/Os are interconnected with GSWAN for information exchange. 300 Telephone connections given to various offices at Secretariat for direct voice communication to any GSWAN node in the state.

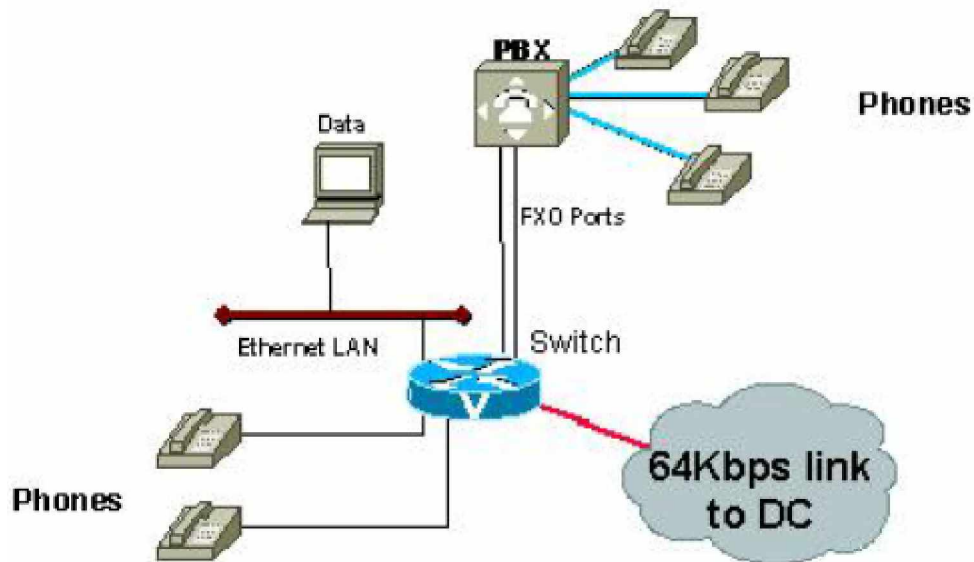


Figure: 5.8 Third tier architecture of GSWAN

5.2.2 Technology and Data Flow in GSWAN

GSWAN is a total IP network. Data, Voice and video travels as IP packets in the network, with a total convergence. An attempt is made to explain the data flow taking place in the network for Data, voice, and video services, as given below-

Data Flow from PC to PC in GSWAN:

- Application on computer encapsulates the data in Layer 7-Layer 5 headers
- Network driver on PC then includes Layer 4 and Layer 3 information, packetization, and encapsulation in IP. This includes source and destination IP address, TCP port, etc.
- NIC encapsulates IP data within Layer 2 MAC header, and sends it out over the LAN.
- If the destination IP address is not on the LAN, the frame reaches the router. Router strips off layer 2 MAC header, and looks at the destination IP address.
- Router does a lookup in the routing table, finds appropriate interface to send the packet out of. If this is a WAN interface, then a Layer 2 PPP header is appended to the packet, and it is queued on the interface. At this time, appropriate QoS/Queuing mechanisms are applied to the packet, based on the configuration done on the router, and the information available in the IP header.
- Once the packet reaches the remote router, the remote router strips off the Layer 2 PPP header and looks at the destination IP address. This destination IP address will typically be on the local LAN.

- Then, the router encapsulates the IP packet into a MAC header and puts it on to the LAN interface. The packet now has the destination MAC address of the PC that the data is destined to.
- The destination PC receives the data, strips off the L2-L7 information, processes it and presents the data to the application after gathering all IP packets in that flow.

Based on Cisco Systems AVVID (Architecture for Voice, Video and Integrated Data) and implemented in 2002, GSWAN connects the state's central offices in Ahmedabad with more than 200 regional offices throughout the state, providing data, voice, and video services. GSWAN connectivity now extends to universities, police stations, and other offices within the state.

5.2.3 Use the entire GSWAN network in Election

The Gujarat government creates a cost-effective and timesaving program that facilitates communications, public services, and information to its citizens.

With the advantage of such efficient entire network of GSWAN, the procedure of authentication (of voter) can be done online. Some modifications would be required such as:

- The GSWAN network could be extended up to the village level.
- On the day of election the GSWAN network could only be used for election, and other uses of this network could be stopped for security purpose.
- Application server and database server could be located centralized at state capital.
- Voting booths, from where the online authentication would take place, could be connected via dial-up and other where the phone line is not available (such as villages, which don't have telecommunication facilities); V-SAT can be used for network connectivity.

5.3 Internet as shared infrastructure using IPsec VPN for the system

A VPN is a communications environment in which access is controlled to permit peer connections only within a defined community of interest, and is constructed through some form of partitioning of a common underlying communications medium, where this underlying communications medium provides services to the network on a non-exclusive basis. In short VPN is private network constructed within a public network infrastructure, such as the global Internet.

A virtual private network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link. The act of configuring and creating a virtual private network is known as virtual private networking.

To emulate a point-to-point link, data is encapsulated, or wrapped, with a header that provides routing information allowing it to traverse the shared or public transit internetwork to reach its endpoint. To emulate a private link, the data being sent is encrypted for confidentiality. Packets that are intercepted on the shared or public network are indecipherable without the encryption keys. The portion of the connection in which the private data is encapsulated is known as the tunnel.

The portion of the connection in which the private data is encrypted is known as the virtual private network (VPN) connection.

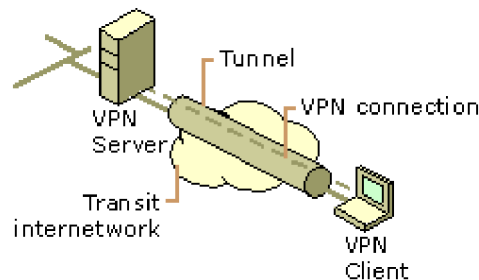


Figure: 5.9 Virtual Private Network connection

VPN connections allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). From the user's perspective, the VPN connection is a point-to-point connection between the user's computer and a corporate server. The nature of the intermediate internetwork is irrelevant to the user because it appears as if the data is being sent over a dedicated private link.

VPN technology also allows a corporation to connect to branch offices or to other companies over a public internetwork (such as the Internet), while maintaining secure communications. The VPN connection across the Internet logically operates as a wide area network (WAN) link between the sites.

In both of these cases, the secure connection across the internetwork appears to the user as a private network communication—despite the fact that this communication occurs over a public internetwork—hence the name virtual private network.

VPN technology is designed to address issues surrounding the current business trend toward increased telecommuting and widely distributed global operations, where workers must be able to connect to central resources and must be able to communicate with each other.

With an Internet solution, a few Internet connections through Internet service providers (ISPs) and VPN server computers can serve the remote networking needs of hundreds or thousands of remote clients.

5.3.1 Common Uses of VPNs

The next few subsections describe the more common VPN configurations in more detail.

- Remote Access over the Internet

VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information. Figure 2 shows a VPN connection used to connect a remote user to a corporate intranet.

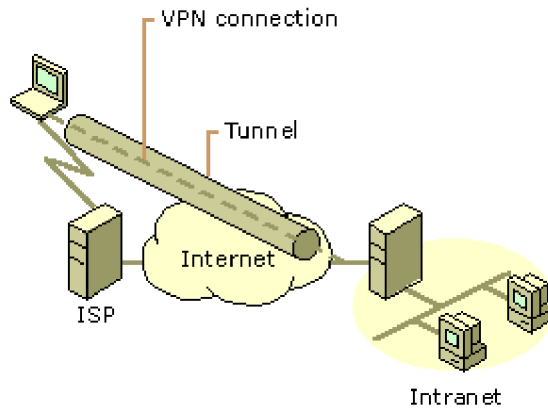


Figure: 5.10

Using a VPN connection to connect a remote client to a private intranet

Rather than making a long distance (or 1-800) call to a corporate or outsourced network access server (NAS), the user calls a local ISP. Using the connection to the local ISP, the VPN software creates a virtual private network between the dial-up user and the corporate VPN server across the Internet.

- Connecting Networks over the Internet

There are two methods for using VPNs to connect local area networks at remote sites:

- Using dedicated lines to connect a branch office to a corporate LAN.

Rather than using an expensive long-haul dedicated circuit between the branch office and the corporate hub, both the branch office and the corporate hub routers can use a local

dedicated circuit and local ISP to connect to the Internet. The VPN software uses the local ISP connections and the Internet to create a virtual private network between the branch office router and corporate hub router.

- Using a dial-up line to connect a branch office to a corporate LAN.

Rather than having a router at the branch office make a long distance (or 1-800) call to a corporate or outsourced NAS, the router at the branch office can call the local ISP. The VPN software uses the connection to the local ISP to create a VPN between the branch office router and the corporate hub router across the Internet.

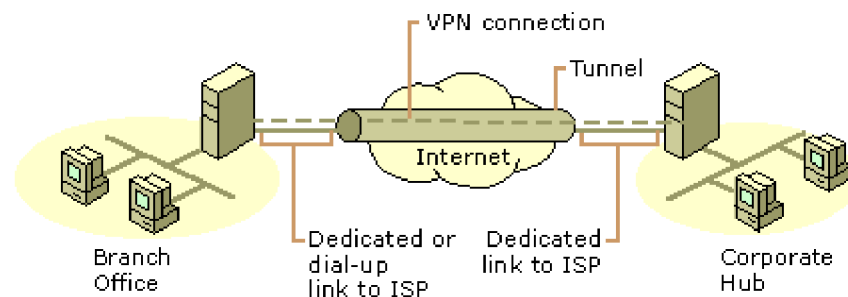


Figure: 5.11

Using a VPN connection to connect two remote sites

In both cases, the facilities that connect the branch office and corporate offices to the Internet are local. The corporate hub router that acts as a VPN server must be connected to a local ISP with a dedicated line. This VPN server must be listening 24 hours a day for incoming VPN traffic.

- Connecting Computers over an Intranet

In some corporate internetworks, the departmental data is so sensitive that the department's LAN is physically disconnected from the rest of the corporate internetwork. Although this protects the department's confidential information, it creates information accessibility problems for those users not physically connected to the separate LAN.

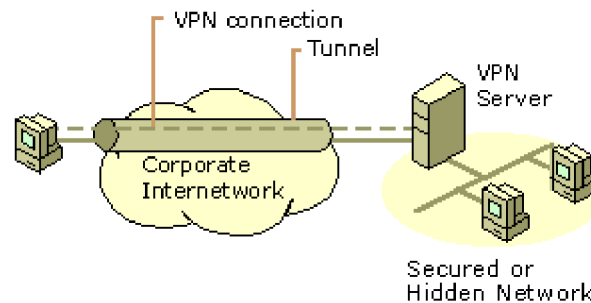


Figure: 5.12

Using a VPN connection to connect to a secured or hidden network

VPNs allow the department's LAN to be physically connected to the corporate internetwork but separated by a VPN server. The VPN server is not acting as a router between the corporate internetwork and the department LAN. A router would connect the two networks, allowing everyone access to the sensitive LAN. By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the department. Additionally, all communication across the VPN can be

encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN.

5.3.2 Basic VPN Requirements

Typically, when deploying a remote networking solution, an enterprise needs to facilitate controlled access to corporate resources and information. The solution must allow roaming or remote clients to connect to LAN resources, and the solution must allow remote offices to connect to each other to share resources and information (router-to-router connections). In addition, the solution must ensure the privacy and integrity of data as it traverses the Internet. The same concerns apply in the case of sensitive data traversing a corporate internetwork.

Therefore, a VPN solution should provide at least all of the following:

- User Authentication

The solution must verify the VPN client's identity and restrict VPN access to authorized users only. It must also provide audit and accounting records to show who accessed what information and when.

- Address Management

The solution must assign a VPN client's address on the intranet and ensure that private addresses are kept private.

- **Data Encryption**
Data carried on the public network must be rendered unreadable to unauthorized clients on the network.
- **Key Management**
The solution must generate and refresh encryption keys for the client and the server.
- **Multiprotocol Support**
The solution must handle common protocols used in the public network. These include IP, Internetwork Packet Exchange (IPX), and so on.

An Internet VPN solution based on the Point-to-Point Tunneling Protocol (PPTP) or Layer Two Tunneling Protocol (L2TP) meets all of these basic requirements and takes advantage of the broad availability of the Internet. Other solutions, including Internet Protocol Security (IPSec), meet only some of these requirements, but remain useful for specific situations.

5.3.4.1 Internet Protocol Security (IPSec)

IP Security (IPSec) was designed by the IETF as an end-to-end mechanism for ensuring data security in IP-based communications. IPSec has been defined in a series of RFCs, notably RFCs 2401, 2402, and 2406, which define the overall architecture, an authentication header to verify data integrity, and an encapsulation security payload for both data integrity and data encryption.

IPSec is a Layer 3 protocol standard that supports the secured transfer of information across an IP internetwork. IPSec is more fully described in the Advanced Security section below. However, one aspect of IPSec should be discussed in the context of tunneling protocols. In addition to its definition of encryption mechanisms for IP traffic, IPSec defines the packet format for an IP over IP tunnel mode, generally referred to as IPSec tunnel mode. An IPSec tunnel consists of a tunnel client and a tunnel server, which are both configured to use IPSec tunneling and a negotiated encryption mechanism.

IPSec tunnel mode uses the negotiated security method (if any) to encapsulate and encrypt entire IP packets for secure transfer across a private or public IP internetwork. The encrypted payload is then encapsulated again with a plain-text IP header and sent on the internetwork for delivery to the tunnel server. Upon receipt of this datagram, the tunnel server processes and discards the plain-text IP header, and then decrypts its contents to retrieve the original payload IP packet. The payload IP packet is then processed normally and routed to its destination on the target network.

IPSec tunnel mode has the following features and limitations:

- It supports IP traffic only.
- It functions at the bottom of the IP stack; therefore, applications and higher-level protocols inherit its behavior.
- It is controlled by a security policy—a set of filter-matching

rules. This security policy establishes the encryption and tunneling mechanisms available, in order of preference, and the authentication methods available, also in order of preference. As soon as there is traffic, the two computers perform mutual authentication, and then negotiate the encryption methods to be used. Thereafter, all traffic is encrypted using the negotiated encryption mechanism, and then wrapped in a tunnel header.

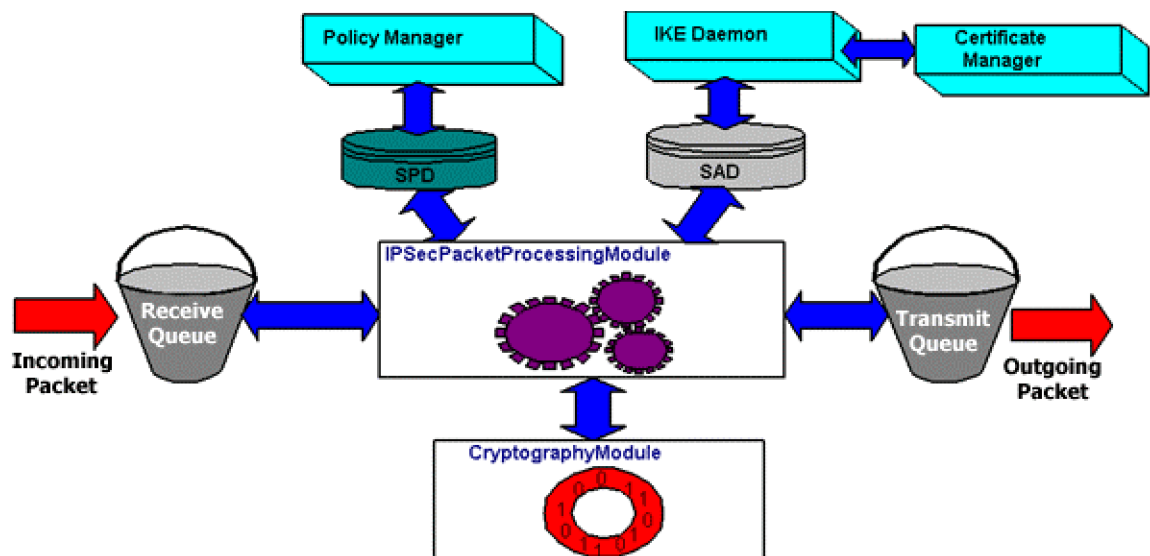


Figure: 5.13 IPsec architecture

IPsec defines two functions that ensure confidentiality: data encryption and data integrity. As defined by the IETF, IPsec uses an authentication header (AH) to provide source authentication and integrity without encryption, and the Encapsulating Security Payload (ESP) to provide authentication and integrity along with encryption. With IPsec, only the

sender and recipient know the security key. If the authentication data is valid, the recipient knows that the communication came from the sender and that it was not changed in transit.

IPSec can be envisioned as a layer below the TCP/IP stack. This layer is controlled by a security policy on each computer and a negotiated security association between the sender and receiver. The policy consists of a set of filters and associated security behaviors. If a packet's IP address, protocol, and port number match a filter, the packet is subject to the associated security behavior.

- Negotiated Security Association

The first such packet triggers a negotiation of a security association between the sender and receiver. Internet Key Exchange (IKE) is the standard protocol for this negotiation. During an IKE negotiation, the two computers agree on authentication and data-security methods, perform mutual authentication, and then generate a shared key for subsequent data encryption.

After the security association has been established, data transmission can proceed for each computer, applying data security treatment to the packets that it transmits to the remote receiver. The treatment can simply ensure the integrity of the transmitted data, or it can encrypt it as well.

- Authentication Header

An authentication header located between the IP header and the transport header can provide data integrity and data authentication for IP payloads. The authentication header includes authentication data and a sequence number, which together are used to verify the sender, ensure that the message has not been modified in transit, and prevent a replay attack. The IPSec authentication header provides no data encryption; clear-text messages can be sent, and the authentication header ensures that they originated from a specific user and were not modified in transit.

5.3.4.2 IPSec VPN Technology Advancements

It is critical to supporting a robust networking solution about security, performance and availability, and management and monitoring.

- Security

Although security improvements have been made across the board for IPSec VPNs, the impact is most direct on remote access and smaller corporate sites. In the past, most security has been handled by a separate firewall at the main hub site, requiring each remote user to be routed through that firewall before gaining access to the corporate network. With the integration of firewalls into VPN devices, the security capabilities are dramatically improved resulting in other benefits as well. Some specific security improvements include the following:

Combined Firewall/VPN Client Software

One of the security issues with remote dial users has been the risk of carrying unwanted users into the corporate network on encrypted tunnels. While it's been possible to deploy remote firewalls to small offices or broadband access users, that hasn't been a practical solution for dial users. When remote firewalls were deployed for smaller branch offices, the management burden on the IT department was increased. Deploying firewalls to remote clients increases the burden exponentially. Today's management solutions reduce these headaches by allowing software upgrades and configuration changes to be pushed out to remote clients.

Integrated Firewall/VPN

As mentioned above, separate firewall and VPN devices have presented management issues. Initially network managers had difficulty in getting both devices configured so that the firewall would not block VPN traffic. Similarly, authentication for remote sites was difficult to accomplish through a separate firewall. With integrated capabilities, performance is improved across the board. Remote sites can connect directly to the Internet without having to go through a centrally located corporate firewall. Also, an added layer of security is gained for remote sites with the firewall and authentication tasks supported. Previously, remote sites may have foregone the separate firewall due to expense or management, which presented a significant risk for DOS attacks.

With new integrated VPN devices, the risk of DOS attacks through a remote user is greatly reduced or eliminated. Finally, authentication can be accomplished within the integrated firewall/VPN rather than the enterprise manager having to set up split tunnels for VPN and Internet traffic.

Enhanced Authentication

End-user authentication is a critical but challenging task to ensure network integrity. Authentication of end-users both externally and internally within the enterprise is important. Since many network breaches occur internally within an enterprise, end-user authentication must be of the highest standards. Fortunately, today's solutions provide a number of different ways for end-users to authenticate including the use of PKI and smart cards or tokens.

PKI support

A PKI provides many functions in the security realm. The most common is acting as a digital signature. The digital signature provides assurance that the sender is who they say they are and the receiver is the intended recipient. PKI also provides message integrity by ensuring the message has not been altered. So a receiver can have confidence that the message is the original message and a third party has not altered it. Lastly, it can block the sender's false denial that the sender sent a particular message (non-repudiation).

Smart card or token support

Smart card or token technology has recently been applied to VPNs. They are a practical way to implement a PKI strategy and provide enterprises with more sophisticated solutions for enhancing user authentication. New technology allows the user to simply insert their smart card or token into the reader on their computer and enter a password and perhaps a user name. This will authenticate the user and contain the necessary keys for encryption. Enterprises using this technology do not have to worry about securing digital certificates on computer hard drives. Keys are contained on the smart card and not placed on the computer hard drive. This prevents any duplication of the key or the chance the key can be obtained by an unauthorized source.

Performance and Availability

With the improvements in the VPN hardware and software, business continuity is improved from several aspects. VPN devices have increased their scalability and processing power, with not only more robust platforms for main corporate sites available, but also smaller solutions for single user or branch office sites. Performance and availability of IPSec VPN solutions has improved in the following key areas:

Redundant Devices and Configurations

VPN gateways and appliances have been improved to support redundant configurations, depending on the need of a particular site. The critical nature of corporate networks requires them to be available 24X7. Any downtime can cost

enterprises revenue and/or operational constraints. The use of redundant devices provides these networks with a higher level of availability. In addition, it may be desirable to have these devices fully configured should the primary device fail. Redundant configuration is supported in two ways today—active/active mode or active/passive mode. With an active/active configuration, two devices load share VPN traffic, and should one fail the second device can support the full traffic load. In the active/passive configuration, the passive device becomes active should the primary device fail. Both of these configurations are capable of sub-second fail over. Just as important is whether the fail over occurs in a stateful or non-stateful capacity. Stateful fail over, a capability a smaller number of vendors support, maintains all the connections during the fail over process. Non-Stateful failovers must re-establish these connections, which can be time consuming in a large network. End-users will not notice stateful failovers but will notice non-stateful ones since they take some time to re-establish the connections.

Traffic Shaping

IP has always been a “best effort” network protocol, but the latest solutions have added traffic shaping capabilities to new IPSec VPN platforms. Bandwidth can be shaped on a per-user or per-application basis. Traffic management can be applied based on source, destination, application type, user, group, or other criteria as defined by the network manager. The results can bring improved performance for users or applications, and

a better utilization of network bandwidth appropriate to the needs of the applications.

Dial Backup Capabilities

For remote users or sites that may be taking advantage of broadband access such as DSL or cable modem services, there has been no integrated backup connection in older VPN CPE. With newer devices, a dial backup facility is integrated so that if the primary connection goes down, the user(s) will still have a network connection through the public switched telephone network.

Dynamic Routing

By supporting OSPF and BGP, deployment of IPSec VPNs in the core of large networks becomes easier. In essence, routing capabilities enable the following:

- Ease the management associated with the central site and remote office network changes.
- Can be used to support the augmentation of legacy services, and also offer alternative paths to route traffic around network congestion or failures.
- Ability to support dual VPN gateways by providing the ability to configure multiple definitions for each tunnel that can be used as a fail over solution when one gateway goes down.

- Dual Internet service provider support so one can be used as a backup as well as for traffic engineering purposes. Enterprises can run critical data across VPN tunnels and maintain a predictable level of network performance.
- Support of full meshes networks. Enterprises can now implement fully meshed networks and augment costly Frame Relay and private lines.

Management and Monitoring

Often management and monitoring capabilities lag other technical developments as service providers and enterprises struggle with initial implementations, regardless of the technology. Today service providers are offering relatively mature management capabilities to support VPNs, and enterprises that are building their own networks have many of the same advantages as the service providers do. Some of the improvements in this area are listed below.

Centralized Device Management

Early VPN deployments had no centralized network management capabilities, which made managing growing networks a time consuming prospect. With new management capabilities, enterprises can better manage large networks as a single entity rather than hundreds or thousands of discrete elements. In dynamically assigned IP address environments, centralized management capabilities are vital for supporting continued, ongoing policy management.

Policy Management

Initial deployments using IPSec VPNs were tedious to configure because there were no policy management capabilities. Each device had to be manually configured using its terminal. As upgrades became available for software/firmware, each had to be installed individually in every network element. End-users were added/deleted/changed one user at a time. Today management systems include user-friendly policy wizards that can be used to define different user group or site profiles. For instance, group templates for the Accounting or Marketing or Engineering groups can be created since each group may require different levels of security. These templates can easily be applied to new users and added to the network, or as new sites are brought online. New configurations can also be pushed to remote sites easily.

Device Monitoring

The ability to cohesively monitor all VPN devices is vitally important for an enterprise. First, it is necessary when trying to diagnose a problem. VPN devices can be monitored for general performance as well as for more detailed parameters useful in determining more specifically what is/has caused problems. Without monitoring, it is virtually impossible to determine the level of performance and know what in the network is not working properly. Necessary data such as how long a device has been down can be captured with proper monitoring techniques.

Reporting

Early reporting capabilities were limited to voluminous log files from singular devices. Determining current performance was time consuming and often undertaken only if the performance was significantly degraded. Today's reporting capabilities summarize critical information in an easy-to-read and easy to manage format. This helps increase the level of security by quickly deciphering the information from the network devices.

One of the benefits that come from a combination of the improved management features is the viability of supporting true fully meshed IPSec VPNs. Without centralized management and policy management for users/sites, fully meshed VPNs would continue to be impractical due to the resources required to define and manage each singular endpoint and predefined interconnections. Until now, most enterprises elected the huband spoke approach for this reason. As enterprises look to utilize non-client-server applications such as Voice Over IP, mesh networks will be a necessity.

5.3.4.3 IPSec VPN Benefits

It has been common to compare IPSec VPNs with Frame Relay as these services have matured over the past few years. Certainly, Frame Relay has proven to be a robust networking solution for nearly a decade. But with today's IPSec VPN technology, the two types of networks can be considered to be on more equal footing than just a year ago.

Costs

The business case for IPSec VPNs has become much more competitive with Frame Relay, although in many cases the final comparison comes down to the network architecture and specific requirements for user support. For example, it is not practical to connect dial users directly to a Frame Relay network, but IPSec VPNs offer a cost-effective alternative for dial users. Similarly, small site-to-site networks, with only a few sites and no dial access requirements, may not benefit from IPSec VPNs. The bottom line is that the costs per mbps are coming closer and closer every day.

Security

Frame Relay has been accepted as a secure solution for site-to-site traffic due to the nature of its PVC connectivity. IPSec VPNs offer the same type of pre-defined connectivity as Frame Relay, but also with encryption. Encryption adds another layer of security to the overall network. Another level of security can be achieved through the implementing of an integrated solution. Integrated solutions combine the firewall and VPN functionality into one device versus having separate devices for

each. This integration enhances the overall level of network security and provides the enterprise with many benefits such as not having to pass unencrypted data to or from the firewall, easier management and better reporting.

Performance

VPNs have largely been non-rate limited, which during peak traffic times could result in spotty performance. With today's IPSec VPN traffic shaping capabilities, this is no longer the case. Also, Frame Relay networks have been limited by standards definitions topping out at DS-3 connection. Conceivably, IPSec VPNs connections will grow in step with Ethernet—fast Ethernet and Gigabit Ethernet, with 10 Gigabit Ethernet on the way—as user demands dictate. Lastly, the dynamic routing capabilities mentioned earlier will increase reliability and performance by enabling dual ISPs and/or utilizing redundant CPE configurations.

Management

IPSec VPN management has surpassed Frame Relay management capabilities by incorporating policy management into configuration and update activities.

Complexity

Initially IPSec VPNs were considered to be more complex than Frame Relay. Tunneling, authentication, encryption, firewalls, and security—these were all new aspects that were required to secure an IP network. With the improvements in management and ease of use, much of the earlier complexity of IPSec VPNs

disappears. With the simplicity and efficiencies afforded by centralized management and policy management, IPSec VPNs become far less complex to install and manage than large Frame Relay networks. IPSec VPNs can support integrated networks – Internet, remote access, corporate intranet, and also business extranets. While Frame Relay works fine for site-to-site networks, implementing fully meshed networks is not practical, especially for large or growing networks.

Flexibility

Finally, with policy management support, IPSec VPNs gain a level of flexibility not practical with today's Frame Relay networks. Changing user privileges for network access is simple. Also by taking on some of the configuration and management of the IPSec VPN, the network manager gains a margin of independence from the service provider.

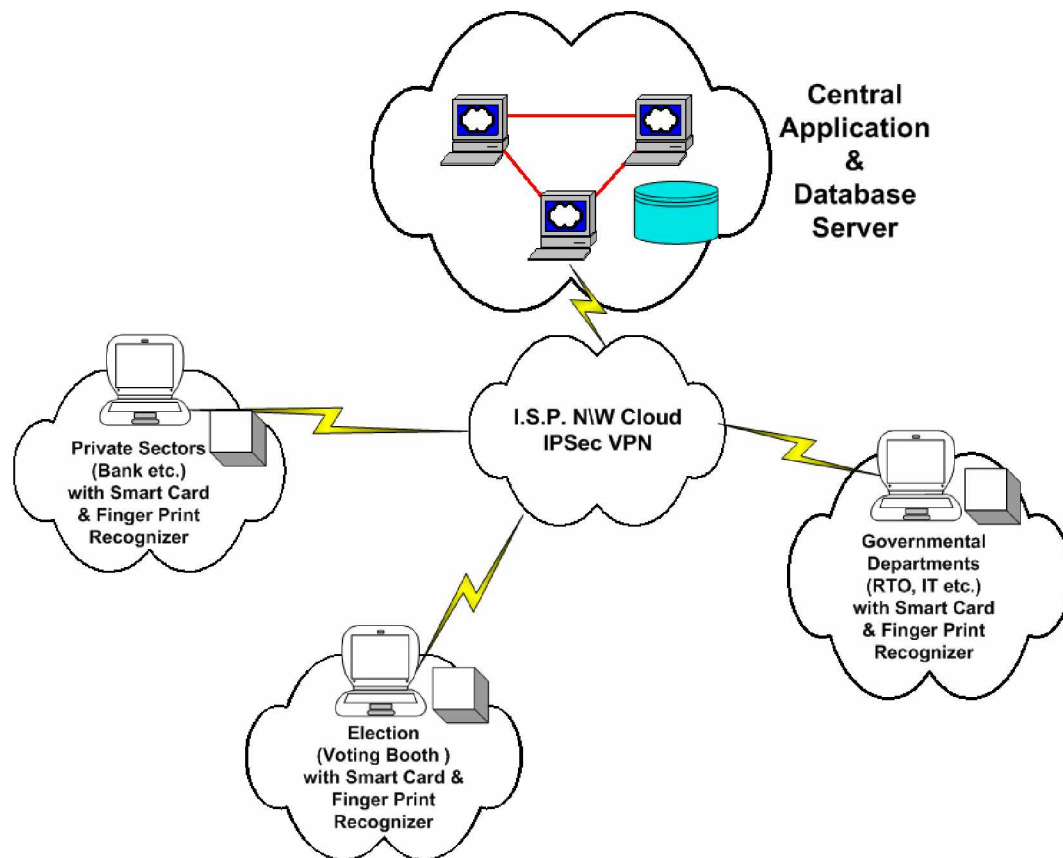


Figure: 5.14 IPSec VPN Solution for the entire system

IPSec is a thorough and complete solution for protecting IP traffic. IPSec protects all traffic against unauthorized modification and eavesdropping, and also securely authenticates the communicating parties. The protocol is as strong as the underlying algorithms it employs, so proper algorithm selection is important to network security.

Regarding to election, the online authentication (of voter) and network connectivity form voting booth to centralized server; IPSec makes it possible to securely transmit information as a very cost-effective solution. IPSec does this in a manner completely transparent to the voters.

5.4 Development and implementation of the application with bio-smart card and generate the prototype that facilitates the e-Election.

Indian government has already facilitated the elections with EVMs that is discussed in chapter-2. But there are some challenges against the government to make the election safer and swifter:

- Main challenge is to stop the illegal voting.
- More man power as well as money is used to conduct the elections.
- It is not paperless election because every time the government has to prepare and dispatch the voter list in hard copies to the related voting booth.
- Polling officers have to check the voter's identity, which is time consuming.
- There might be such problems can happen also that the voter has the ID-proof but he/she cannot vote, because his/her name is not in the voter list.
- Certain voters can only vote in certain voting booths, any voter cannot vote in any voting booth. If voter is in other city he/she cannot vote in that city because his/her name is not in that city's voter list.

Because of these reasons such a system is required, which can overcome the current manual election system. Here I have

tried to design and generate a prototype over current election system with the help of unique identity smart card (Bio-Smart Card).

This system contains one central database, where all the details of the citizen are to be stored. It will generate the unique identity number (CIN) of the citizen. Any governmental department or private sector can access this central database in restricted manner.

5.4.1 Server and Client configuration for the system

- Server Configuration

- Hardware

- § Intel Pentium – IV 2.4 GHz or higher Processor

- § 512 MB RAM

- § 360 GB HDD

- § Gigabit Ethernet Card

- Operating System

- § Microsoft Windows 2003 Enterprise edition

- Software

- § Oracle 9i Server

- § VPN Application Server

- Client Configuration

- Hardware (*minimum requirement)

- § Intel Pentium – I 200 MHz or higher Processor*

- § 32 MB RAM

- § 4 GB HDD

- § Ethernet Card

- § USB Support (for the Bio-Smart Card device)

* Minimum requirement of hardware to utilize the current resources

- Operating System
 - § Windows 9x
- Software
 - § Oracle 9i Client
 - § VPN Client
- Configuration of Hardware-Software for development of the Entire System
 - Server Configuration
 - § Hardware
 - Intel Pentium – IV 2.4 GHz Processor
 - 256 MB RAM
 - USB Support
 - Ethernet Card
 - § Software
 - Microsoft Windows 2003 Enterprise Edition
 - Oracle 9i database server
 - Client Configuration
 - § Hardware
 - Intel Pentium – IV 2.4 GHz Processor
 - 256 MB RAM
 - USB Support
 - Ethernet Card

§ Software

- Microsoft Windows XP
- Oracle 9i Client
- Microsoft Visual Basic 6.0

o Network Connectivity

§ Ethernet Switch is used to perform the Client – Server connectivity.

5.4.2 Network Architecture for the System

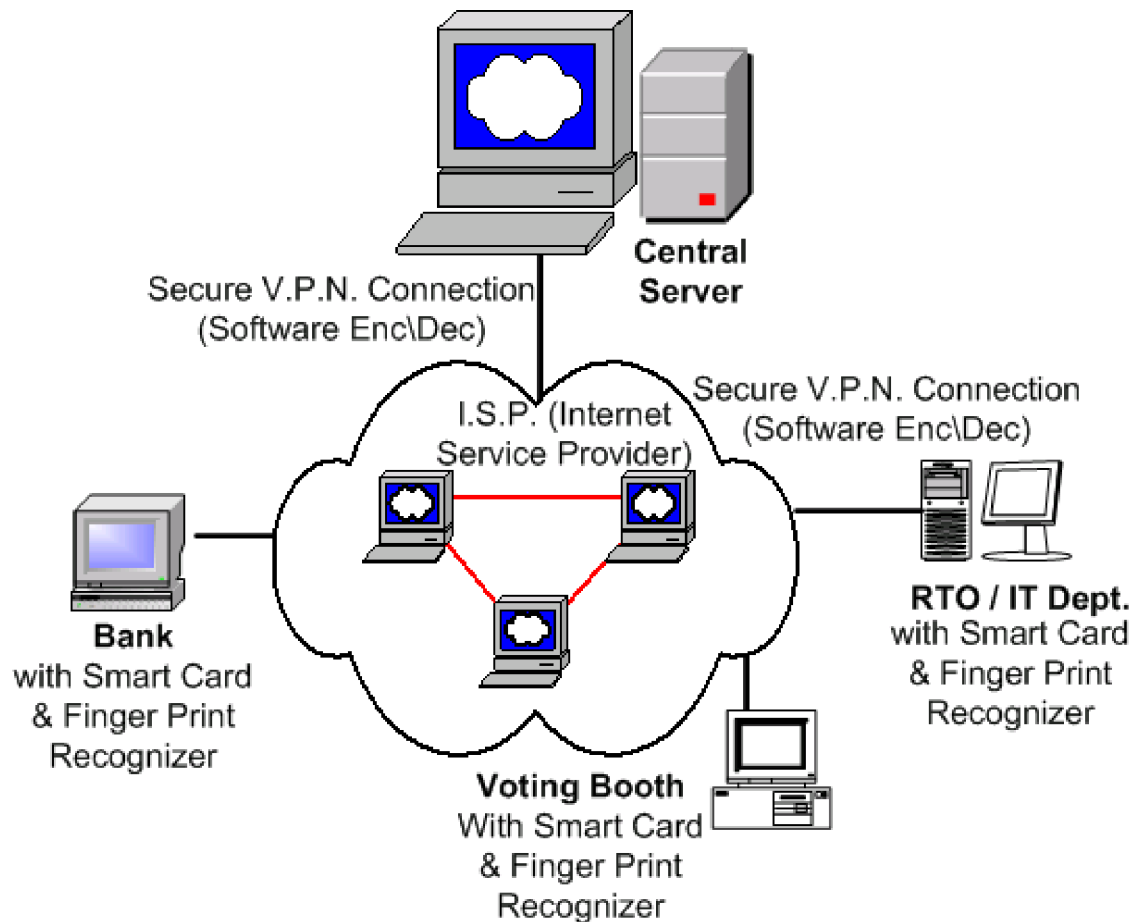


Figure: 5.15 System Architecture

For entire system network connectivity would be taken from any Internet Service Provider and from which the Server can be accessed to the entire clients of the system.

Hence the network is over the Internet to stop any outside interference to entire network the IPsec – VPN solution or entire governmental network like GSWAN can be used to

perform the client – server communication (as discussed in topics 5.2 and 5.3 of this chapter).

Here in this model application two departments from government (RTO, Income Tax) and bank as private sector are taken in for consideration.

RTO department can access the details of the citizen to view or inquire only, and then RTO can give the license to the citizen according to their rules and regulations. The Income tax department and Bank can do the same. With this system citizen carries only one as driving license/PAN card/Bank Card rather than to carry multiple cards.

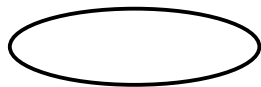
In the elections citizen can vote only one time from any voting booth in any city.

5.4.3 Life Cycle Model of the System

- a) Data Flowcharts
- b) Database Tables
- c) System Modules: Design and Description

a) Data Flowchart

Symbol Description



Shows the database table name



Shows the Processing elements



Shows the data flow point



Shows Report activity

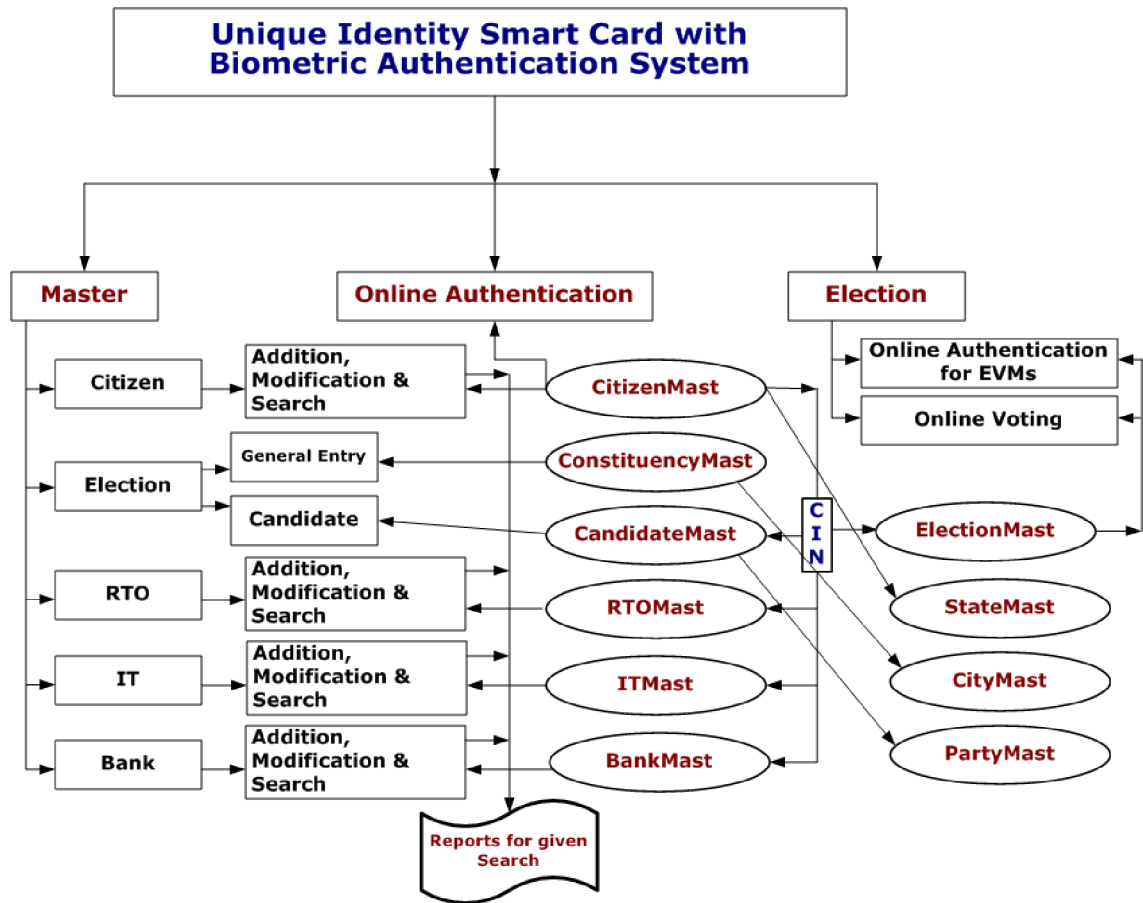


Figure: 5.16 Dataflow Chart of System

b) Database Design

The system has following database tables:

CITIZENMAST	for all the details of the citizen
STATEMAST	Master table for the States of India
CITYMAST	Master table for the Cities of State
CONSTIMAST	Master table of Constituency for Election
PARTYMAST	Master table for political parties registered for the Elections

RTOMAST	for the RTO department
ITMAST	for the Income Tax department
BANKMAST	for any bank
ELECTIONMAST	for online authentication for voting in Election
USERMAST	Master Table of Users and Login Passwords for the application

Among all these tables the unique primary key is CIN (Citizen Identity Number) and that is generated by application automatically. If there is no CIN in CitizenMast any other record cannot be inserted in to the other its related table.

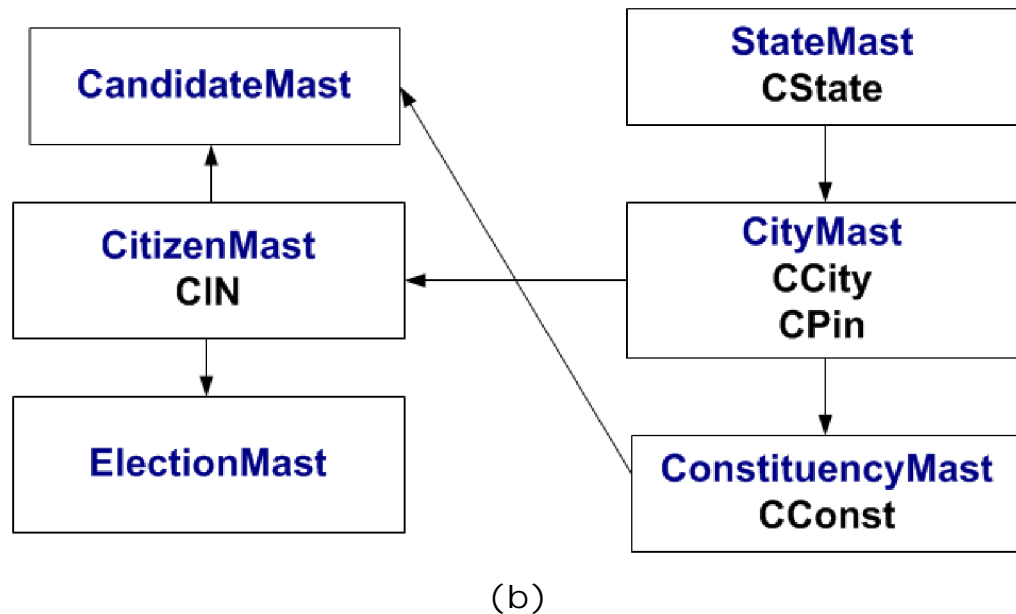
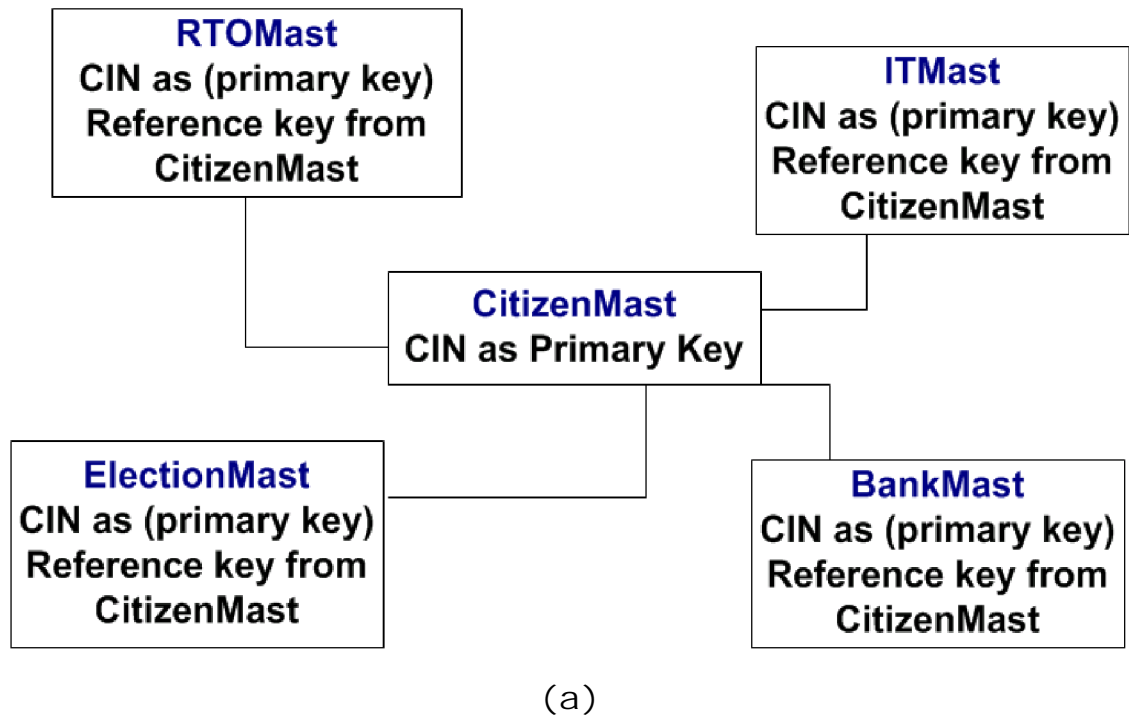


Figure: 5.17(a, b) Database Architecture

CitizenMast Table

Field Name	Field Type with Constraints	Description
CIN	Varchar2 (15) Primary key Not Null	Citizen Identity Number
CFName	Varchar2 (40) Not Null	First Name of the Citizen
CSName	Varchar2 (40) Not Null	Second Name of the Citizen
CLName	Varchar2 (40) Not Null	Last Name of the Citizen
CAdd1	Varchar2 (45) Not Null	Address of the Citizen
CAdd2	Varchar2 (45)	Address of the Citizen
CAdd3	Varchar2 (45)	Address of the Citizen
CCity	Varchar2 (50) Not Null	City of the Citizen
CTal	Varchar2 (50) Not Null	Related Taluka Place to City
CDist	Varchar2 (50) Not Null	Related District Place to City
CPin	Varchar2 (6) Not Null	Pin code of the City
CState	References StateMast (CState)	

CBDate	Date Not Null	Birth date of the Citizen
CPhone	Varchar2 (15)	Phone Number
CMob	Varchar2 (10)	Mobile Number
CEmail	Varchar2 (50)	E-Mail ID
CISDate	Date Not Null	Citizen Card Issue Date
CIXDate	Date Not Null	Citizen Card Expiry Date
CBGrp	Varchar2 (12) Not Null	Blood group of the Citizen
CSex	Number (1) Check (CSex = 0 or CSex=1)	Sex of the Citizen (1 for Male & 0 for Female)
CImg	BLOB	Citizen's Photo Image
CImgLn	LONG	Image Length

StateMast Table

Field Name	Field Type with Constraints	Description
CSCODE	Number Not Null, Unique	State Code
CSTATE	Varchar2 (50) Not Null, Unique	Name of the State

CityMast Table

Field Name	Field Type with Constraints	Description
CPIN	Varchar2 (6) Not Null	Pin code of the City
CCITY	Varchar2 (50) Not Null	City Name
CTALUKA	Varchar2 (50) Not Null	Taluka of the City
CDIST	Varchar2 (50) Not Null	District of the City
CSTATE	References StateMast CState)	State of the City

RTOMast Table

Field Name	Field Type with Constraints	Description
CIN	Varchar2 (15) References citizenmast (CIN)	Citizen Identity Number With reference from Citizenmast Table
ValFrm	Date Not Null	License Valid From Date
ValTo	Date Not Null	License Valid To Date
ValTFrm	Date	License for Transport Vehicle Valid From Date
ValTTo	Date	License for Transport Vehicle Valid To Date
ValDrv	Varchar2 (60) Not Null	License Type (License to Drive)
IssDate	Date Not Null	License Issue Date
DLN	Varchar2 (15) Not Null	Driving License Number

ITMast Table

Field Name	Field Type with Constraints	Description
CIN	Varchar2 (15) references citizenmast (CIN)	Citizen Identity Number with reference from Citizenmast Table
PAN	Varchar2 (15) Not Null unique	Personal Account Number
ISSDATE	Date Not Null	PAN Issue Date

Bankmast Table

Field Name	Field Type with Constraints	Description
CIN	Varchar2 (15) References citizenmast (CIN)	Citizen Identity Number with reference from Citizenmast Table
AccNo	Varchar2 (16) Not Null	Citizen's Account Number with the Bank
AccType	Varchar2 (30) Not Null	Account Type
AcIsDate	Date, Not Null	Account Issue Date

PartyMast

Field Name	Field Type with Constraints	Description
	Number	Code for Party
PARTYCODE	Not Null, Unique	
	Varchar2 (60)	Name of the Party
PARTYNAME	Not Null	
CSYMB	BLOB	Party Symbol
CSYMBLN	LONG	Length of the Symbol

ConstituencyMast Table

Field Name	Field Type with Constraints	Description
CCONST	Varchar2 (50)	Constituency
	Not Null	Name
CSTATE	Varchar2 (50)	State of the
	Not Null	Constituency
CPIN	BLOB	Pin code of
		Constituency

ElectionMast Table

Field Name	Field Type with Constraints	Description
CIN	Varchar2 (15) References citizenmast (CIN)	Citizen Identity Number with reference from Citizenmast Table
Voted	Number (1) Check (voted=1 or voted=0)	To Check whether Citizen voted or not. (1 for Voted and 0 for Not Voted)
VDate	Date Not Null	Voting Date
Votedto	Varchar2 (65)	Vote to Candidate (CIN of the Candidate along with the constituency is to be Stored)

UserMast Table

Field Name	Field Type with Constraints	Description
UNAME	Varchar2 (50) Not Null	User Name
UPWD	Varchar2 (50) Not Null	Password of the User
UGRP	Varchar2 (50) Not Null	Group of the User

c) System Modules

Form Description and Design (Module wise)

1. Login Screen

It is the general authentication for users of the application, specific users can only access the specific modules (i.e. user of the RTO group can only access the module related to RTO Department). Only Administrator will get the over all rights to access the entire application.

Unique Identity Smart Card with Biometric Authentication System

User Name: administrator

Password: *****

Group: ADMIN

OK **Cancel**

Guide
Dr. N.N. Jani
Prof & Head

Research Scholar
Dhaval R. Kathiriya

Department of Computer Science, Saurashtra University - Rajkot

Figure: 5.18 Login Screen

2. Main Screen

This is the main screen of the application from which the different modules can be accessed.

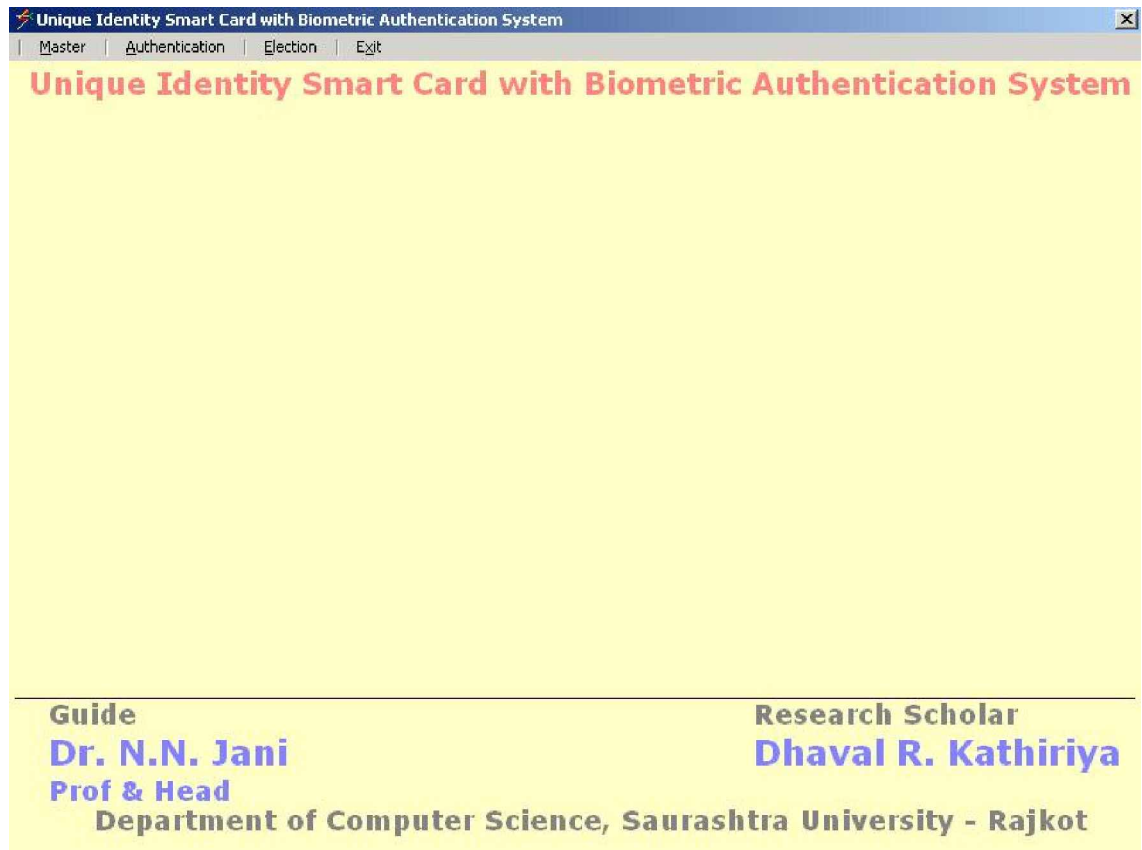


Figure: 5.19 Main Screen

3. Citizen Module

From this module the Unique Identity Smart Card can be issued and for this several entries are required to enter. Citizen Identity Number (CIN) will be automatically generated. Once the “Save” button is pressed and it will also ask for the fingerprint of the citizen to whom the card is to be issued, and then it will also ask the photo image of the citizen.

Unique Identity Smart Card with Biometric Authentication System

Master | Authentication | Election | Exit

Citizen ▾ Add Ctrl+A
Election ▾ Edit Ctrl+E
RTO ▾ Search Ctrl+S
IT ▾
Bank ▾

Smart Card with Biometric Authentication System

Enrollment of Citizen

☐ Male ☐ Female State

Citizen Identity Number (CIN)

First Name Second Name Last Name

Address Pin Code 360002 City RAJKOT

 Taluka RAJKOT District RAJKOT

Phone Mobile E-Mail

Birth Date Blood Group Card Issue Date Card Exp. Date

Save **Exit**

Figure: 5.20 Citizen Module (Add Mode)

It also serves the facility like Modification, Search and Reports also. (City or State wise reports are in html format)

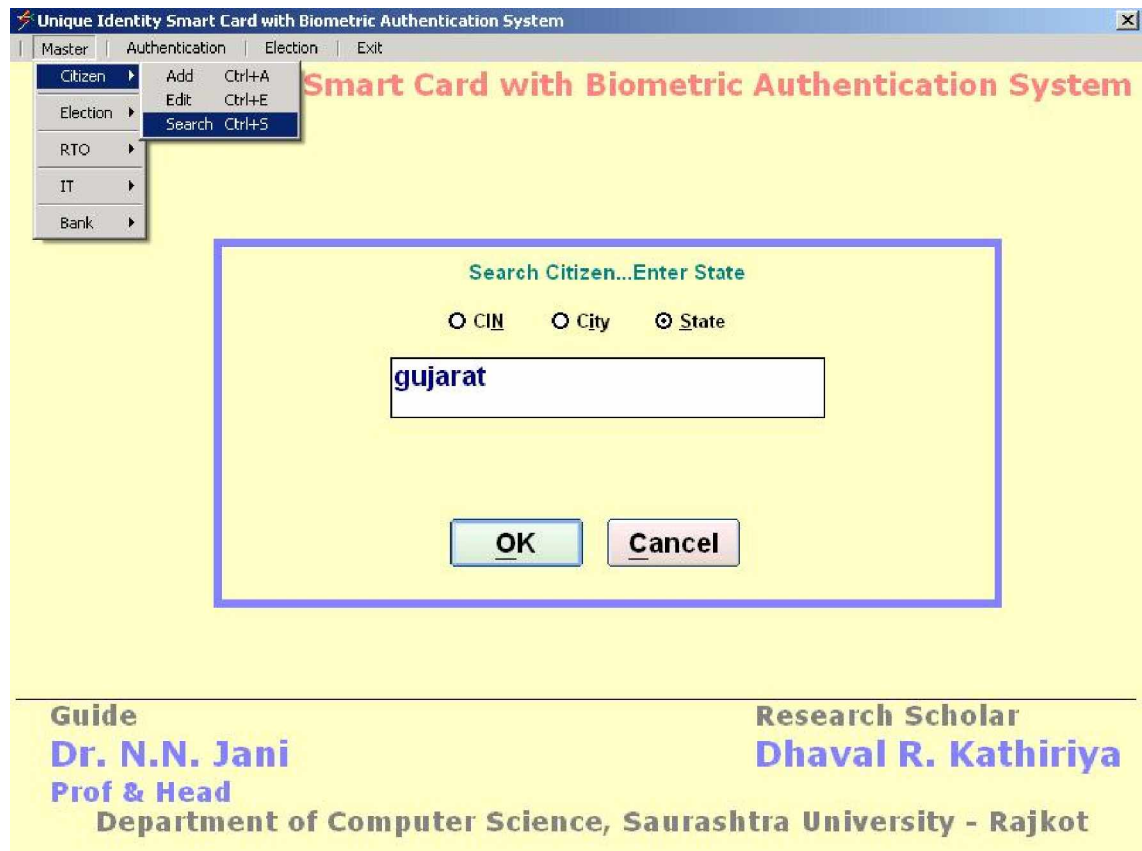
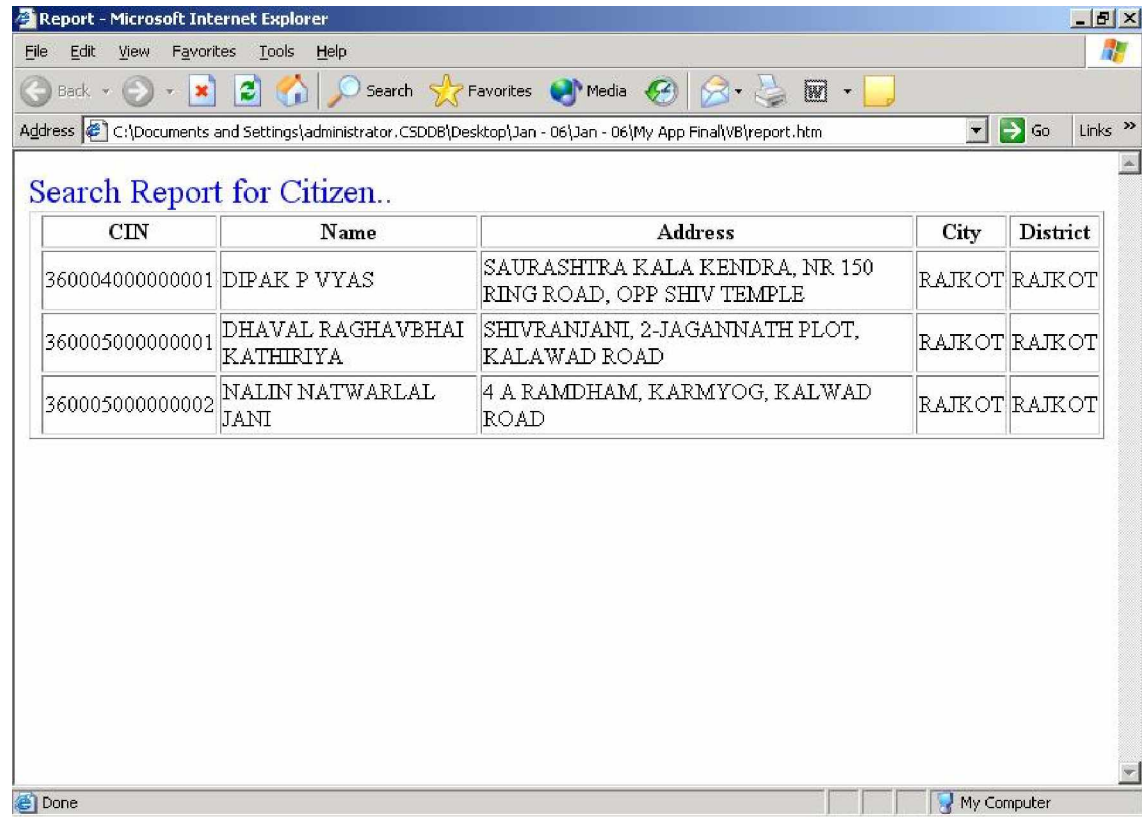


Figure: 5.21 Citizen Module (Search Mode)

If the given search value is valid and in the database it will show the report in the HTML format. When the application ends the report file will automatically deleted.



Search Report for Citizen..

CIN	Name	Address	City	District
360004000000001	DIPAK P VYAS	SAURASHTRA KALA KENDRA, NR 150 RING ROAD, OPP SHIV TEMPLE	RAJKOT	RAJKOT
360005000000001	DHAVAL RAGHAVBHAI KATHIRIYA	SHIVRANJANI, 2-JAGANNATH PLOT, KALAWAD ROAD	RAJKOT	RAJKOT
360005000000002	NALIN NATWARLAL JANI	4 A RAMDHAM, KARMYOG, KALWAD ROAD	RAJKOT	RAJKOT

Figure: 5.22 Citizen Module (Report)

4. Election Module for Candidate and general entry

General Entry like State, City, Constituency and Political party for registration to election commission can be done from this module.

Unique Identity Smart Card with Biometric Authentication System

Master | Authentication | Election | Exit

Citizen | Election | RTO | IT | Bank

Identity Smart Card with Biometric Authentication System

Add New

☐ State ☐ City ☒ Contituency ☐ Party

State Name: GUJARAT

Constituency Name: 360002

RAJKOT

Save **Exit**

Guide
Dr. N.N. Jani
Prof & Head
Department of Computer Science, Saurashtra University - Rajkot

Research Scholar
Dhaval R. Kathiriya

Figure: 5.23 Election Module (General Entry)


Candidate's registration for the election can be done online from this module. First it will authenticate the candidate from the Bio-Smart Card device and then display the following screen.

Unique Identity Smart Card with Biometric Authentication System

Master | Authentication | Election | Exit

Election: Candidate Entry for Constituency

Election Symbol

 Citizen Identity Number (CIN) ☐ Female

State Pin Code

Constituency Party

First Name	Second Name	Last Name
DHAVAL	RAGHAVBHAI	KATHIRIYA

Address	City	Pin Code
SHIVRANJANI	RAJKOT	360005
2 JAGANNATH PLOT	Taluka	District
KALAWAD ROAD	RAJKOT	RAJKOT
		State
		GUJARAT

Phone	Mobile	E-Mail
02812577394	9427289085	DRKATHIRIYA@YAHOO.COM

Blood Group	Birth Date
05/07/1979	O + VE

Department of Computer Science, Saurashtra University - Rajkot

Figure: 5.24 Election Module (Candidate Entry)

5. RTO Module

This module is for RTO department to issue the driving license to the citizen. It will ask the CIN of the citizen to add record/issue the license.

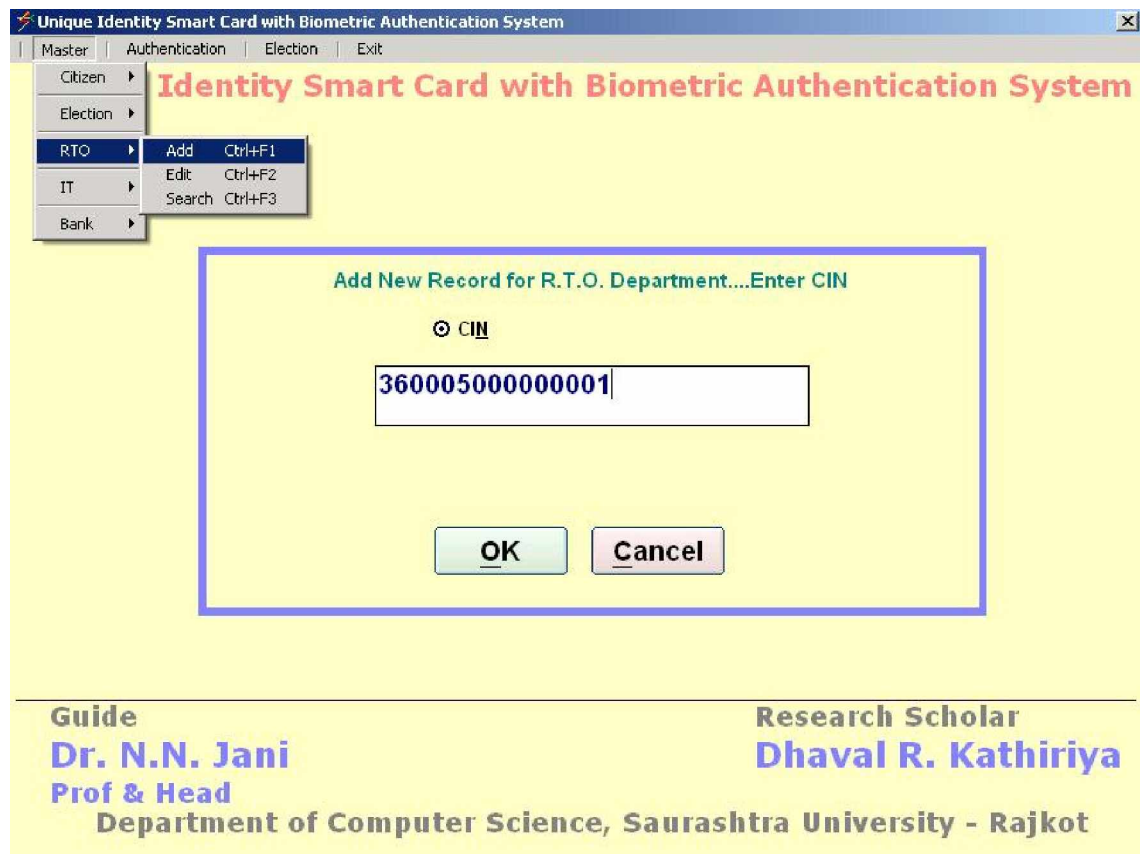
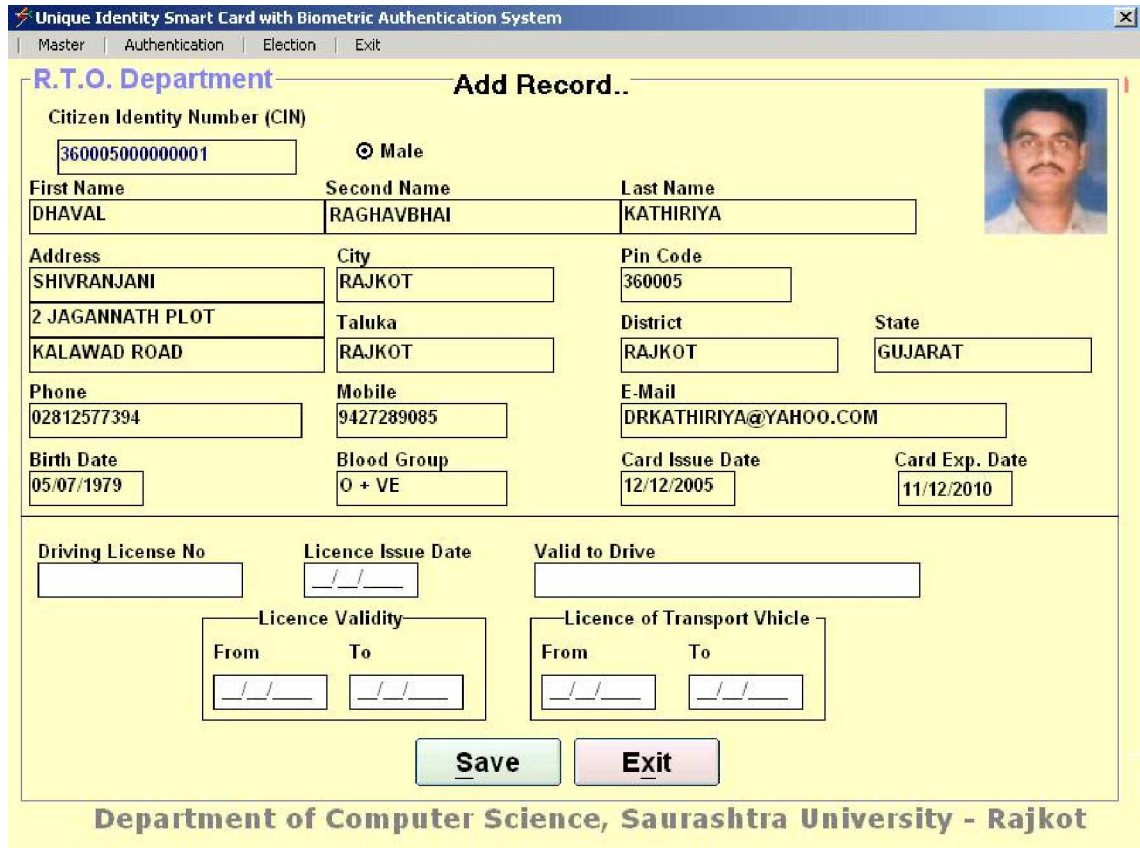


Figure: 5.25 RTO Module (Add Record – CIN Entry)

If the given CIN is true then it will display the full detail of the Citizen. RTO group user can only add the details related to license. This module covers the Modification; Search and Reports facility to RTO related records.



Unique Identity Smart Card with Biometric Authentication System

Master | Authentication | Election | Exit

R.T.O. Department **Add Record..**

Citizen Identity Number (CIN)
360005000000001

☒ Male

First Name: DHAVAL Second Name: RAGHAVBHAI Last Name: KATHIRIYA

Address: SHIVRANJANI City: RAJKOT Pin Code: 360005
2 JAGANNATH PLOT Taluka: RAJKOT District: RAJKOT State: GUJARAT
KALAWAD ROAD

Phone: 02812577394 Mobile: 9427289085 E-Mail: DRKATHIRIYA@YAHOO.COM

Birth Date: 05/07/1979 Blood Group: O + VE Card Issue Date: 12/12/2005 Card Exp. Date: 11/12/2010

Driving License No: Licence Issue Date: Valid to Drive:

Licence Validity: From: To: Licence of Transport Vehicle: From: To:

Save **Exit**

Department of Computer Science, Saurashtra University - Rajkot

Figure: 5.26 RTO Module (License Detail Entry)

Search record of R.T.O. Department....Enter CIN

☒ CIN ☐ City ☐ State


380014000000001

Figure: 5.27 RTO Module (Search by CIN)

R.T.O. Department Search for: gj/01/256213498

Citizen Identity Number (CIN)
 ☒ Male

First Name MAHESH	Second Name M	Last Name MERAMAN
Address PANCHVATI APT NR ALFRED PLAZA PALDI	City AHMEDABAD Taluka AHMEDABAD	Pin Code 380014 District AHMEDABAD State GUJARAT
Phone 0792568235912	Mobile 9825679178	E-Mail MMMERAMAN@GMAIL.COM
Birth Date 05/01/1980	Blood Group B + VE	Card Issue Date 30/12/2005 Card Exp. Date 29/12/2010



Driving License No gj/01/256213498	Licence Issue Date 18/06/2004	Valid to Drive MC, HMV
Licence Validity From: 18/06/2004 To: 17/06/2014		Licence of Transport Vhicle From: 18/06/2004 To: 17/06/2010

Figure: 5.28 RTO Module (Search Mode)

6. IT Module

This module is for ITO department to issue the PAN to the citizen. It will ask the CIN of the citizen to add record/issue the PAN.

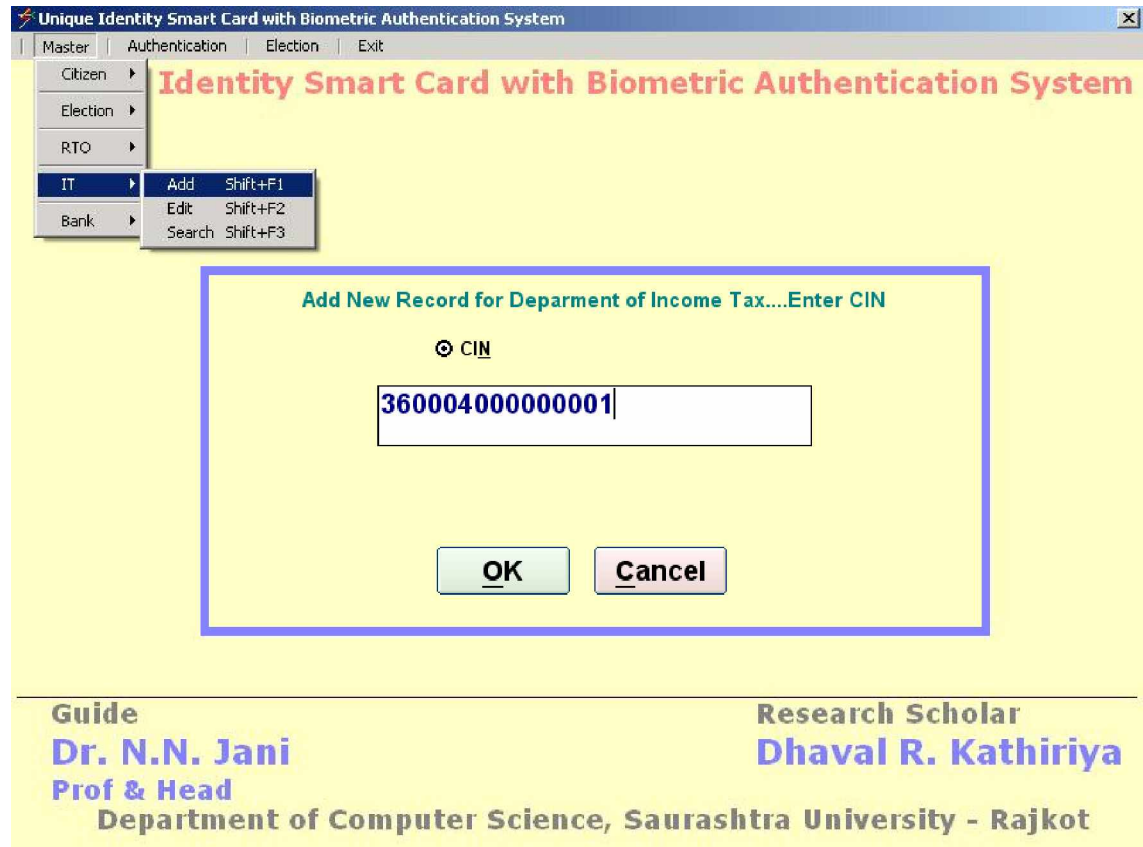



Figure: 5.29 IT Module (Add Record - CIN Entry)

If the given CIN is true then it will display the full detail of the Citizen. IT group user can only add the details related to PAN. This module covers the Modification; Search and Reports facility to IT related records.

Department of Income Tax — **New Record Saved...**

Citizen Identity Number (CIN)
 ☒ Male

First Name: Second Name: Last Name: 

Address: City: Pin Code:
 Taluka: District: State:

Phone: Mobile: E-Mail:

Birth Date: Blood Group: Card Issue Date: Card Exp. Date:

Personal Account No. - PAN: Issue Date:

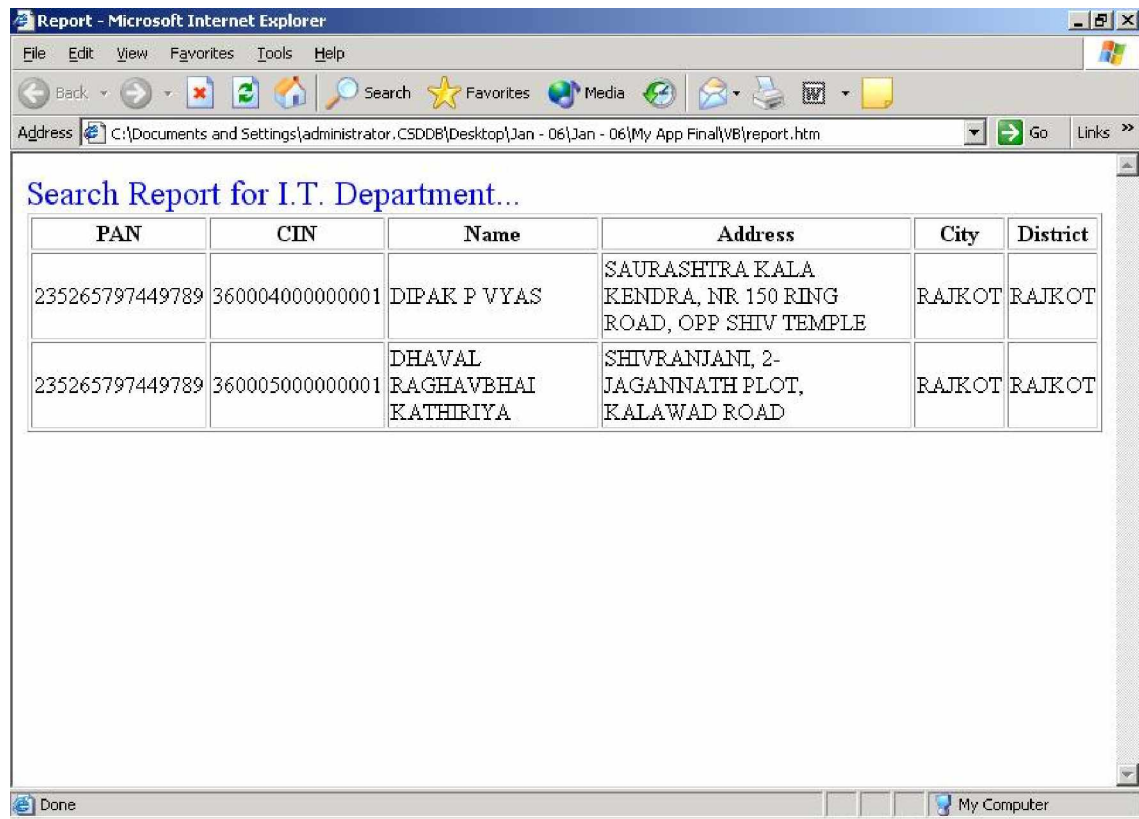
Figure: 5.30 IT Module (PAN Entry)

Search record of Department of Income Tax....Enter City

☐ CIN ☒ City ☐ State

Figure: 5.31 IT Module (Search Record by City)

If the given city is in the database it will show the report in the HTML format. When the application ends the report file will automatically deleted.



Search Report for I.T. Department...

PAN	CIN	Name	Address	City	District
235265797449789	360004000000001	DIPAK P VYAS	SAURASHTRA KALA KENDRA, NR 150 RING ROAD, OPP SHIV TEMPLE	RAJKOT	RAJKOT
235265797449789	360005000000001	DHAVAL RAGHAVBHAI KATHIRIYA	SHIVRANJANI, 2-JAGANNATH PLOT, KALAWAD ROAD	RAJKOT	RAJKOT

Figure: 5.32 IT Module (Report)

7. Bank Module

This module is for Bank to issue the Account to the citizen. It will ask the CIN of the citizen to add record/issue the account.

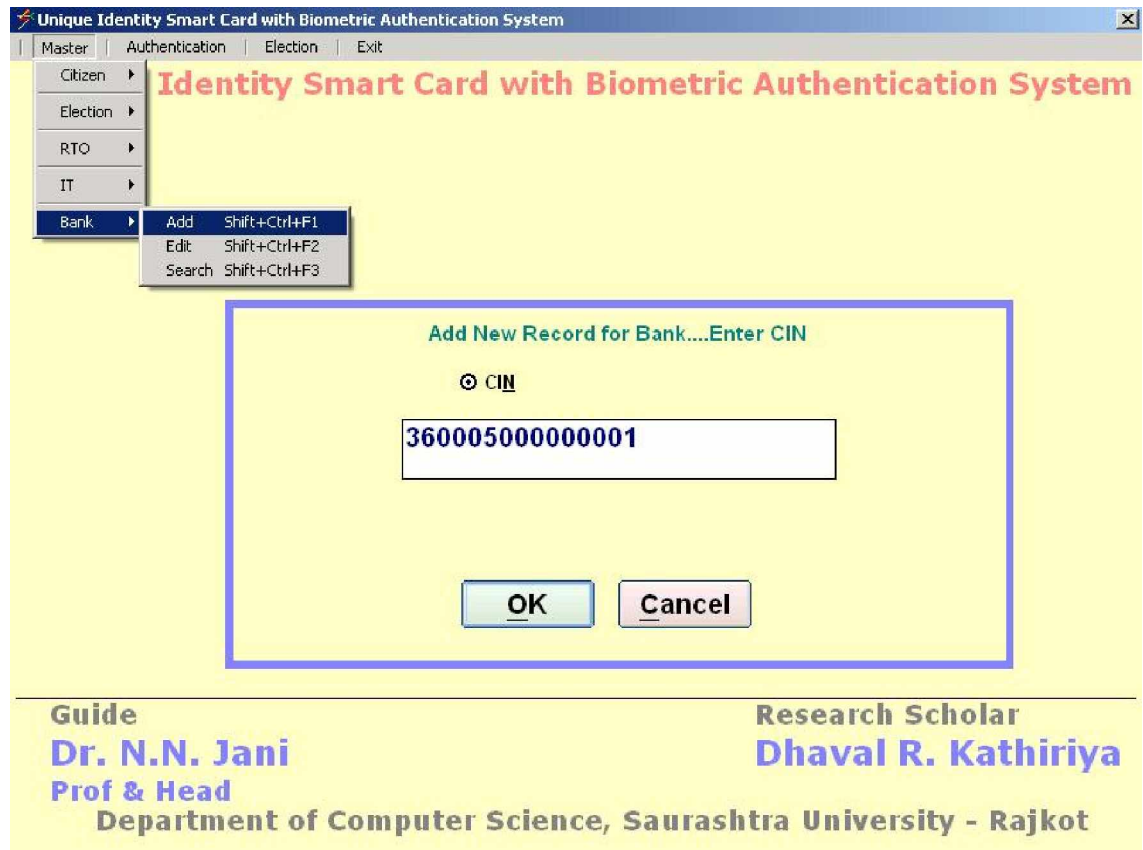


Figure: 5.33 Bank Module (CIN Entry)

If the given CIN is true then it will display the full detail of the Citizen. Bank group user can only add the details related to its account. This module covers the Modification; Search and Reports facility to Bank related records.

Unique Identity Smart Card with Biometric Authentication System

Master | Authentication | Election | Exit

Unique Identity Smart Card with Biometric Authentication System

Bank **Add Record..**

Citizen Identity Number (CIN)
360005000000001

☒ Male ☐ Female

First Name: DHAVAL Second Name: RAGHAVBHAI Last Name: KATHIRIYA

Address: SHIVRANJANI City: RAJKOT Pin Code: 360005
2 JAGANNATH PLOT Taluka: RAJKOT District: RAJKOT State: GUJARAT
KALAWAD ROAD

Phone: 02812577394 Mobile: 9427289085 E-Mail: DRKATHIRIYA@YAHOO.COM

Birth Date: 05/07/1979 Blood Group: O + VE Card Issue Date: 12/12/2005 Card Exp. Date: 11/12/2010

Account No: Account Issue Date: Account Type:

Save **Exit**

Department of Computer Science, Saurashtra University - Rajkot

Figure: 5.34 Bank Module (Account Entry)

Search record of Bank....Enter CIN

☒ CIN ☐ City ☐ State

365601000000002

Figure: 5.35 Bank Module (Search Record by CIN)

Bank **Search for : 5213245220000042**


Citizen Identity Number (CIN)

☒ Male

First Name NILESH	Second Name B	Last Name NAKUM
-----------------------------	-------------------------	---------------------------

Address AMBIKANAGAR	City AMRELI	Pin Code 365601
LATHI ROAD	Taluka AMRELI	District AMRELI
NR SCIENCE COLLEGE		State GUJARAT

Phone 0279223091	Mobile 9825258121	E-Mail N_NAKUM@REDIFFMAIL.COM
Birth Date 12/08/1978	Blood Group AB +	Card Issue Date 05/12/2005
		Card Exp. Date 04/12/2010



Account No 5213245220000042	Account Issue Date 09/08/2003	Account Type Savings
---------------------------------------	---	--------------------------------

Figure: 5.36 Bank Module (Display Record)

8. Authentication Module

Using this module user can verify the citizen. This module can be used for general purpose to authenticate the citizen for RTO, IT or Bank. After the success full authentication the entry can be done for related group.

First citizen card has to be inserted in the device and then the following dialog appears the citizen will have to put the finger on the bio smart card device.

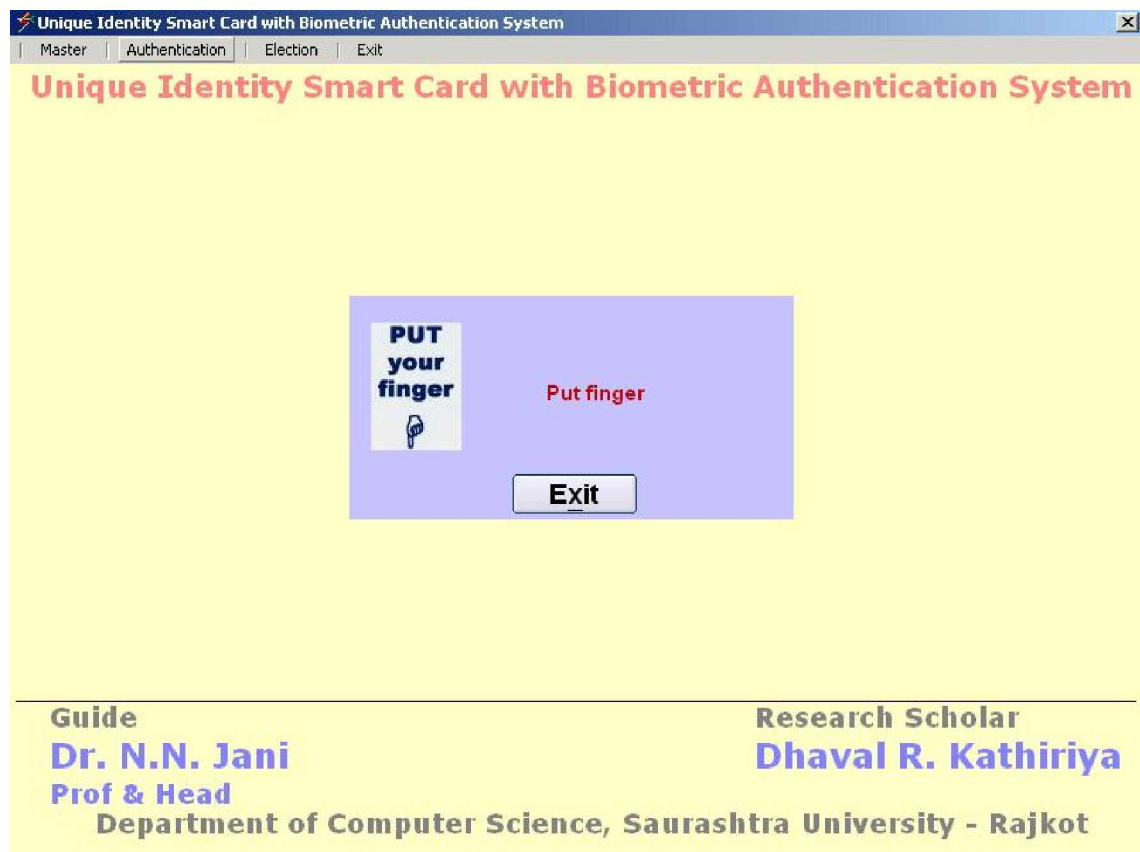


Figure: 5.37 Authentication Module


If the given fingerprint is true then the following screen will appear.

Authentication Successful...

Citizen Identity Number (CIN)
360004000000001

☒ Male ☐ Female

First Name	Second Name	Last Name	
DIPAK	P	VYAS	



Address	City	Pin Code	
SAURASHTRA KALA KENDRA	RAJKOT	360004	
NR 150 RING ROAD	Taluka	District	State
OPP SHIV TEMPLE	RAJKOT	RAJKOT	GUJARAT

Phone	Mobile	E-Mail	
02812599356	9825614504	DPVYAS2000@YAHOO.COM	

Birth Date	Blood Group	Card Issue Date	Card Exp. Date
14/04/1962	A +	21/12/2005	20/12/2010

Exit

Figure: 5.38 Authentication Module (Display)

9. Election Module for Online Voting

This module is designed to authenticate the citizen for election and then citizen can vote online. It has two options first for EVMs where only online authentication is required and second for online voting where online authentication and voting both needed.

If the first option selected then the authenticated citizen can be allowed only one time to vote through EVM. The general dialog for authentication will appear after the citizen has inserted his card in to the device.

Between both cases the citizen is allowed to vote only once. If citizen is authenticated for EVM the he cannot vote Online or vice versa.

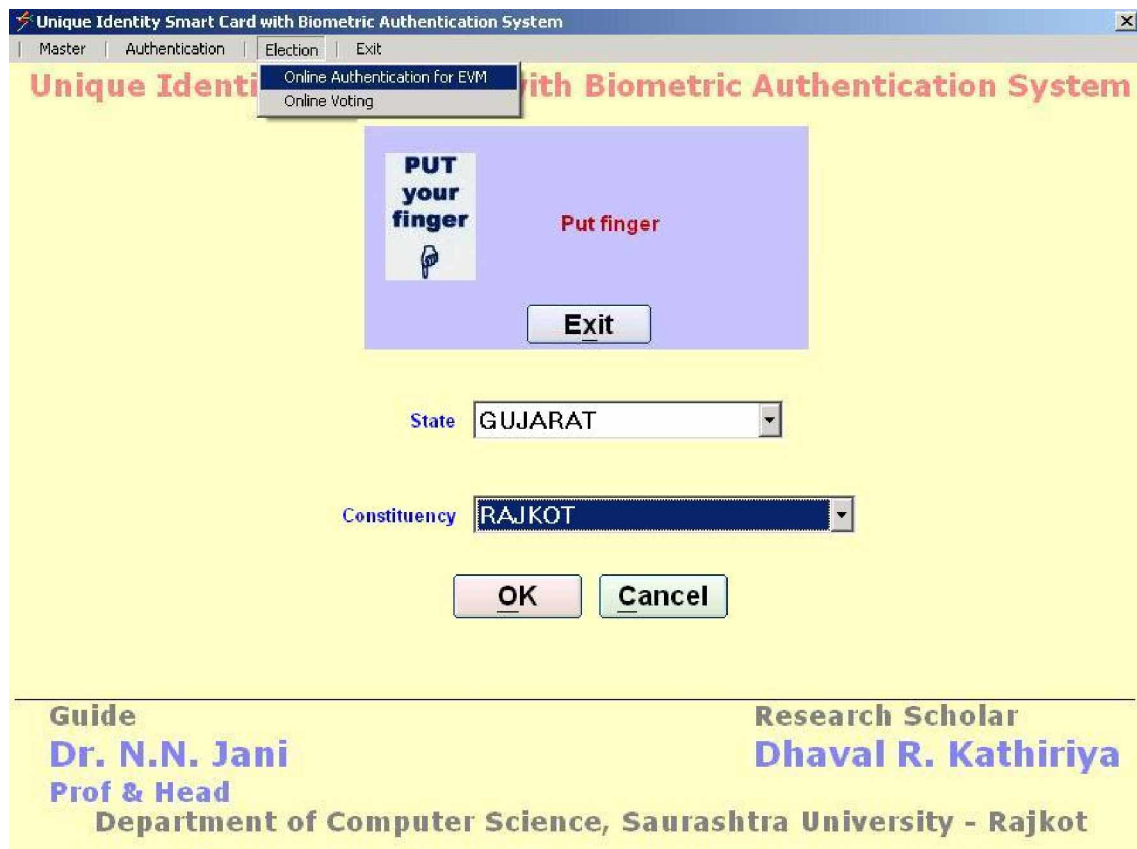


Figure: 5.39
Election Module (Online Authentication for EVM)

If the second option "Online Voting" is selected then if the authentication of the citizen is successful then following screen will appear.

The list of the candidates (related to the election constituency) will be displayed after their election symbol. Citizen can vote online by selecting the desired candidate. The screen will be disappeared once the citizen has selected the particular option.



Figure: 5.40 Election Module (Online Voting)

5.4.4.1

Compare the process of voting through the modeled and prototyped system with voting system that uses EVMs

Following figure 5.42 shows the model layout of the current voting process of the election using the Electronic Voting Machines for a polling station.

As discussed in Chapter – 2, it requires minimum three polling officers, polling agents of the related parties, and one presiding officer. Voter is allowed to vote only from the fixed voting booth related to his/her area.

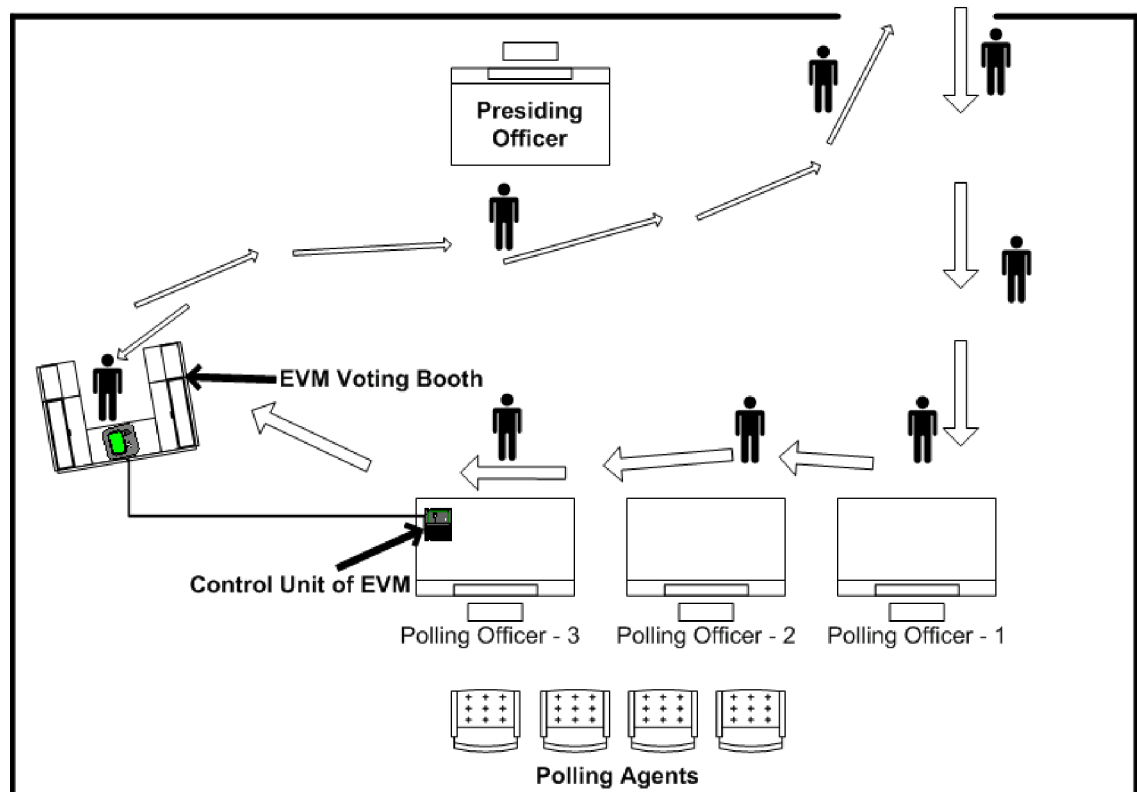


Figure: 5.42 Layout of EVM Polling Station

Figure 5.37 shows the proposed model layout for the polling station in which the focused system is used to vote the online.

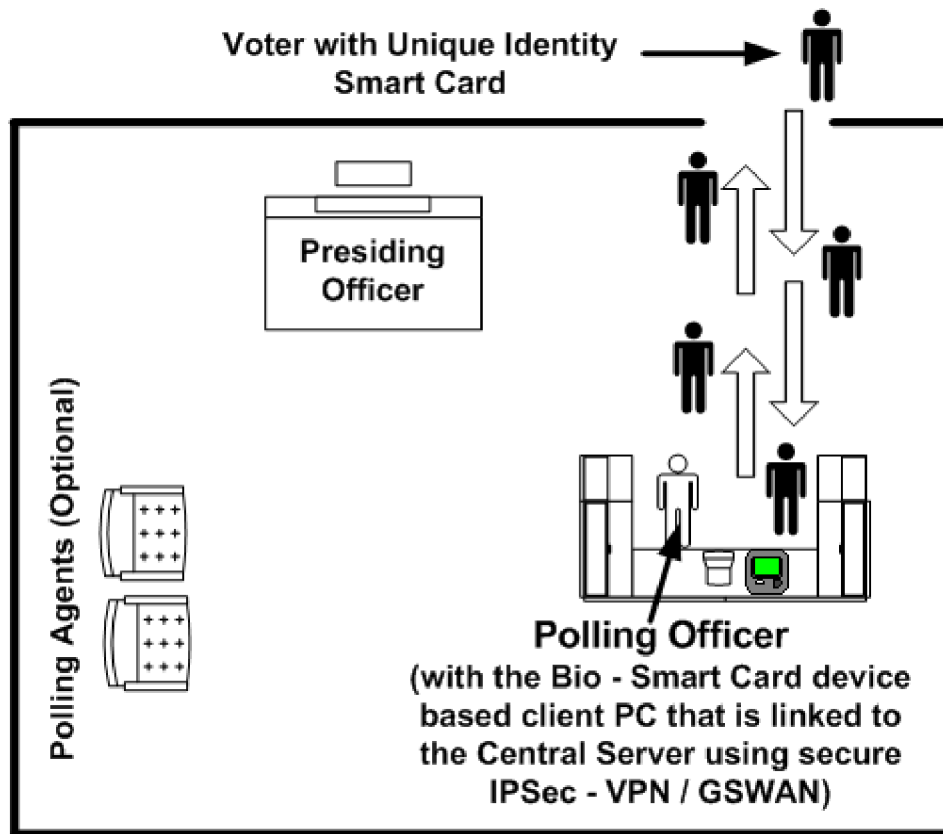


Figure: 5.37

Model Layout of polling station using the focused system
of Online Voting

In this proposed model only one polling officer is required. Presiding officer and polling agents could be made optional. This process is secure and does not require checking manually the multiple I-cards (one out of the approved) of the voters. The system automatically verifies the voter online by using the

voter's smart card and the fingerprint via the Bio-Smart card device that is attached to the PC. The polling officer has to only observe the authentication process of voter that is to be done online.

No one can cast illegal vote in this system. Voter can vote only once in a day of election from any voting booth. This model takes much less time for voting process than the voting process of the existing EVM based model.

5.4.4.2 Counting using the proposed model

The counting of votes using the EVMs is easier than the traditional counting through the ballot papers. But even with EVMs, there are some complications like after the voting, security and transportation of the EVMs up to the day of counting the votes is a critical issue for data protection.

For counting in the proposed model the administrator or the chief Election Commissioner has to fire only one query on the central server for each constituency. It is not necessary that at the central server itself the counting process be done. But at the different client end, with rights of administrator level the counting process could be done.

This election results could be declared within a few minutes. For example after the voting is over, counting can be distributed to every constituency or district place level, there should be a main administrator level person of the election

commission, who has all the rights for counting process in the related district place.

Footnote Reference:

- IPsec VPN Design,
Cisco Press Publication, (USA)
- End-to-End QoS Network Design,
Cisco Press Publication, (USA)
- CCSP Cisco Secure VPN Exam Certification Guide,
Cisco Press Publication, (USA)
- VPNs Illustrated: Tunnels, VPNs, and IPsec,
Addison Wesley Professional Publication, (USA)
- www.gujaratinformatics.com
- www.gswan.gov.in
- www.ssimail.com
- www.cisco.com
- www.microsoft.com
- www.vpnlabs.com
- www.networkworld.com

Research Outcome and Conclusion

This research has made exhaustive study of existing mechanisms adopted for the voting with partial automation. The study has concluded various challenges in the partial automated system of voting in the election system. The severe challenges are the time to preserve data on the device use at the voter end. The other challenges are not that critical are operating environment such as clean electric power to avoid accidental la functioning of the device. And sometimes even possibility of the data loss. This aspect is critical aspect to be taken care in such a mission critical application.

The focused research was to meet these challenges and deliver a flexible, safe & secure, enhancement of the automation to the possible extent. The research finding under the rigorous study and analysis of phases, situations and data has generated an model with a architecture which is implemented and the set goals are verified by a prototype working model of the system built around the available special devices and the software developed for effective implementation.

It would be a great benefit to the Citizens and the Government, if one single agency maintains all the personal details of the citizen and the citizen is required to intimate only to one agency for the change. All the agencies can access the database and maintain their local data always updated. All

state governments, local governments, other departments' can use this information for their purpose.

The outcome of this model, both government and citizens will get advantage to take and give services/information among each other. Citizen can easily update his/her details at any time from any where in the country; at the same time every governmental department will get his/her details. Government has to maintain only one database instead of maintaining many databases related to its departments. Smart card and biometric technology will give the ultimate security to maintaining the transactions with the Citizen Card.

Using this unique identity smart card based model, election could be very secure, trusted and swifter. This strategy of e-Governance would take less manpower, less time, and give more accurate and significant output to the system. It would be completely the paperless election. Using online authentication there would be the most reliable and secure way to identify the voter by his/her own unique biometric identity.

The process of counting the votes is very less than the current counting process for the votes from EVMs. Using this model, the election is online and data lying over the central server, the counting of votes could be done within a few minutes for a constituency.