CHAPTER-2

LITERATURE SURVEY

ANALYSIS OF ELECTRONIC VOTING SYSTEM IMPLEMENTED IN VARIOUS COUNTRIES

India is one of the world's largest democracies with a community of 1.1 billion; India has an electorate of 714 million persons over 828 thousands polling stations, 1.37 million voting machines and 5.5 million polling officials cover 543 parliamentary constituencies. Past experience of electoral process enforced us to focus on the use of latest technology in E-voting process. The current voting mechanism has many security problems, and it is very difficult to prove even simple security aspects about them. A voting system that can be demonstrated correct has many considerations. Some of the major concerns for a government regarding electronic voting systems are to expand election activities and to minimize the election expenses. Still there is some opportunity of work in electronic voting system in terms of authenticity of voters and to protect the electronic voting machine from offenders.

This chapter provides an overview of the experiences of other countries using electronic voting system. The comparative study on the adoption of electronic voting systems implemented at the international level is described in this chapter.

Rest of the chapter is organized as follows:

Section 2.1 presents the introduction followed by the definition of electronic voting in Section 2.2. International standard of electronic voting has been briefly given in Section 2.3 followed by the comparison of the features in different system in Section 2.4. Section 2.5 presents the comparative analysis of electronic voting systems and finally chapter has been summarized in Section 2.6.

2.1 INTRODUCTION

Electronic Voting Machine is a basic electronic machine that is used to store the votes in place of ballot papers and boxes which were used in traditional voting system [53]. It is a simple device that is operated smoothly by the polling officers and the voters. It is a single machine without any network connection, and nobody can hamper with its

programming and change the result. Keeping in mind the unpredictable power supply position in many areas in the country, the machines have been made to run on the simple batteries. EVM has only two main units: Control unit and Ballot unit. The main role of the Control Unit is to store all information and control the working of EVM. The solution which controls the operation of the control unit is written into a micro chip on a in a manner which can not be altered**..** Once it burn**,** cannot be read, replicate or modified. The EVM uses effective coding to increase security of data communicated from ballot unit to control unit. The recent EVM have also implemented real time clock and date-time facility which authorize them to record the real time and date whenever a key is pushed. When the voting is over and the close button is pushed, the machine does not receive any information or store any vote. With the pressing of "TOTAL" button, the control unit displays the total number of votes stored in the machine till that time which can also be verified with the manual register of voters. EVM display screen on control unit displays total number of votes recorded in at a polling station along with candidate-wise votes recorded in the machine when the 'RESULT' button is pushed by the counting officer in the presence of counting representative at the vote counting centre. The control unit also exposes any physical damaging made, if any, with the associating cable and communicate the same in the display unit.

As everybody watched the electoral situation occurred in Florida in 2000, people started wondering; "Wouldn't all our problems be solved if they just used E- Voting?" People all over the world soon started taking a hard look at their voting material and procedures, and trying to find out how to improve them [13]. There are many strong reasons for moving towards Remote Internet Voting like voter convenience, increase voter confidence and voter turnout. However, there are many serious technical and social issues that make Remote Internet Voting infeasible in the visible future. Therefore, many technologists have suggested that remote poll-site electronic voting, where the voter can vote at any poll-site seems to be the best step forward as it meets all requirements including convenience without compromising with security aspect in electoral process.

Electronic voting means the use of computer based equipments in an election to register ballots. In general, E-voting stands for a method where electronic systems are used in all phases of electoral process in including registration, vote cast, counting and results notification[24].

Manual elections are very expensive and time consuming. In previous manual elections in India, a nationwide ballot consumed thousands of tons of stationary paper including about 4 lacs phials of indelible ink and required about 3 million strongboxes to store them under heavy security until the votes were counted. In the past, it took up to three – four days to count the votes, with hired personnel spending day and night in secured areas manually counting each ballot. Sometimes demanding for repeat the counting resulting for the minimum margin difference of the votes between the top two candidates coupled with large number of invalid and uncertain votes.

The electronic voting machines are intended both to reduce errors and to speed up the counting process. Advantages of Electronic Voting Machine over the conventional ballot paper/ballot box system are

i. It removes the possibility of invalid and uncertain votes which, in many cases, are the root causes of dispute and election appeal.
ii. It makes the procedure of counting the votes much faster than the traditional system.
iii. It decreases to a great expanse the quantity of paper used so saving a large number of trees making the process eco-friendly.
iv. It minimized the cost of printing almost zero.

The Caltech/MIT Voting Technology Project [18] came into existence in order to develop a new voting technology in order to prevent a recurrence of the problems that threatened the 2000 U. S. Presidential Elections. The report assesses the magnitude of the problems, their root causes and how technology can reduce them. They address a wide range of "What is" issues including voting procedures, voting equipment, voter registration, polling places, absentee and early voting, ballot security, cost and public finance of elections, etc. Authors in [18] proposed a novel framework for voting technology to move away from monolithic voting structures. The framework is called "A Modular Voting Architecture ("Frogs")" [19, 20, 21] in which both the vote generation and vote casting has been proposed to be perform on separate systems. Framework "Frog" creates a permanent audit series to have better security. In this framework, machine used for vote casting is open- source whereas machine used for vote generation can be licensed or open-source.

In "Electronic Voting" [22], Rivest addresses some issues like the "secure platform problem" and the impossibility of giving a receipt to the voter. He also provides some personal opinions on a host of issues including the striking dissimilarity between e-commerce and e-voting, the dangers of adversaries performing automated, wide-scale attacks while voting from home, the need for extreme simplicity of voting equipment, the importance of audit-trails, support for disabled voters, security problems of absentee ballots, etc.

The NSF Internet Voting Report [23] addresses the feasibility of different forms of Internet voting from both the technical and social science perspectives, and defines a research agenda to pursue, if Internet voting is to be viable in the future. It groups Internet voting systems into three general categories as follows:

- ***Poll-site Internet voting:*** It offers the promise of greater satisfaction and effectiveness in that voter could cast their ballots from any poll site and the tallying process would be fast and definite. More importantly, since election officers would control the voting platform and the physical environment, managing the safety risks of such systems is reasonable.
- ***Kiosk voting:*** Voting machines would be located away from conventional polling places, in such convenient public places as malls, libraries, colleges or schools just like ATM . The voting platforms would still be under the supervision and full control of election officials. Physical environment could be modified by the election officials as per need to address security and privacy concerns and prevent any kind of outside interference or coercion.
- ***Remote Internet voting:*** It aims to maximize the percent of voting by maximizing the convenience and access of the voters to enable them to cast their votes from internet access with no restriction on geographical location. Concept of remote internet voting is very attractive and offers significant benefits by taking the advantages of ICT in electoral process provided security issues has to be addressed properly during framework design and implementation.

The report includes the feasibility of each of these categories and to provide research recommendations for the long-term future. It then identifies criteria for election systems. Finally, it addresses the technological issues (including voting system vulnerabilities,

reliability, testing, certification and standards, specifications of source code, platform compatibility, secrecy and non-coercibility, etc.) and social science issues (such as voter participation, voter access, the election process, voter information, deliberative and representative democracy, community and character of elections, distribution of roles, legal concerns, voter registration, etc.).

The California E- Voting Report [11] suggests a strategy of evolutionary comparatively revolutionary change towards completing the objective of providing voters with the possibility to register their ballots at anytime from anywhere via the Internet. The report defines four different Internet voting methods – Internet voting at voter's polling booth, Internet voting at any polling booth, Remote Internet voting from Country computers or kiosks, Remote Internet voting from any Internet connection – and the corresponding technical and design requirements that must be better when implementing any of the stages. It addresses the advantages, implementation and security issues of each of the four stages. They assured that supplementary technical changes are necessary before remote Internet voting can be implemented as a useful mechanism to improve contribution in the elections process and that current technology however would allow for the applications of new voting systems that in turn would allow voters to register a ballot over the Internet from a computer at any one of a number of county-controlled polling station. Finally, the report presents the findings and recommendations of the task force on policy issues [12].

An extensive survey of e-voting technology has been provided in "E-Voting Security Study" [34]. This study presents a survey on the projects in academic and commercial sector. It also identifies the various threats, potential sources of attack and possible methods of attack in such voting systems. Security objectives and major requirements of E-voting have been clearly specified in this work.

In [1], authors presented a mathematical framework for a secure election that involves an administrator, a counter and the voter connected by an anonymous channel. Practically focused projects build on the blind voting protocol. In [5], the use of unseeing signatures to certify that only enrolled voters can vote and that each enrolled voter votes only once, and at the same time maintain the privacy of voter's is implemented. It allows voters to validate separately that their votes were counted correctly and anonymously challenge the results, should their votes be miscounted.

Another project called E-VOX [6] at MIT implemented a simplified, user-friendly version of the FOO framework[1] using Java, Netscape and JDBC (Java Database Connectivity). This system is still involved in teaching and research and was used for an Undergraduates Association election at MIT in 1999. “Multiple Administrators for Electronic Voting” [7] improves this further by distributing the authority among multiple administrators to prevent vote forging.

“An untraceable, universally verifiable vote scheme” [4] presents a remote voting scheme that applies the technique of blinded signature to a voter's ballot so that it is difficult for everyone to detect the ballot back to the voter. They achieve the required properties of privacy, universal verifiability, convenience and untraceability, but at the expense of receipt-freeness.

The E-Poll (Electronic Polling System for Remote Voting Operations) project [40] investigates broadband mobile communications based on the UMTS standard for providing the E-Poll network with the required bandwidth and security. This makes it possible to use E-Poll kiosks anywhere, within a private, reliable and protected network. The voter-recognition system is based on an innovative smart card with an embedded biometric fingerprint reader, which performs voter recognition with absolute security.

In [10], authors presents a system for reliable electronic voting which does not depend on uninterrupted network connections between polling booth and the vote-tallying server. They build the system on a disconnected (or, more accurately, an intermittently connected) environment, which behaves well in the absence of network connectivity.

“Security Criteria for Electronic Voting” [2] considers some basic criteria for confidentiality, integrity, availability, reliability, and assurance for computer systems involved in electronic voting. After an assessment of the realizability of those criteria, it concludes that, operationally, many of the criteria are inherently unsatisfiable with any meaningful assurance.

In [28], Rubin identifies the new risks brought about by introducing the state-of-the-art technology into the election process, which may not be worth taking. The major security risks identified include those at the voting platform – including malicious payload (attack programs, remote administration and monitoring toolkits, etc.) and delivery mechanism (worms, viruses and bugs, active content downloaded automatically, etc.) – and the communications infrastructure – including (distributed) denial of service

attack, DNS server attack, etc. The security issues in social engineering and in using specialized devices are also identified.

Discussions on requirements, threat perceptions and socio-political issues regarding electronic voting can be found in [3, 25, 26, 27, 35].

Most of the people have dealt with e-commerce operations. This is already a part of everyday life. However, e-voting is not still a transparent method for voting. The construction of electronic voting system is one of the most challenging security-critical tasks, because of the requirement for detecting a trade-off between apparently conflicting safety requirements like privacy vs. audit ability. Thereby it is very difficult to adopt traditional methods of e-commerce. For example, in electronic commerce there is always a probability to discussion regarding the content of operations. Buyers obtain receipts to show their involvement in transactions. E-voters, in turn, must not obtain any receipts, because this would authorize voters to promote their votes.

In 2003, Estonia begins the project of electronic voting. The main focus was to apply electronic voting in the elections of the local government assembly in the year 2005. In 2004 month of January, a batch of American security experts disclosed the security report of Secure Electronic Registration and Voting Experiment [31]. The Secure Electronic Registration and Voting Experiment (SERVE) system was designed for deployment in the year 2004 primary and common elections and allows the qualified voters to vote electronically with the help of internet. After investigating the security of SERVE, the batch of security experts recommended that the SERVE should be closed. They also announced that they do not trust that differently constituted projects could be more secure than the SERVE. Their conclusion was that the real problems to success in electronic voting are not skills, resources, etc; it is the fact that given the current Internet and PC security technology, electronic voting is an essentially impossible task.

The Secure Electronic Registration and Voting Experiment project was terminated indeed in January 2004. The Estonian security experts published their security analysis at the end of 2003. They declared that in *practical sense* the Estonian e-voting system is secure enough for implementation.

This contradicting situation was the main initiator of this work. By closer view, both security reports are consistent and contain truthful and convincing arguments. One of the main reasons for two totally different results was the lack of unified security analysis in

both reports. Some of the arguments were quite emotional, being based on experts' subjective opinions and "common wisdom" [29].

Considering the security aspects of personal computers, it is impossible to design electronic voting systems, which are completely secure for each and every user. The main major security goal of voting is not to change the final results and not to insult the theory of democracy. The single incidents with users are still important but they do not have influence to the final result. Moreover, even in traditional voting systems small-scale incidents are acceptable. Therefore, in security analysis of e-voting, the need is to concentrate on large-scale threats [32].

One of the rational approaches of security is known from theoretical cryptography: security reductions, which are proofs that security conditions are held under certain combinatorial assumptions, such as hardness of factoring or Diffie-Hellman problem. For proving security, there is a need for empirical assumptions about the real world. Moreover, in theoretical cryptography the adversaries are considered to be Turing machines, which are well-defined and relatively easy to study. The real world adversaries are human beings with unpredictable behavior and different motives. Hence, for analyzing security, there is a need of real world adversary models. There are works, which attempt to model real world adversaries.

In information technology, biometrics mention to technologies that compute and examine human body features, as fingerprints, eye retinas and irises, voice patterns, face patterns and hand menstruation, for authentication processes. Authentication by biometric confirmation is growing common in collective and general security systems, customer electronics and point of sale applications. In security, the driving force behind biometric confirmation has been satisfaction. This biometrics is the science and technology of computing and examines the biological data of a person.

An authentic and precise identification/verification technique may be designed using biometric technologies. Biometric authentication employs unique combinations of tangible physical features- fingerprint, facial features, iris , voice, hand geometry and vein patterns [46]. Cogent Systems is a leading source of Automated Fingerprint Identification/verification Systems (AFIS), and other fingerprints biometric solutions to authorities, law enforcement agencies and other companies in the world. Cogent's AFIS solutions enable its persons to record fingerprint images electronically, encode

fingerprints into search files and exactly compare to a set of fingerprints from database carrying potentially millions of fingerprints in microseconds [36][43].

Biometric systems are widely used technology for identification and verification purpose by pattern matching. Identification means to find a match between the input pattern and the one which is already stored in data base. For example in biometric attendance system, when a student applies his/ her finger on the biometric device for scanning, a newly generated pattern compared with the stored templates in data base to find a match. If match is found, then the person will be allowed to pass through that area. On the other hand verification means the process of checking whether an input pattern belongs to the claimed identity or not [47].

2.2 DEFINITIONS

The category "electronic voting" is potentially broad, referring to several distinct possible stages of electronic usage during the course of an election. For the purposes of this research work, distinctions are made between the following terms:

- ***Electronic voting:*** Electronic voting is a voting process where electronic machines are used to facilitate vote without using paper ballots. Once recorded, an electronic vote is stored digitally and transferred from each electronic voting machine to a counting system [41].
- ***Electronic vote counting***: Vote counting through electronic means is known as electronic vote counting. In this phase of election, ballots are tabulated for publication of election results. It this method of counting, voters are allowed to cast their votes without using electronic medium, but counting these votes is done with the help of an electronic system and award seats through an electronic vote counting system [41].

2.3 INTERNATIONAL STATUS OF ELECTRONIC VOTING

- ***Brazil:*** Brazil is the largest nation in South America and in Brazil currently all votes are registered by electronic voting machines. The Brazilian Supreme Election Court authorized the use of Electronic voting method in the 1996 Brazilian metropolitan

elections. In the year 2000, the Brazilian government had transformed to fully electronic voting and established over 400,000 kiosk-style machines in elections that year. The voting machines feature an integrated screen and keyboard .To vote for a candidate, voters only need to press on the keyboard the number designated for a particular candidate. The candidate's picture then appears on the screen. Voters can confirm, reject, choose another candidate or start the selection process again. The Brazilian electronic voting technology is extraordinary in that the voting machine tallies the votes itself once voting finishes, producing the result both digital and printed details of the number of votes given to each candidate. 12,000 machines used to present a ballot paper that the voter could peruse and submit in a box for recount. These paper-trail machines were successfully used during the election [41].

- ***India:*** In India first election using electronic voting was held from April 20 to May 10, 2004. The legal approval in the year 1989 to allow the use of Electronic Voting Machines, they have been used in many state level elections but were never used for an entire general election before this. Electronic Voting Machines were prepared by Electronics Corporation of India and Bharat Electronics. The Electronic Voting Machine has mainly two units, one for control by the polling officers and the other for the uses of voters to cast their vote. The ballot unit requires voters to press the button next to the candidate's name and symbol and the control unit registered the vote. A light next to the button glow and a short beep sound follows indicate the vote has been registered. The polling personal then take necessary step to enable the next voter to cast their vote. The Electronic Voting Machine comes in a reusable carry pack and can operate on a battery power source in remote areas. According to Election authorities, each EVM can record five votes' minute or nearly 3,000 votes in a polling day [24, 37].
- ***Belgium:*** In Belgium Electronic voting was approved by law in 1994, and widely used in the 1999 and 2000 general and municipal elections. In the general elections of May 18, 2003, 3.2 million Belgian citizens were able to vote electronically. Belgium's apply similar approach as Ireland's in that it does not modify the voting process, but rather replaces the ballot paper with a machine at the polling station and then uses an electronic counting system to tally the results. In 2003, an audit report released by the Federal Public Service of the Interior approved the systems after a simulation based on around 1 million votes [57].

- Some difficulties were recorded during the 2003 voting (May 18) in the Belgium elections where electronic polling booths were in use for the general elections, which renewed both federal assemblies of the country. Delays occurred in voting operations in some localities causing some polling stations to have to remain open well after the official closure time of 3 p.m. Voters therefore had to wait for a long time to cast their vote in some areas. Most did wait, due to Belgium's compulsory voting system and fines for failing to do so, but it was reported that an estimated 10% of voters abstained from the ballot in certain areas [58].

- ***Australia:*** In Australia EVM started in a close election in 1998. The Australian Capital Territory (ACT) is one of eight states and territories in Australia. Members of the ACT parliamentary Assembly are elected using a corresponding presentation electoral system known as the Hare-Clark system. Hare-Clark is a variant of the single transfer vote system used in Ireland. Selector vote by success preferences for separate applicant. To be elected, an applicant needs to collect a quota of votes. Each voter has a single vote, which can be transferred from one candidate to another candidate on the basis to the preferences shown until all the vacancies are filled. In the ACT, the Hare-Clark system is used to elect 17 candidates from 3 multi-member electorates. The electorates of Brindabella and Ginninderra each select 5 candidates, and the electorate of Molonglo select 7 candidates.
  - A close election in 1998 in the ACT found numerous problems in the state's hand-counting system, when two candidates were separated by only three or four votes. After recounting, officials discovered that out of 80,000 ballots, they had made about 100 mistakes. Ultimately, the ACT Electoral Commission adopted a new system known as eVACS or Electronic Voting and Counting System. The system was created (by a company called Software Improvements) to run on Linux, which is a widely used, freely available open-source operating system [39].
  - The eVACS-based voting machine combination of a Personal Computer and offers ballots in 12 different languages, including the language Serbian and Farsi. English audio is also includes in the system for vision-impaired and

uneducated voters. The swapping of the bar code by the voter over a reader that resets the machine for an upcoming voter to vote and calls up a ballot.

- The eVACS- based voting system find problems like it is hard to use barcode readers and even small delays in notification of results on and after election night, it was well received by voters.

- ***Italy:*** In Italian electronic scrutiny system was involved in the large scale election in 2004. According to the Italian Government, the main advantages of an electronic scrutiny system would be easier and faster operations, more accurate vote counting, faster and secure transmission of results and an increase in overall election efficiency.
  - The Italian government has not yet released detailed technical specifications of the planned electronic vote counting system [41].
  - A national ad-hoc Commission will assess the pilot, with particular reference to the efficiency of the system, and address any problems it may encounter. The Commission will then make any necessary recommendations in order to prepare the system for wider testing in future elections [25].
- ***Argentina:*** Argentina started an electronic voting system in the year 2003. This system is basically based on the machines which are already used in country Brazil. The electronic voting machines (EVMs) parallel ATMs. At the time of voting each voters presents identity proof at the polling booth and the registrar enters the voter's identity number at a keyboard with a display. If it appears OK on the display, then the voters is authorized to vote and goes behind a place where the Electronic Voting Machine is located [32].
  - The screen of the Electronic Voting Machine shows the first office that the voter will vote for all the active parties that introduced candidates, each paired with a number. The voter chooses his or her preference by punching a key with the number of the selected party. The screen shows the name and photo of the selected candidate. To authenticate the selection, the voter punches a green key. If the voter wants to change the preference, he or she punches a red key. Once the preference has been made, the voter pushes a white key and then the green key to authenticate. The system also allows voters to cast "blank" votes, which in Argentina are counted in order to

calculate the percentage of votes obtained by each party. After completing a vote for a particular office, another screen appears with the following office to choose and continues until the ballot is completed. At this point the Electronic Voting Machine disables, preventing a second vote [29].

- ***United Kingdom:*** United Kingdom started EVM in May 2002, tested various technological improvements to voting or vote counting such as touch-screen voting machines while others tested techniques for voting remotely. Some jurisdictions allowed voters to cast their ballots using electronic methods such as interactive voice response (IVR) technology, PC-based systems and handheld mobile devices via short message service (SMS). Some of these jurisdictions allowed voters to cast ballots from PCs or kiosks in public places such as shopping centres. In the Electoral Commission's report to reviewing the e-voting trials it is found that the hardware and software performed successfully and without any significant problems. It also identified no evidence of fraud during the polls, although it did express concerns about potential security and privacy violations [16, 25, 31, 32].
- ***Costa Rica:*** The EVM system was tried out in elections for mayors, district councilors, municipal district councils and aldermen on December 1, 2002. Electors who choose to vote electronically are given a blank receipt signed on the back by the members of the panel presiding over the polling station. The electors' choice at each election is indicated on this receipt either by the electors themselves or with the aid of an assistant using a printer provided for that purpose. The chairperson of the Receiving Board activates the system so that each elector can vote. Electors are then presented with a monitor screen showing a ballot paper with the list of parties. Electors vote for the number of the party of their choice, they are then shown the ballot paper for district councilors, and must follow the same procedure. When each elector has finished voting, he or she must take the receipt and fold it so that the signatures of the members of the panel are visible, then drop it into the relevant ballot box. Once the paper is in the box, the elector's ID card is returned and he/she must leave the polling station [44][33].
- ***Spain:*** Spain has experimented with various forms of electronic voting. In the March 14, 2004 general elections, numerous small-scale, non-legally binding electronic voting trials were successfully conducted. These included diverse technologies in

addition to strictly Irish-style electronic voting systems such as Internet and SMS remote voting.

On November 16, 2003, three e-voting pilot tests were successfully conducted during the elections to the Parliament of Catalonia. This included remote voting via the Internet for eligible voters living abroad, and touch-screen voting coupled with an electronic counting system [33].

2.4 COMPARING FEATURES

This section gives a comparison of the features of different systems with reference to the following three dimensions which are most important over the introduction of electronic voting systems.

i. Whether a country's system uses a paper audit trail.
ii. Whether the system permits an anonymous, blank or spoiled ballot.
iii. Whether the software is open source or proprietary.

- **Paper audit trails:** Out of the ten countries surveyed, only Brazil used paper audit trails on any significant scope. The Brazilian government introduced them on a limited basis for the October 2002 elections where paper audit trails were used on 12% of all machines. The system allowed voters to see the printout of their vote, before both paper and electronic votes were recorded and saved. The paper audit trails were phased out by October 2004 in Brazil.
- **Basis by which system was introduced:** In all ten countries surveyed, electronic voting was first introduced in either limited constituencies or for sub-national elections. Ireland, which introduced electronic voting first in the three constituencies in the 2002 elections, would also fall under this category. Furthermore, the trials in progress in a number of countries where national-level elections have not yet used fully electronic voting. In several cases (e.g. Brazil, Australia) the authorities audited the results from a subset of the machines to verify whether the results were accurate or not.
- **Treatment of blank or invalid votes:** Two of the systems permitted blank votes to be cast (Brazil and Australia), and both of these preserved the anonymity of the voter casting such votes. In the Brazilian system, a blank vote is included in the count of

total valid votes, while in Australia it is not. India's system does not permit invalid votes to be cast, owing largely to substantive reasons and the fact that the level of invalid votes has traditionally been very high, and one of the key advantages for electronic voting was seen as the ability to reduce the high level of invalid voting. Belgium's system no longer permits the casting of blank or invalid votes.

- **Open-source versus proprietary software:** Two of the countries surveyed (Australia and Belgium) post the source code of the electronic voting software used on the Internet for inspection. Australia initially posted its software source code and Belgium chose this measure in 1999, in order to increase public confidence in the system. Brazil permits a partial inspection of its code for a short time before the election and it was only available for inspection by political parties and by the electoral commission.

.

2.5 COMPARATIVE ANALYSIS OF ELECTRONIC VOTING SYSTEMS

TABLE 2.1: COMPARISON AMONG THE COUNTRIES OF ELECTRONIC VOTING SYSTEM

Country	E-Voting	Company	Election Type	Electoral System	Introduced Year	Year Used	Software Used	Hardware Used	Problems
India	668 million	BHEL	State	FPP	2001	2009 /2004 /2003 /2001	EPROM	EVM	None
Belgium	3.2 million	Steria	General & Municipal	Open PR-List	1994	1999	Digivote, Jites, Stesud	DEVS	2003: 500 power and computer failure
Brazil	66 million	UniSys & Diebold	All Govt. Level		1996	1996 /1998 /2000 /2002	GEMS	GX-1 integrated processor	None
Australia	218000	Software Improve	ACT federal	PR-STV	2001	2001	eVACS	PCs	None

UK	1.5 million	SVS	Local Govt	FPP	2000	2000 /2003	AVC	DRE	Mobile e-voting
Spain	3000	Indra	Municipal	PR-List	2002	2003	SIRE	SIRE System	None
Canada	98000	CanVote	Municipal	FPP	2002	2003	CanVote on Linux	CanVote Internet	None

2.6 SUMMARY

This chapter briefly describes the terminology used in E-voting system including the international status of electronic voting. Comparative analysis of electronic voting techniques implemented in various countries with a scope of improvement in them has been presented well. Analysis of various biometric techniques has been described in the next chapter.