A Trustable Electronic Government Voting Management Framework Using Trusted Platform Module (TPM)

Research · April 2015

DOI: 10.13140/RG.2.1.2248.1442

STAFFORDSHIRE
UNIVERSITY

A·P·I·I·T
ASIA PACIFIC INSTITUTE OF INFORMATION TECHNOLOGY

A Trustable Electronic Government Voting Management Framework Using Trusted Platform Module (TPM)

Mervat Adib Bamiah

TP020123

A dissertation submitted in partial fulfillment

Of the requirements of

Staffordshire University for the Degree of

Msc. Information Technology Management (ITM)

July 2010

DECLARATION

I declare that this dissertation entitled as “A Trustable Electronic Government Voting Management Framework Using Trusted Platform Module (TPM)” is my own work except the sources that I have quoted and cited in reference list.

Name: Mervat Adib Bamiah

Signature: Bamiah

Date: 30 July 2010

DEDICATION

Specially dedicated to my beloved Uncle

Mohammed Imran Bamiah

ACKNOWLEDGMENT

I would like to thank Almighty Allah for supporting me through doing and completing my thesis, a special thanks to my uncle Mohammed Imran Bamiah for giving me scholarship to complete my master and his kind wife. Also thanks to my family my mother, father, sisters and brothers; with their encouragement I faced all the challenges during my study.

Warm thanks to my teachers and my supervisor Mr. Ali Dehghantanha, least but not last thanks to my kids who were so patient for me to complete my studies and return back home. Thank you all from the bottom of my heart.

ABSTRACT

Voting is the process through which citizens can determines their leaders. The quality of this governmental voting service has to be maximized, for the citizens to trust that their election is counted and the result of voting is accurate and fair. Cost and security are the two most important factors to the success of electronic government voting system. Many of nowadays and current governmental critical issues in most countries is the election process, which lead to disturbance in citizens trust towards their governments, like for an example what happened in Iran and some other countries, proves the importance of Electronic Government Voting service. in this research the aim is to manage, and suggest solution, or at least a framework for fulfilling the gaps that lead to electronic voting security issues, wrong election will not only be social crisis, but also economic crisis due to the high cost of the inaccurate election process.

Through this research there will be an overview literature review on E-Voting system, its current status, and the suggested solution by implementing trusted platform module (TPM) for enhancing the security and providing trustworthy E-Voting system.

TABLE OF CONTENTS

List of Figures 9
List of Tables 11
List of Appendices 11
CHAPTER-ONE INTRODUCTION 12
1.1 Introduction 13
1.2 Problem Statement 15
1.3 Aims and Objectives 17
1.4 Deliverable(s) 17
1.5 Research Outline 18
1.6 Conclusion / Summary 20
CHAPTER-TWO LITERATURE REVIEW 21
2.1 Introduction 22
2.2 Benefits of E-Voting System over Traditional Voting 24
2.3 Dimensions of E-Voting Systems 24
2.4 Tasks of E-Voting System 25
2.5 Emergence of E-Voting System 26
2.6 Effectiveness of E-Voting Among Different Countries 31
2.7 Existing E-Voting Systems 33
2.8 Review of Related Work 38
2.9 Security Requirements for Cryptographic Voting Protocols 42
2.10 E-Voting Issues / Problems 43
2.11 Trusted Secure E-Voting System using TPM 46
2.12 Benefits and Weaknesses of Using TPM 51
2.13 Success Cases Implemented TPM 54
2.14 Critical success factors for E-Voting System 55
2.15 Increasing E-Voting Voter Turnout 56

2.16 E-Voting Future 57
2.17 Summary / Conclusion 59
CHAPTER-THREE RESEARCH METHODOLOGY 60
3.1 Introduction 61
3.2 Research Methodology Outlines 61
3.2.1 Literature Review Research Methodology 62
3.2.2 Problem identification methods 63
3.2.3 Data Analysis and Interpretation Methods 64
3.2.4 Proposed Framework 64
3.2.5 Evaluation 64
3.2.6 Refining 64
3.2.7 Documentation 64
3.3 Research approach 65
3.4 Research Philosophy -Paradigm 65
3.5 Research Methodology 66
3.6 Research Design 66
3.7 Justification of research Paradigm and Methodology 66
3.8 Time Horizon 67
3.9 Ethical Consideration 67
3.10 Conclusion 67
CHAPTER-FOUR DATA ANALYSIS AND INTERPRETATION 68
4.1 Introduction 69
4.2 Users Profiling-(Characteristics of the Respondents) 69
4.3 Questionnaire (1) Problem Finding 70
4.3.1 Question one (Education level) 70
4.3.2 Question Two (Nationality) 71
4.3.3 Question Three (E-Voting Channels) 72
4.3.4 Question Four (E-Voting Problems) 77
4.3.5 Question Five (TPM Proposed Solution) 83
4.4 Summary of Data Analysis _ E-Voting Questionnaire 84
4.5 Findings of the analysis 85

4.6 Conclusion 85

CHAPTER-FIVE FRAMEWORK 86
5.1 Introduction.. 87
5.2 Benefits of Data Analysis and Interpretation.. 87
5.3 Use of Literature Review in creating artifacts 87
5.4 E-Voting Management Framework Security Requirements................................ 88
5.5 Assumptions Requirements of the Proposed Framework.................................... 89
5.6Toward Trustable E-Voting Management System Framework 90
CHAPTER-SIX FRAMEWORK EVALUATION 99
6.1 Introduction.. 100
6.2 Primary Evaluation Questionnaire Feedback.. 101
6.2.1 Question one (Education) 101
6.2.2 Question Two (Nationality) 102
6.2.3 Question Three (E-Voting Framework with TPM) 103
6.2.4 Question Four (E-Voting channels with TPM)... 104
6.2.5 Question Five (E-Voting attacks mitigated by TPM) 109
6.3 Findings of the Evaluation Analysis 114
6.4 Secondary Framework Evaluation.. 115
6.5 Conclusion 116
CHAPTER-SEVEN CONCLUSION 117
7.1 Introduction.. 118
7.2 E-Voting and Information Technology Management...................................... 119
7.3 Conclusion related to the research Questionnaire – Problem 120
7.4 Recommendation / suggestion 121
7.5 Limitation of the Study 121
7.6 Self Review.. 122
7.7 Future Direction.. 122
7.8 Conclusion 123
References.. 124
Glossary 130

List of Figures

Figure (1.1) Research Outline 19

Figure (2.0) E-Democracy Application Framework 19

Figure (2.1) E-Voting process 25

Figure (2.2) Historical Timeline E-Voting Machines 27

Figure (2.3) Paper Voting 28

Figure (2.4) Lever Machines 28

Figure (2.5) Punch Cards 29

Figure (2.6) Optical Scans 29

Figure (2.7) DRE 30

Figure (2.8) Internet Voting 30

Figure (2.9) Human view 35

Figure (2.10) Technical view 36

Figure (2.11) Technical view 37

Figure (2.12) TCG Standards 47

Figure (2.13) TPM Software Stack (TSS) 48

Figure (2.14) TPM Features 49

Figure (2.15) Different methods for securing password 52

Figure (2.16) VAIO _ TPM 54

Figure (2.17) Risks/Security 56

Figure (3.1) E-Voting Research Methodology 61

Figure (4.1) Education 70

Figure (4.2) Nationality 71

Figure (4.3) E-Voting Channels 72

Figure (4.3.1) Paper Ballot 73

Figure (4.3.2) Touch Screens 73

Figure (4.3.3) Kiosk 74

Figure (4.3.4) I-Voting 74

Figure (4.3.5) IVR 75
Figure (4.3.6) (iDTV) 75
Figure (4.3.7) Telephone 76
Figure (4.3.8) Mobile (SMS).. 76
Figure (4.4) E-Voting Problem... 77
Figure (4.4.1) Viruses (Hacking).. 78
Figure (4.4.2) User Spoofing 78
Figure (4.4.3) Man-in- the- Middle 79
Figure (4.4.4) Denial of service 79
Figure (4.4.5) Repudiation.. 80
Figure (4.4.6) Fraud 80
Figure (4.4.7) Privacy 81
Figure (4.4.8) Ballot secrecy 81
Figure (4.4.9) Accessibility 82
Figure (4.4.10) Trust 82
Figure (4.5) TPM – Solution 83
Figure (5.1) Proposed Framework 91
Figure (5.2) Proposed Framework Part One 92
Figure (5.3) Proposed Framework Part Two 95
Figure (5.3.1) Proposed Framework Part Two TPM 96
Figure (5.3.2) Proposed Framework Part Two TPM 98
Figure (6.1) Education 101
Figure (6.2) Nationality 102
Figure (6.3) Framework Security Enhancement 103
Figure (6.4) TPM for E-Voting Channels 104
Figure (6.4.1) TPM for Touch Screens 105
Figure (6.4.2) TPM for Kiosk 105
Figure (6.4.3) TPM for I-Voting 106
Figure (6.4.4) TPM for IVR 106
Figure (6.4.5) TPM for (iDTV) 107
Figure (6.4.6) TPM for Telephone 107

Figure (6.4.8) TPM for Mobile (SMS) 108
Figure (6.5) TPM for E-Voting Problems 109
Figure (6.5.1) TPM for Viruses 110
Figure (6.5.2) TPM for User Spoofing 110
Figure (6.5.3) TPM for Man-in- the- Middle 111
Figure (6.5.4) TPM for Denial of service 111
Figure (6.5.5) TPM for Repudiation 112
Figure (6.5.6) TPM for Fraud 112
Figure (6.5.7) TPM for Privacy 113
Figure (6.5.8) TPM for Ballot secrecy 113

List of Tables

Table (2.1) Threats and TPM solutions comparing with existing solutions 46
Table (4.1) Summary OF questionnaire (1) 84
Table (6.1) Summary Question (6.2.4) 108
Table (6.2) Summary Question (6.2.5) 114

List of Appendices

Appendix (1) Project Proposal 131
Appendix (2) Literature Review 138
Appendix (3) Gantt chart 164
Appendix (4) Log Sheets 164

CHAPTER-
ONE

INTRODUCTION

1.1 Introduction

Electronic Voting System (E-Voting) implies the use of automated and electronic devices to cast votes in the election process that can be used in any field that an individual needs to select a preference such as in education field" vote for student leader", in our daily life E-Voting is used in TV contest like *American Idol* program where people cast their votes online to select their preference. A critical usage of E-Voting is in Government election process to select the nation's leader. It is a critical procedure that needs to be trustworthy and trustable for the citizens to choose their preference without any hesitation and for high election turnout. Integrating or upgrading from traditional voting to E-Voting system has many advantages like simplifying the voting procedure, reducing the election cost, reducing counting vote's time procedure and reducing the social costs *(Yang, C., et al. 2009).*

The implementation of E-Voting has become globally widespread allowing increased access to information in the voting process for citizens everywhere, anytime, offering the scope for better verification and oversight for election supervision procedures which requires standards to ensure that the voting process is clear, robust and precisely understood so that confidence in the results is ensured. E- voting, Direct Recording Electronic Systems (DRE), or online voting are the mechanism for voters to record their confidential, secure choice of their preferences. Examples of E-Voting System transmission devices are Optical scanners, touch-screens, or Internet voting *(Singleton, K. 2008).*

According to Independent Commission report on Alternative Voting Methods in the UK states that it is quite possible that telephone voting can increase voter turnout at a manageable cost because it is useful and offers great accessibility to a wide range of services, the popularity, flexibility and portability have inspired people to use it in various functions including its usage as a polling machine, mobile voting system provides a more convenient means of e-voting. The E-voting system entities are voters who cast the votes, Certificate authority who gives the certificate to the voter, Administrator who checks the voters' eligibility, Counter: who count the voters' votes, Election commissioner for the election monitoring process and receiving complaints from entities involved *(Ahmad, T., et al 2009).*

However, E-Voting System have many security issues such as: hacker invasion, limited by software manufacture, vote rigging by using computer, incorrect program, vote fraud, Manipulation by fake votes and hard ware technical problems , Electronic Government Voting System is critical service according to its impact on nations future, for an example manipulation of voters voting result can be performed by selecting the wrong president which will cause disturbance, unease in citizen's life, economic crisis, and political issues...Etc., as happened recently in Iran.

E-Voting System is a challenging approach for increasing Electronic Participation. However, lack of citizens' trust is the main obstacle that prevents its successful realization. Traditional voting was having several issues, the voting method held cost a large numbers of resources and money plus, the tally clerk could perform erroneous judgment which will lead to the injustice and incorrect election result which made it necessary to integrate information technology into the voting process in recent years to overcome traditional voting problems such as E-Voting, Internet voting, cell phone E-Voting, and Post-voting that were proposed in USA, UK, and several European countries *(Yang, C., et al. 2009).*

The main obstacle of this research is to introduce a framework for E-Voting management system through using TPM, as trustable platform module for secure environment and overcoming the security issues found in E-Voting System. Trusted Platform Module (TPM) is produced by trusted computing group (TCG) that can be implemented as a stand-alone or integrated component which enables trust in computing platforms *(TCG, 2009),* to overcome and enhance the E-Voting security issues, based on the literature review and the analysis of the experts' feedback after data gathering stage.

1.2 Problem Statement

A substantial amount of literature exists on critical success factors relating to the success of E-Voting systems. The problem identified in the critical governmental election service is the lack of trust in the E-Voting operation according to many factors such as; the security is not up to the level of gaining trust and confidentiality of the system, the other factor is that there are many channels to cast a vote that have to be administrated and managed well to get an accurate voting results, let alone technical factors such as machine performance and usability. In the election industry currently, many different service vendors are integrating different levels of automation, operating on different hardware platforms and employing different solution architectures. There are global focus on E-Voting systems and its initiatives; which produce a great need for a consistent, auditable, automated and interoperable election system.

E-Voting System have many security issues that are vital such as: confidentiality and availability attack (Interception and Interruption: when an unauthorized person (hacker invasion) gain access to the data to destroy it), Data integrity and authentication attack (Modification and Fabrication: when an unauthorized person (hacker invasion) tampers or inserts counterfeit data), attacking person’s identity (Impersonation). Other attacks can be systematic such as: limitation by software manufacture, vote rigging by using computer, incorrect program, vote fraud, Manipulation by fake votes and hard ware technical problem *(Council of Europe, 2003).*

E-Voting System has been introduced with it concerns about system reliability, accuracy, and trustworthiness. Existing E-Voting Systems are complex and provide a relatively low level of assurance, it is difficult for independent evaluators to be confident that these systems will record and count the votes accurately *(Sturton, C., et al 2009).*

Moreover, in order to completely verify the voting machine, it is necessary to also verify the interface to human voters, of the voting machine is consistent with the behaviour expected by Voters. In view of the current E-Voting System existing insecurity, the key of the system is to solve the e-voting problems. Current E-Voting Systems are not sufficient to satisfy trustworthy elections as they do not provide any proof or confirming evidence of their honesty. One area of E-voting system is wireless E-voting that has distance bottleneck problem mainly through the external transformation, how to discover illegal status to enter E-voting system network, can real-time display the results of E-Voting System securely and accurately response to the satisfaction of voters *(Lee, Y., et al. 2010).*

Another area in E-Voting Systems issues are result of well-publicized security concerns with (DRE) voting machines, as there are no verifiable physical record of a voter's choices also issues that arise when paper ballots are used in elections. As an example Florida's infamous "butterfly ballot" and its "hanging chads," resulting in politically-charged calls for a recount during the 2000 U.S. Presidential Election that resulted dramatic series of changes in America's voting history. The voting problem is defined in terms of security requirements. It starts from the trade-off between receipt-freeness and individual verifiability. If a voting system provides any receipt which enables the voter to verify his vote in the final tally, then that receipt can also be used for vote buying or selling. *(Cetinkaya, O., 2008).*

The greatest danger to public e-voting systems is not detecting attacks or affecting the result of the contest. Extensive security monitoring and auditing with cross checking are a critical part of e-voting system security. The Trusted Platform Module (TPM) and Mobile Trusted Module (MTM) are promising security technology solutions for the future of secure computing systems by providing hardware-based foundation of trust, enabling enterprises and governments to implement, manage, and enforce a number of trusted Crypto-Graphy, storage, integrity management, attestation and other information security capabilities. TPM is a microcontroller that can be installed on any computing device and can store keys, passwords and digital certificates. It is affixed to the motherboard of a device. The chip also includes a random number generator and the ability to perform certain cryptographic operations, such as the generation of new keys. *(TCG, 2009)*

In this research the suggested solution is applying a trusted platform from a trusted group that has gained the *ISO* to enhance the security level, also because TPM is nowadays is becoming a standard requirement to be implemented in the operating systems and devices, becomes almost cost free, that is another important factor to be considered. This will enhance the presentation of the framework proposed in more credible approach and enhance the evaluation process from management perspective, although it will be tested and evaluated by experts.

1.3 Aims and Objectives

The aim of this project is to provide a trustable E-Voting System Management framework using Trusted Platform Module (TPM).

The objectives needed to achieve the above aim are as below:

1.3.1 Critically analyse the effects and issues of implementing TPM in the current E-Voting System.

1.3.2 Justifying the Pros & Cons of using TPM in the E-Voting System.

1.3.3 Proposing a Management Framework for using TPM in the E-Voting System.

1.3.4 Considering practices that should be adopted to reduce risks of using TPM in the E-Voting System.

1.4 Deliverable(s)

Upon the completion of this research the final will be as follows:

1.4.1 Evaluating and reviewing the current E-Voting System Management Framework, and identify the gaps which are in the current E-Voting Management Framework to be targeted by TPM.

1.4.2 Producing Trustable E-Voting System Management Framework using TPM.

The proposed framework will be evaluated and tested by security experts.

1.5 Research Outline

This dissertation is divided to 6 chapters as follows:

Chapter 1: Introduction

This chapter provides background information about E-Voting system in order to identify the gaps, then discussion on the aims, objectives, deliverables and issues involved.

Chapter 2: Literature Review

This chapter provides an overview literature review related to the research topic with relation to the model existed and more justification on the problems or issues of E-Voting system.

Chapter 3: Research Methodology

This chapter will discuss the design of strategies and approaches to be followed in order to conduct and complete superiority research. Research guidelines, study population sampling methods, source of data, data collection methods will be included in this chapter.

Chapter 4 – Data Analysis and Interpretation

Raw data obtained from the research survey process will be checked and observed in this chapter, first the study on the outcome of data collection. Then, consistent data are tested according to the developed hypothesis on their significance and will continue interpretation of the analysis results.

Chapter 5 – Artefact-Framework

Upon data analysis and interpretation, chapter five will discuss and proposes framework using TPM**,** How literature review helped to create the framework and testing the artefacts.

Chapter 6 – Evaluation of the Framework

After the framework has been developed it has to be evaluated through two methods, primary evaluation done based on the literature review and the second evaluation is done through questionnaire feedback.

Chapter 7 – Conclusion and Recommendations

Upon data analysis and interpretation, chapter seven will discuss the summary conclusion of the study, and then recommendations will be given, to increase the success of election system by using trustable E-Voting system in alignments with the Information technology.

Research Outlines

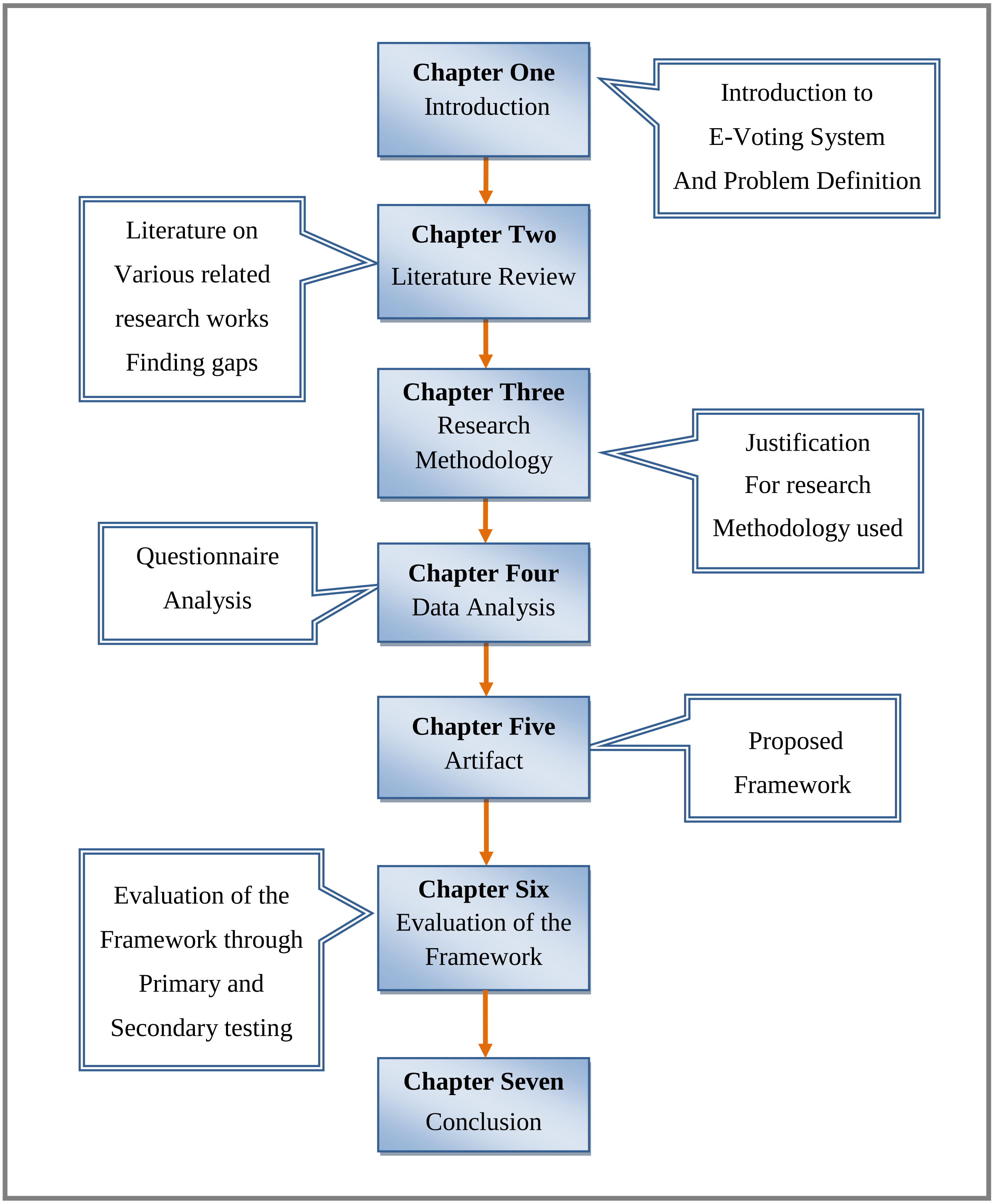


Figure (1.1) Research Outline

1.6 Conclusion / Summary

In this chapter a brief discussion on introduction, aims and objectives, research background and the problem of the research have been conducted in order to have a clear knowledge about the different area of E-Voting system. It is necessary to use every possible means to optimize secure accessibility, usability and to maintain confidence in the E-Voting system through the available devices.

The E-voting process decreases the expenses associated with printing and mailing of paper ballots. Each voter may cast his or her vote electronically, Critical factors of any voting process include accuracy, reliability, security, and the ability to be verified to gain trust in E-voting system that should accept votes from any location, be fast and user-friendly, requires no special skills or additional devices, and allows access to only eligible voters by accepting only one vote per eligible voter.

Evaluation on the usage of TPM as a trustable E-Voting Management Framework will be discussed based on the identified research issues, the objectives of this research work in two folds, first to make use of TPM in the current E-Voting System o enhance its security and mitigate its threats, second to develop trust among e-voting system elements. These two objectives would lead to the development of e-voting security framework that is able to gain users trust and perform in effective, efficient, secure, reliable and accurate way.

CHAPTER- TWO

LITERATURE REVIEW

2.1 Introduction

The huge adoption and usage of information technology improved government services and the vibrancy of democracy. As for presidential election, governments have trusted technology with adopting of E-Voting systems that offers enhanced voter convenience and eliminate the need for subjective recounts. E-voting would make the election process more accessible and convenient to users, but it will not maximize the voter's turnout, also site security is considered as a major barrier to E-Voting adoption in various countries *(Moynihan, D., 2004).* E-Voting refers to the use of computerized voting equipment to cast ballots in an election securely by implementing the cryptographic voting protocols to make it secure and applicable. The security requirements for cryptographic voting protocols are privacy, eligibility, uniqueness, fairness, receipt-freeness, accuracy, verifiability, and elaborate checklists presentation *(Cetinkaya, O., 2008).*

E-Voting as a part of electronic government which is defined as "the use of information technology to support government operations, through engaging citizens, and providing government services" which includes not only electronic administration but also electronic participation by citizens through voting process *(Prosser, A., Krimmer, R., 2004).* As for the internet voting application and technical complexity combined with the political processes E-Democracy application framework is developed as shown in the figure below.

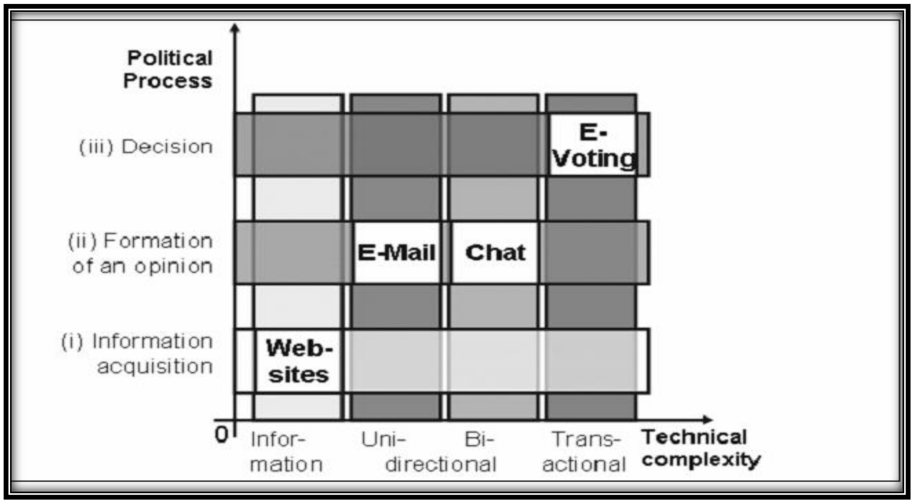


Figure (2.0) E-Democracy Application Framework, (Prosser, A., Krimmer, R., 2004)

As the figure shows four application have resulted from combining technology with democracy, such as Websites as information provision for citizens, E-Mail communication , Chats with politicians as discussion takes place at the same time, finally E-Voting where a decision is ultimately taken. It is an application that encompasses of different types of voting embracing both electronic means of casting a vote and counting votes. E-voting system entities are voters who cast the votes, authority who gives the certificate to the voter, Administrator who checks the voters' eligibility, Counter: who count the votes, Election commissioner for the election monitoring process and receiving complaints from persons involved *(Ahmad , T., et al,. 2009).*

E-Voting includes DRE devices, Optical scan devices, Kiosks, Telephone voting, Wireless Application Protocol (WAP) voting, Short Message Service (SMS) voting, Internet voting and any electronic counting specific devices *(Borras, J, 2009).* All these different E-Voting channels have to be maximum secured to gain the voters trust and acceptance to use the preferred channel. E-Voting System system can be divided into three main categories: *Hardware**:*** any mechanical, electromechanical, and electrical hardware parts, *Software**:*** all software components such as operating system, drivers, compilers, programs, databases, rules used in the program, procedures and sequences (order of voting events, voting protocol, encryption techniques, and *Human factor*: this factor comprises usability, rules, strategies (e.g. information flow, security management), politics, and other diverse aspects such as transparency, acceptance, and trust. *(Ondrisek, B., 2009).*

There are many issues identified in the existing E-Voting systems related to security, which decreases the trust and confidentiality of the E-Voting system, and may lead to low turnout in casting votes. This literature review examine the existing work related to A Trustable Electronic Government Voting Management and suggests an applicable solution in order to overcome the E- voting problem by introducing The Trusted Platform Module (TPM) which is a promising security technology solutions for the future of secure computing systems by providing hardware-based foundation of trust, enabling enterprises and governments to implement, manage, and enforce a number of trusted Crypto-Graphy, storage, integrity management, attestation and other information security capabilities *(TCG,2009).*

2.2 Benefits of E-Voting System over Traditional Voting

Benefits of E-voting system are as follows: (*EJEG Electronic Journal of E-Government, 2005).*

2.2.1 E-voting system can cast and count votes with higher convenience and efficiency.

2.2.2 E-voting system increases the speed and accuracy of ballot tabulation.

2.2.3 E-voting system saves materials required for printing and distributing ballots.

2.2.4 E-voting system offers better accessibility for people with disabilities.

2.2.5 E-voting system offers a flexible ballot design that can be modified at the last minute.

2.2.6 E-voting system provides multiple-language support for the ballots.

2.2.7 E-voting system prevents unintentional mistakes by voters (both in over voting and under voting.

2.3 Dimensions of E-Voting Systems

There are four dimensions that have huge impact on E-Voting systems adoption which are Politics, Law, Technology, and Society. *(Prosser, A., Krimmer, R., 2004)*

Politics

It is important to recognize what kind of political system exist (constitutional monarchy, parliamentary democracy, etc.), the method and frequency of voting as well as general statistics on elections (who are eligible voters, electoral districts, what is the number of polling stations), Adding the official attitude towards the implementation of E-Voting systems.

Law

The kind of legal system with the electoral law in special, are the basis for the technological solution. For E-Voting systems the existing legal principles for elections are important, the way E-Voting is implemented and in which stage E-Voting is in the legislation-making process.

Technology

The technological infrastructure of the implementation of a digital national ID card, the digital signature, the adoption of international E-Voting standards, and the level of E-Government offerings in general.

Society

The level of political participation and the turnout of voting, the public attitude, and the penetration rate of different e-voting channels, finally the Internet transactions in the society.

2.4 Tasks of E-Voting System

E-Voting system tasks (processes) are identified in three stages as shown in the figure below under the supervision of the management and the help of helpdesk candidates.

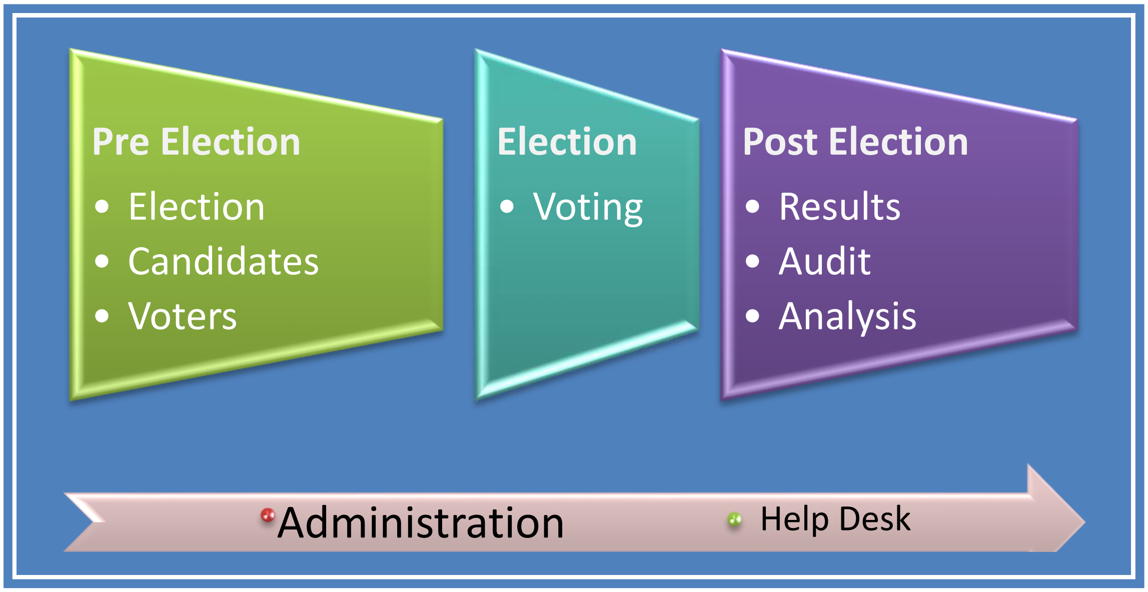


Figure (2.1) E-Voting process, (Borras, J 2009)

2.4.1 Pre – Election process

At the beginning of the election the organizers of the process will announce the information and the duration time of the E-Government Voting process, and then they determine who is eligible to vote at the permitted time after that ballot preparation and distribution this phase includes election information , candidates and the voters identification.

2.4.2 Election process

Voters can choose between casting their votes physically at the election place (poll site), remotely by internet voting (online / email) or by Mobile SMS according to the different channel voters preference, after authenticating and authorizing themselves by providing identification to a trusted official workers, for preventing over or under votes administrators validates the credentials of those attempting to vote when the election process begins.

2.4.3 Post - Election process

After voters have casted their votes, the administrators collect the votes then votes are processed and an election result is audited calculated and presented.

2.5 Emergence of E-Voting System

The future is always based on history, for better understanding of E-Voting systems a brief description of the emergence of E-Voting system is described in this section; the first form of E-Voting process was punch card system in 1960s. Some countries including India, the Netherlands, Brazil, Canada, Ireland, Venezuela, Switzerland, France, and the United Kingdom utilized some form of E-Voting technology to collate, count, and confirm election results *(Singleton, K. 2008).* In the early 20th century, the issues of rising numbers of voters, multiple elections falling down the same day and second-round runoffs which caused many countries to consider replacing ballot boxes with "voting machines" (Qi Yao et al. 2009) was limited to putting some buttons and vote counters in a booth before interest waned fatally after the unpromising results of 1970s trials in Europe and North America.

Only in the late 1980s did the first E-Voting systems were implemented online, used on a national scale in Belgium and Holland in the early 1990s and Brazil in 1996. France ran a few trials in Bordeaux and Brest in 1980 but the real test of the all-in-one electronic booth with a "built-in ballot box" was the 1999 European Union elections, followed by its use for the 2000 referendum for reducing the presidential term of office from seven to five years.

According to *(Singleton, K. 2008)* Out of the 79 million Americans who voted in the 2000 Presidential election, 28.9% used some form of an E-Voting device which is quit huge percentage almost 23 million that shows the importance of e-voting system on the turnout of citizens vote percentage that can change the whole elections results. Tony Blair, British prime minister, announced in July 2002 that in the British 2006 general election, citizens would vote in any of four ways: online by Internet, by mail, by touch-tone telephone, or at polling places through online terminals. All the counts of the elections would be done electronically. Providing many alternatives for citizens to vote will facilitate the voting process, and will effect positively on the voting turnout, let alone reducing the queue of voters standing for hours to take their turns. As the time passes by technology improves and E-Voting systems also are developing to overcome the issues that comes with the technology.

As shown in the figure (2.2) below E-Voting systems are recently implemented around 36 years, while the other voting technology such as paper ballots has a history of 164 years, the emergence of Australian secret ballots on 1888 till now is more than 119 years. Optical scan is also a technique which has evolved only around 45years and still in use for casting votes.

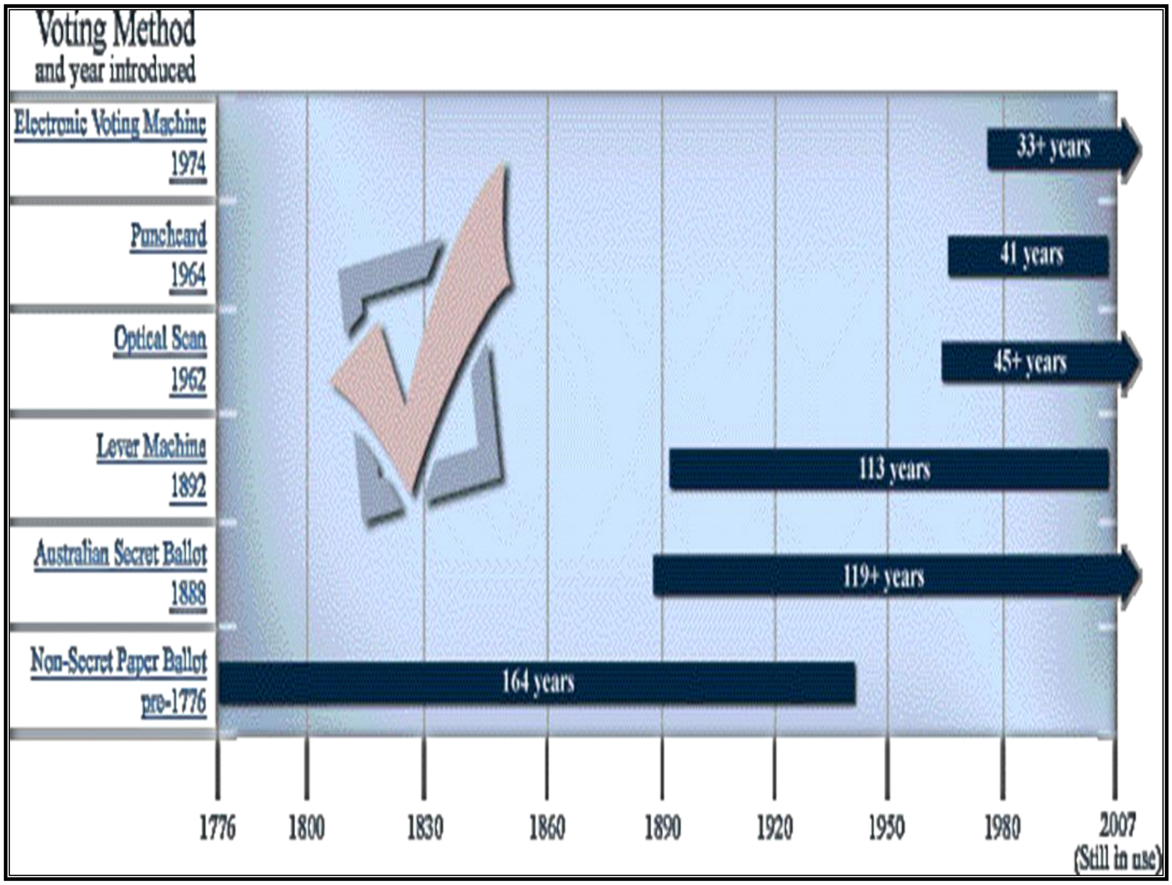
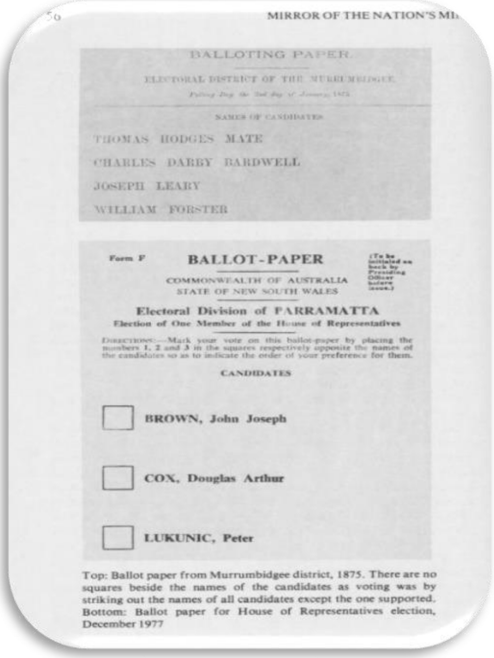


Figure (2.2) Historical Timeline E-Voting Machines (ProCon.org, 2009)

In the past, voters have to be presented in polling place physically, to cast their votes using paper ballots of various stock weights on which the names of all candidates and their information are printed. Voters record their choices, in private, by marking the boxes next to the candidate they select, and then they drop the ballot in a sealed ballot box. That was the method used in traditional voting. Through the next section a discussion about evolving of voting methods until recent E-Voting status will be conducted.

Paper Based Voting

The first country to adopt paper ballot system for elections was Australia 1856; the voter takes a blank ballot and uses a pen or a marker to indicate his preferred candidate. There are some issues with this method such as populations are increasing and some legible voters are not available at election time, let alone disabled people voting problems. Other issue is that; hand-counted ballots is a time and labor consuming process, advantages are with the simplicity of voting process, it is easy to manufacture paper ballots and the ballots can be retained for verifying *(Ying Lai, J., 2008).*



56 MIRROR OF THE NATION'S MI

BALLOTING PAPER.

ELECTORAL DISTRICT OF THE MURRUMBIDGEE.

Polling Day the 2nd day of January, 1875.

NAMES OF CANDIDATES.

THOMAS HODGES MATE

CHARLES DARBY BARDWELL

JOSEPH LEARY

WILLIAM FORSTER

Form F **BALLOT-PAPER** (To be initialed on back by Presiding Officer before issue.)

COMMONWEALTH OF AUSTRALIA
STATE OF NEW SOUTH WALES

Electoral Division of PARRAMATTA
Election of One Member of the House of Representatives

DIRECTIONS:—Mark your vote on this ballot-paper by placing the numbers 1, 2 and 3 in the squares respectively opposite the names of the candidates so as to indicate the order of your preference for them.

CANDIDATES

□ **BROWN, John Joseph**

□ **COX, Douglas Arthur**

□ **LUKUNIC, Peter**

Top: Ballot paper from Murrumbidgee district, 1875. There are no squares beside the names of the candidates as voting was by striking out the names of all candidates except the one supported. Bottom: Ballot paper for House of Representatives election, December 1977

Figure (2.3) Paper Voting *(Wright, J., 2004)*

Mechanical Lever voting machines

Lever voting machines introduced 1892, are peculiar equipments, each lever is assigned for a corresponding candidate. The voter pulls the lever to poll for his preferred candidate. This voting machine can count up the ballots automatically, but its interface is not user-friendly enough, and training to voters is necessary. These machines are no longer made; the trend was to replace them with direct recording electronic systems. *(Ying Lai, J., 2008)*

Figure (2.4) lever Machines *(Social Studies, n.d)*

Punch Cards

Punch card voting system is made of cards and a metallic hole-punch device for recording votes. Voters punch holes opposite their preferred candidate. Then the ballot is placed in a ballot box, or entered into a computer vote-tabulating device at the precinct. This mechanism counts votes automatically, the issue was people cannot punch the card out cleanly, resulting in confusing to interpret ballots, if the voter's perforation is incomplete, the result of voting is not accurate which makes it necessary to find another alternative for election process..*(Ying Lai, J., 2008)*

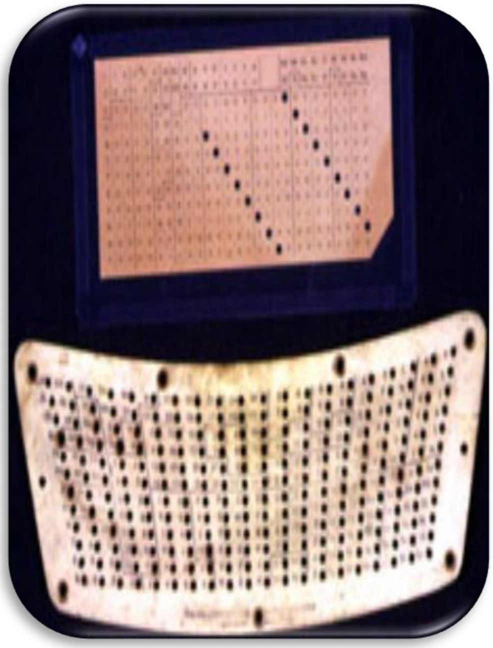


Figure (2.5) Punch Cards (Social Studies, n.d)

Optical Scan Voting Machines

Voters record their choices by filling in the rectangle, circle or oval, or by completing the arrow. After voting, the voters either place the ballot in a sealed box or computer-tabulating device that computes the total result. This machine counts up ballots rapidly. However, if the voter fills over the circle, it will lead to the error result of optical-scan. There was a need for much accurate system, DRE was the new alternative. *(Ying Lai, J., 2008)*

Figure (2.6) Optical Scans (Borchuck, J., 2007)

Direct Recording E-Voting Machines

Direct Recording E-Voting Machines (DRE) has no ballot; the possible choices are visible to the voter on the front of the machine. The voter directly enters his / her selection into electronic storage with the use of a touch-screen, push buttons, or similar device. An alphabetic keyboard is provided also. Electrovote 2000 as an example is basically a touch screen voting method; the vote can be done by key board. Microvote uses push-buttons to register a vote. The ballot is preprinted on paper protected behind a window between the rows of buttons. It cannot be touched or removed by the voter. Once a vote has been made, a light indicates that a choice has been recorded. Its weakness; Navigation through multi-screen ballots is poorly addressed on many DRE, also The introduction of DRE voting options at various locations away from polling places, like **Internet voting** which has There are three types ; *Polling Site Internet Voting*: voters cast votes via the internet from client machines in official polling places. *Kiosk Internet Voting*: voters cast their votes via Kiosks that are distributed in public places, and *Remote Internet Voting:* voters cast their votes, via home, workplace, or public internet terminals *(ACE, 2010).* Techniques such as internet and telephone voting, raises the issue of identifying the voter remotely to ensure that the person voting is indeed a voter, and that he cannot vote more than once and that the vote is secret. That led to searching for security solutions to solve these E-Voting problems which are the main aim for this research.

Figure (2.7) DRE, (Social Studies, n.d)

Figure (2.8) I-voting, (Wordpress, 2009)

2.6 Effectiveness of E-Voting Among Different Countries

Recent years, a considerable number of countries have adopted E-voting systems for its election process; here is a brief description of some countries around the world. Aim is to enlighten the current status of E-Voting system among different countries to gain more knowledge about the real implementation issues as follows:

United States

United States held election collaterally in several ways; each state can choose the suitable way to hold elections independently. As there were some issues concerning E-Voting, such as uncounted vote casts, or election system crashed during the Election Day. Secretary of State Kevin Shelley established an "Ad Hoc Touch Screen Task Force" to research the debates on DRE in February 2003 .Shelly advanced that DRE should include voter verifiable paper audit trails (VVPAT) to solve electoral debates. ***(****Ying Lai, J., 2008)*

Japan

Japan adopted E-Voting for local election in 2002 in Okayama; mayor election of Hiroshima city in February 02, 2003; and mayor election of Kyoto city in February 08, 2004. Considering election of Nimi city for example, electoral centered surveyed the voters' reliability when the election finished. 83% of voters considered that E-voting system is trusted. 56% of them considered that the results of E-voting and paper-based voting are the same therefore E-voting is sufficient for reliable. The reasons why voters can't trust the E-voting system are voters worried about the abuses in E-voting system, and they cannot make sure their ballot are recorded correctly ***(****Ying Lai, J., 2008).*

Belgium

Election for the Federal Parliament in Belgium started in May 18, 2003. Electoral center held short-term training to assist voters to be familiar with E-voting system which improved the counting efficiency in the election process. *(Ying Lai, J., 2008).*

Brazil

Brazil adopted E-voting since 1998. When the voter reaches the polling place, he/she shows his/her identity card for authenticating; if he/she is an eligible voter, he/she can get the ballot for E-voting. Brazil's E-voting system transmits votes to electoral center immediately, so that the count of votes can announce rapidly while the voting finished. *(Ying Lai, J., 2008).*

Voting status in Africa

Governments of Africa have many elections, including in ***Tunisia*** and ***Equatorial Guinea***, serve only to legitimize incumbent rulers. In ***Guinea***, thousands of people marched peacefully in the streets of the capital, calling on the military junta to step down, and go for free and fair elections to be held. The respond was brutally, killing a reported 158 people in the streets of Conakry, and injuring thousands. *(Cyllah, A., IFES, 2010).*

Mauritania elections are ineffective, and sometimes as in ***Niger*** democratic processes slip rapidly away. ***Kenya*** election 2007 and ***Zimbabwe*** 2008 were futile and dangers according to Libya's Colonel Muammar Gaddafi saying that multiparty elections in Africa led to bloodshed. Even in countries that have suffered from failed, fraudulent elections or refusal from ***Nigeria***, people increased their demands for reform and accountability, and for recognition of their fundamental human rights, even at risking their lives and limb. ***Ghana*** has emerged as a bastion of democracy, while ***Sierra Leone*** and ***Liberia*** have demonstrated the power of elections to help solidify peace after civil war. *(Cyllah, A., IFES, 2010*)

2.7 Existing E-Voting Systems

The need to know the existing E-Voting system is to overcome the issues that they have, and to develop a trustable system which is the aim of this research conducted. In the following section some examples of existing E-Voting systems and their weaknesses.

AccuVote-TS

This E-Voting system is provided by Diebold Election Systems. It includes touch screen, card reader, keyboard, headphone, and paper tape printer. The process on this system is done by selecting the candidate on the touch screen, and then the vote will be printed on paper tape. The weakness of this system is that all the electoral information (such as identity authentication, audit, or counting of votes) is stored in Microsoft Access database without password so there are high risks of attack. *(Ying Lai, J., 2008).*

iVotronic

This E-Voting system is provided by Election Systems and Software (ES&S). It provides multi-language, and uses flash memory to save voting records. Personal Electronic Ballot (PEB) a device which is similar to disk has to be used to start the machines, to access recorded votes and to transmit data over the network. Because the PEB's password is only three characters, the risk of password breaking and hacking exists. *(Ying Lai, J., 2008).*

eSlate 3000

This E-Voting system is provided by Hart InterCivic. It provides the voter with personal identity number (PIN) as four digits to login to the E-Voting machine. The voter rotate selector wheel to select the preferred candidate. Each terminal connects to the server which is named JBC (Judges Booth Controller), and then the counting votes will be saved in MBB (Mobile Ballot Box). This system doesn't encrypt voting data, so there are some risks of data Security vulnerability to hacking or fraud. *(Ying Lai, J., 2008).*

AVC Edge

This E-Voting system is provided by Sequoia Voting Systems. It is a multi-language polling machine which includes touch screen and flash memory for saving voting recorded, it has a weakness that it stumbles when this machine operated in the elections. E-voting system crashes when the voter chose language and the counting of votes is not correct. *(Ying Lai, J., 2008).*

SAVIOC

It is an open source E-voting system that all the source code and software can be downloading from its official website. The system is written in C language, and it can be saved in disk with FreeDOS. This system operates from disk; it is not connected to any networks and most of keys on the keyboard are disabled, so that attackers can't find the way to invade. Their advantages are its simple disposition and low cost, but on the other hand, there are short of GUI and ease of use on SAVIOC. *(Ying Lai, J., 2008).*

Scantegrity

This E-Voting system is provided by independent cryptographer David Chaum, with researchers from the University of the George Washington University, MIT, Maryland-Baltimore, the University of Ottawa and the University of Waterloo. It uses cryptographic techniques to let both voters and election auditors check whether votes have been cast and counted accurately. To cast a vote, the voter takes a paper ballot and fills in the optical-scan oval next to the name of the selected candidate bubble using a pen with a special type of ink, then a three-digit confirmation number already printed on the ballot using an invisible marker will appear. This code will be used also for checking the city election website to confirm the status of the casted votes. The weakness of this system is that it is not possible to link an individual ballot to a specific candidate; auditors can verify that the codes do lead to the recorded votes. Another issue is that the cost of adopting new optical scan machines on a large scale and maintaining them. *(Vijayan, J., 2009).*

High Level Model

High Level Model is designed to accommodate all the feedback and input from the members of the committee, presented in two views, the human view and the technical view.

High Level Model – The Human View

The human view indicates that the election process begins by the election of a president, voters chooses one of the candidates according to their preference. The information about the candidates should be available for the voters when casting their votes. The voters should be registered first and authenticated in order to prevent fraud then voters decide upon the candidates list to select their preferred nominee and cast their votes which will be audited and counted securely and the results will be published as shown in the figure (2.9).

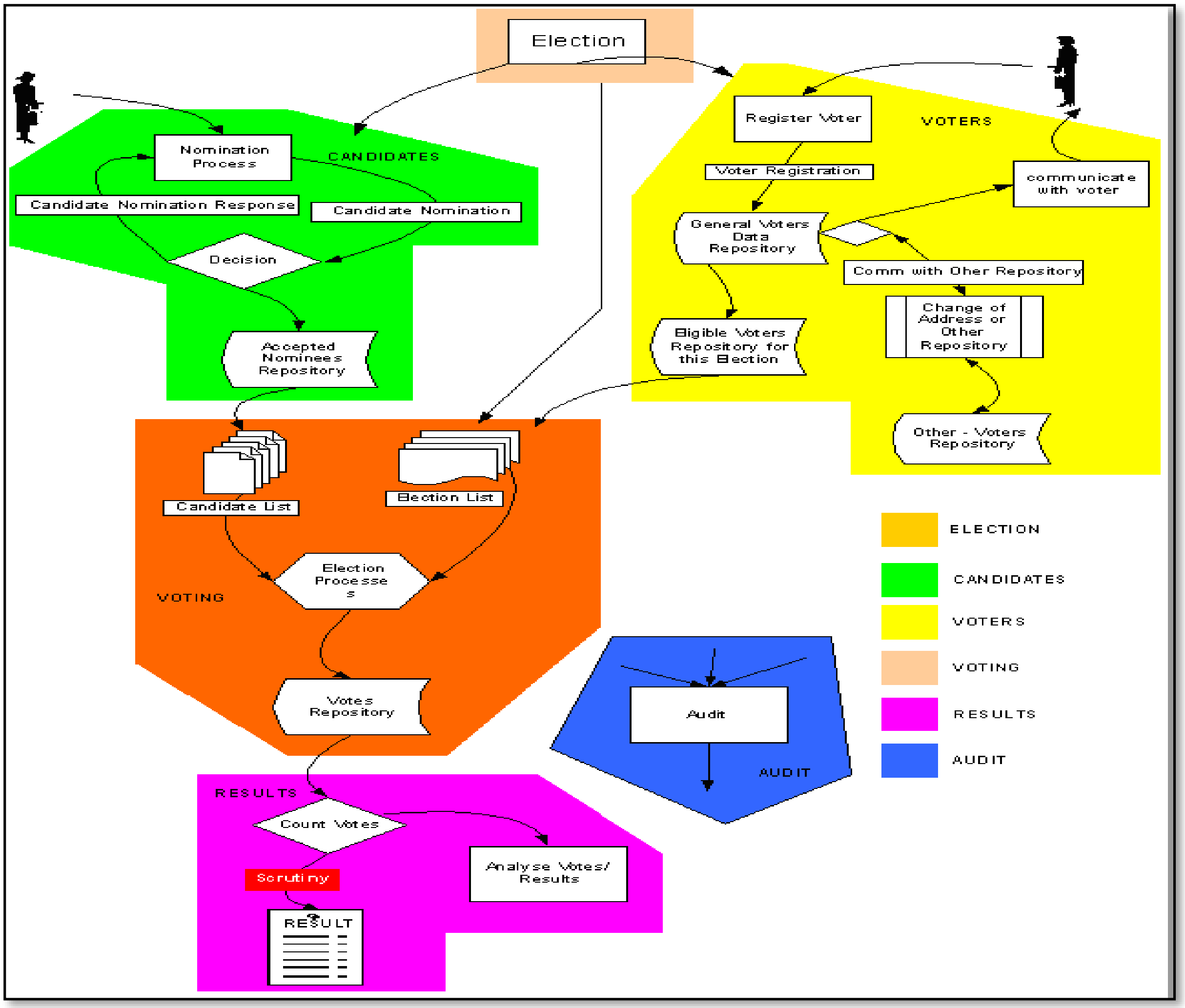


Figure (2.9) Human view, (Borras, J., 2004)

High Level Model – The Technical View

In technical voting model the voting process is described according to the physical and logical parts (hardware, software and operating systems) assuming that various systems would be involved in providing the voting process and regard each system as an independent entity. As the figure (2.10, 2.11) shows, the voter will be voting using a choice of physical channels such as postal or paper ballot , or the voter can vote using 'electronic access methods' where voter can utilize a number of possible e-voting channels (Kiosks, Mobile (SMS)…etc) .

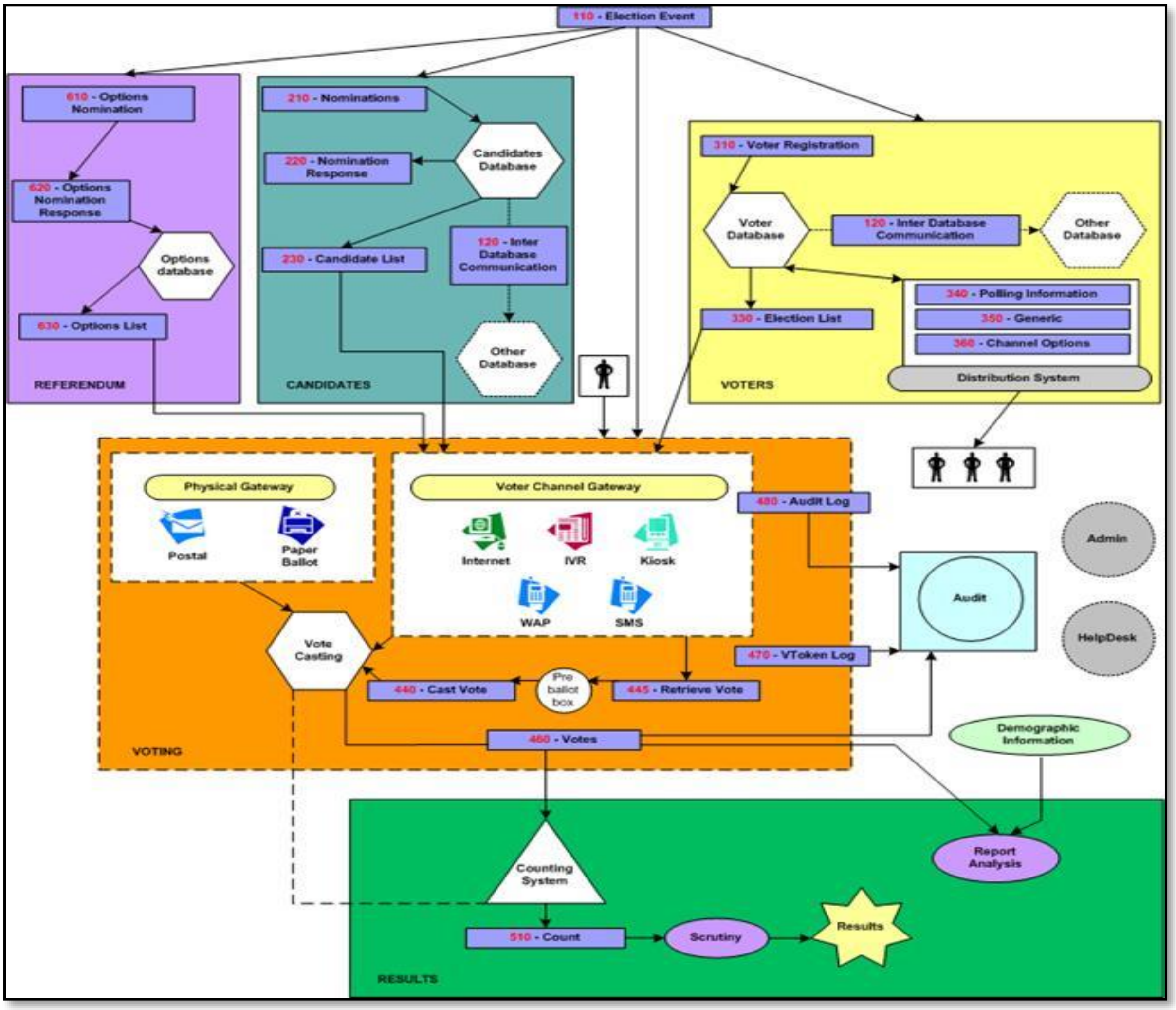


Figure (2.10) Technical view, (Borras, J., 2004)

Each channel may have a gateway acting as the translator between the voter terminal and the voting system, which are in proprietary environments. Where a voter's right to vote in any particular contest needs to be determined.

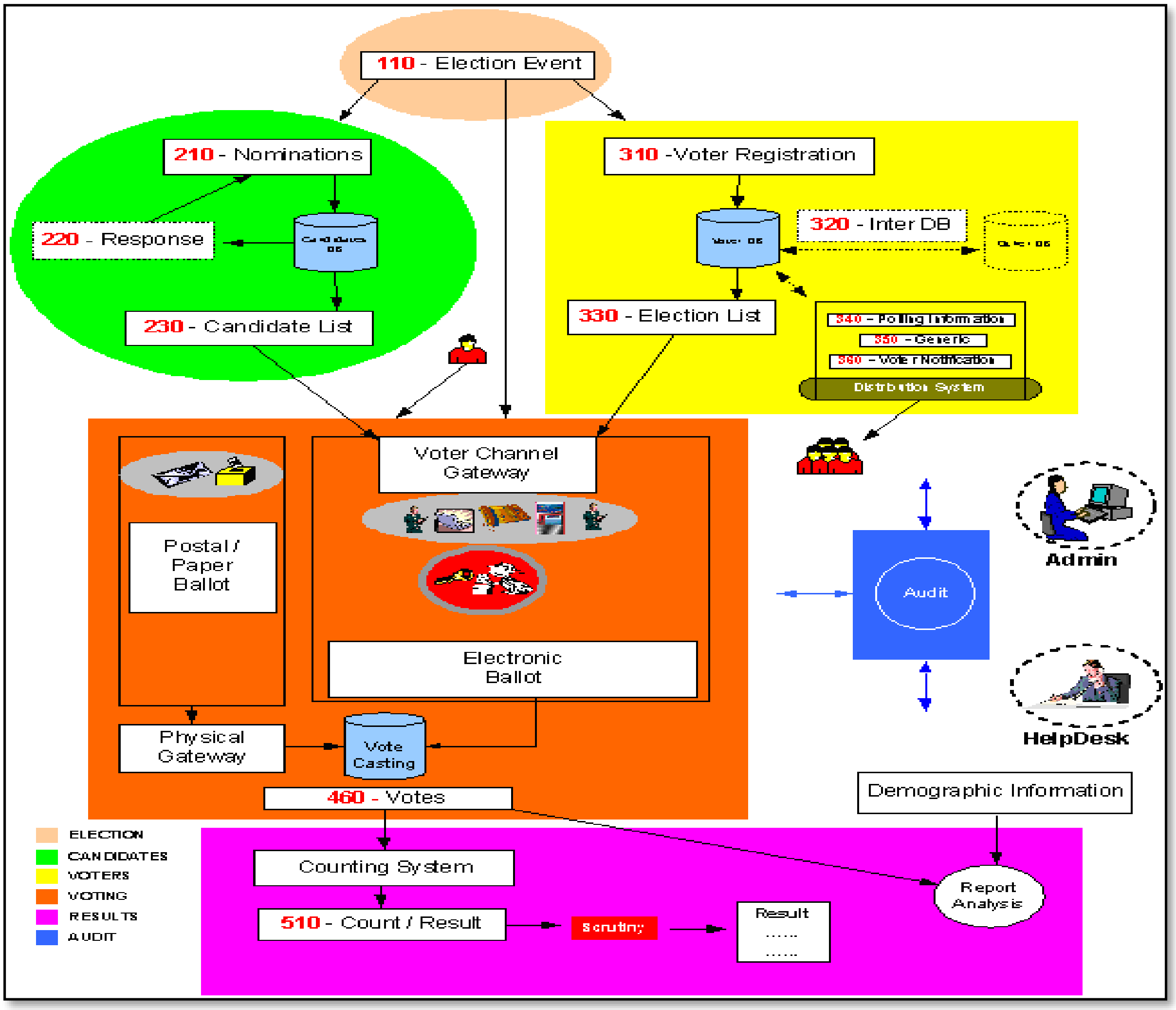


Figure (2.11) Technical view, *(Borras, J., 2004)*

To create balloting information, input data is needed about the election, the candidates available and the eligible voters for exchanging such information between e-systems. Lack of security will weaken the trust of people and will make the system vulnerable to several problems such as unauthorized privilege escalation, incorrect use of cryptography, vulnerabilities to network threats, and poor software development processes and Voters can cast unlimited votes without being detected by any mechanisms within the voting terminal software. *(Borras, J., 2004).*

2.8 Review of Related Work

E-Voting systems began in 1981 as a simple flexible; protocol that enables voters to create a receipt for their preference was introduced by Chaum. In 1988 Colin Boyd introduced another scheme which was designed for *"Yes/No"* voting, quantity of options can be increased by adding new encryption keys, voters verified by authorities. He tried to improve his system in 1989 by adding voter's second private key to assure full privacy. Up to 1992 A. Fujioka et al. Invented protocol that combines the techniques of blind signatures and anonymous channels. However, serious issues that involve accuracy; which let the authorities vote for the voters that have not participated in the election, and voters must return when commitments on all ballots are open, which decreases quantity of votes and facilitate coercion. While in 1997 Okamoto introduced a schema based on Unstoppable channels that made it possible to design a receipt-free schema. It has a weakness of lost property, if the coercer provides the voter with information for the trap-door bit commitment scheme which made his schema hard to implement *(Rusinek, D., Ksiezopolski, B, 2009)*

According to R.Mercuri (*Lee et al., 2010),* that fully E-Voting systems do not provide any way verifiability of voters recorded ballot cast, transmitted, or tabulated, which lead to Manipulation and fraud . In 2002, R.Mercuri proposed a method for voter verifiable ballots that d printed paper ballot that and keep it behind E-Voting machine window to prevent voters from tampering with it. While voter verifiable paper increase voters trust it also increases maintenance costs and election complexity as to support printing and collecting of paper ballots.

In 2002 and 2004, D. Chaum proposed a method to provide voters with a coded receipt that reflects their vote but does not reveal it to anyone else. In his scheme, the voting machine prints the coded receipt on the two layer each separate layer is a series of meaningless dots when laminated together they reveal the voter's choices by using visual cryptography when laminated together. The voter verifies the laminated receipt and then selects one of the two layers to retain as a receipt. The remaining layer should be surrendered to a poll worker and shredded. If there is a chance of knowing which layer is selected by the voter then the voting machine could cheat, thus the cost to implement D. Chaum's scheme is relatively high because of its requirement that all voting machines be equipped with special printers. *(Chaum, D., 2008).*

In 2005 Researchers from University of Pisa, Italy introduced SEAS that was described as a secure system for polling over computer networks. It was based on *Sensus* protocol (*Sensus* vulnerability is that allows one voter to cast vote in place of those that abstain from the vote) but *SEAS* avoids Sensus vulnerability. SEAS require a list of eligible and registered voters to be available before the election takes place. But it does not assure that no one can view votes before the end of the election. And does not assure uncoercibility and it enables only universal verifiability; fraud can be detected after the voting ends. *(Rusinek, D., Ksiezopolski, B, 2009).*

Also in the same year, United States Patent Office introduced TruVote Patent covers the methods and apparatus for the validation and verification of voting by a voter, voters should be presented physically and there are high cost for paper printing and maintaining (*Gibbs, A., 2005*). Still more investigation are made as in 2006, Researcher from Rice University introduced VoteBox which is an end-to-end cryptographically secure voting system platform prototype that is developed for experiment the voting security technologies. The code is written in Java, and runs on computers with Windows, Macintosh, and Linux operating systems. *(Öksüzo˘gluy, E., Wallach, D., 2009).*

By 2007 Cetinkaya and Odanaskoy introduced DynaVote protocol, that secures all of requirements listed in the *general overview* section as follows; The *dynamic ballot* ensures diversity of votes which prevent coercibility. The *PVID* scheme that solves the anonymity problem *uses* blind signatures and has two main security flaws: The coercer may buy voter's signed identity or just make voters give it directly to the coercer to send a vote in place of the voter. The Authorities may replace votes in place of voters that have not taken part in the election because only the authorities' signature is verified *(Rusinek, D., Ksiezopolski, B, 2009).*

Still researchers are trying to improve E-Voting systems, Chaum, and other researchers introduced End-to-End (E2E) systems such as Punchscan, Pr^et-_a-voter and Three Ballot, in these systems Voters can check that their votes are recorded accurately using a receipt, and observers can verify that the tally is correctly constructed, without compromising ballot secrecy. The weakness is that they require special kind of paper ballots format. Punchscan ballots4 require two sheets of paper, and Prêt à Voter ballots randomize candidate name order (Chaum et al. 2008).

After that Chaum and researchers from University -Maryland-Baltimore, University of Ottawa and the University of Waterloo introduced Scantegrity as an enhancement to optical scan systems, and it is a system which allows voters and administrators to go online and verify whether votes have been correctly recorded. It uses cryptographic techniques to check whether votes have been cast and counted accurately. During the voting process a voter takes a paper ballot and fills in the optical-scan oval using a pen with a special type of ink. When the bubble is filled, it reveals a three-digit confirmation number already printed on the ballot using an invisible marker. Voters can use that confirmation code to later log into the Web site to confirm that their votes were recorded accurately. The issue is to adopt optical-scan systems on a larger scale, which are high cost to operate and maintain (Chaum et al. 2008).

To enhance Scantegrity system and to improve it; student in George Washington University developed Scantegrity II that uses invisible ink on paper ballots for casting votes with a special pen that reveals randomized code, the weakness that is not possible to link an individual ballot to a specific candidate; auditors can verify that the codes do lead to the recorded votes. Another issue is that the cost of adopting new optical scan machines on a large scale and maintaining them *(Vijayan, J., 2009).* Yee Designed a DRE with a greatly reduced trusted code base to simplify software inspections, but the Inspections cannot prevent malicious tampering of the DRE immediately prior to operations. Jorba, *et al* Scytl architecture using a hardware security module to protect chained digital signatures. The issue was they were Vulnerable to compromise through theft and replacement of the media *(Fink, R., and Sherman, A., 2009).*

Several End-to-End cryptographic voting protocols (voter's ability to verify the election from vote casting to vote counting) have been developed and introduced beside Scantegrity and Scantegrity II such as Punch scan, Pr^et-_a-voter, Three Ballot which are provided solutions that aim to enhance the confidence in the democratic process but still needed more security optimization *(Kelsey, J., et al., 2009).*

TPM was introduced as a trusted solution to overcome previous E-Voting systems issues, and was first used by Arbaugh for voting in on-line protocol to attest systems through a central server. The weakness was that he Omitted key design details. Followed by Rössler, *et al* that used TPM in postal-voting where each voter submits a ballot encrypted with a public key to the tallying server, also Omitted key design details. As for Paul and Tanenbaum proposed E-Voting system architecture incorporating TPMs, but the issue is that TPMs' role assures only presence of correct software the platform state, and it is not bound to the casted ballot. Feldman, *et al* using technology from the TCG, but could not prevent malicious code from changing future votes by altering data before it was sent to the storage device. As for Pearson *et al* gave comprehensive overview of TPMs, and Challener provided an excellent practical guide to the TPM for software developers. Although TrouSerS introduced an open source implementation of the TSS, Strasser provided an open source TPM emulator to aid development. While Sevinc Described key distribution protocol that sends secrets from a server to a TPM-enabled client, but the weakness is that server has no way to attest the software state of the client.

For overcoming all those past TPM issues Fink, R., and Sherman, A., Combined End-To-End Voting with Trustworthy Computing for Greater Privacy, Trust, Accessibility, and Usability, Because E2E systems cannot fully satisfy ease of administration, information assurance and usability alone. Trusted Computing (TC) with the usage of TPM increases privacy by ensuring the correct software is running. TC helps enable optimum usability and accessibility by making it possible to build trustworthy electronic interfaces. And helps voters catch problems in the polling location, making voting safer and better for everyone at the cost of more complicated engineering design and key management. *(Fink, R., et al 2009)*

E2E Gaps in Voting System Attributes, Although E2E features achieve many E-Voting system goals, several gaps remain because of untrustworthy software and poor usability. Trusted Computing TPM can benefit three critical areas: Privacy is platform attestation used to control signature keys only allows voting when the system has booted the correct software, mitigating the risks of unauthorized software disclosing private information, such as Scantegrity II ballot codes. Second TPM controls can reduce reliance on trusted chains of custody by ensuring that only the correct platform can access valid data. Finally verifying correct software operation is crucial to detecting problems early and for more usability.

In addition to catching under votes and over votes prior to casting, managing the device signature key in hardware and sealing it to the correct platform state would allow the ballot to be signed only when the correct software was running. Additionally, sealing to the TPM prevents theft of the signature key. In this research framework will be developed based on the TPM module, and will be provided from the initial stage of E-Voting securing the information storage devices, network , communication and channels preferred for casting votes, such as mobiles and pc's. Most of the devices and operating systems now have imbedded TPM, which lower the cost of applying new technology as will be described in suggested solution area and chapter five framework development.

2.9 Security Requirements for Cryptographic Voting Protocols

E-Voting system must achieve its security requirements to be an acceptable trustworthy system. These requirements are listed as follows *(Cetinkaya and D. Cetinkaya, 2007).*

2.9.1 Voter Privacy

Privacy must be preserved through all the election process in order to assure privacy implementation of both **Unlink ability** (No person should be able to deduce any relationship between registration identity, the voter's public key and the voter's casting vote) and **Intractability** (No person should be able to trace the IP address or be able to deduce any relationship between the voter and his vote*)*.

2.9.2 Eligibility

Only eligible voters can cast votes after registration.

2.9.3 Fairness

No partial tally is revealed before the end of the voting period to ensure that all candidates are given a fair decision even for the counting authority should not be able to have any clue about the results.

2.9.4 Uncoercibility

Any coercer including the authorities should not be able to extract the value of the vote and should not be able to coerce a voter to cast his vote in a particular way. Any voter must be able to vote freely.

2.9.5 Receipt-freeness

It indicates that the system does not provide a confirmation of the receipt of the vote which may yield its content both during and after the election ends. This is to prevent vote buying or selling.

2.9.6 Accuracy

Accuracy can be achieved in two ways: All valid votes should be counted correctly, cannot be altered, deleted or copied. All counted votes should be valid and correct, eligible and uniqueness should be satisfied. No person can disrupt or influence the election by adding false votes or be able to vote in the place of others, even if they are eligible voters but they cannot vote for some reasons or they abandoned voting process in any stage.

2.9.7 Individual Verifiability

Indicates that each eligible voter can verify that his vote is counted correctly by using published data, voters can validate that the ballot and authorities response are correct also Voter can safely re-request data during the voting process *(Cetinkaya and D. Cetinkaya, 2007).*

2.10 E-Voting Issues / Problems

There are many issues according to the current E-Voting system that will be listed and described as follows:

2.10.1 Software and Hardware Reliability

There are concerns that mechanical failures as for an example in touch-screen machines arising from electrical outages and other causes may leave votes uncounted or miscounted, with no means of recovery or Hardware clocks set wrong. As for software deficiencies in some E-Voting systems may affect election outcomes such as poorly designed , developed using inferior software engineering processes, designed without (or with very limited) external audit capabilities, intended for operation without obvious protective measures, Deployed without rigorous, and scientifically-designed testing and Insufficient audit data unable to collect data from some voting machines.

2.10.2 Vulnerability to Hacking

Criminals could hack an E-Voting machine and steal votes using a malicious programming approach. If DRE programming can be manipulated, that same logic dictates that the programming could be surreptitiously altered to change election results after the paper ballot is printed.

2.10.3 Fraud

Fraud by *Election authorities*; they may cheat by knowingly allowing ineligible voters to register, allowing registered voters to cast more than one vote, or systematically miscounting or destroying ballots.

Fraud by *Ineligible voters*; they may register (often under the name of someone who is deceased) or eligible voters may register under multiple names.

Fraud by *Registered voters*; eligible and non eligible voters may be impersonated at the polls, and ballot boxes, ballots, and vote counting machines may be compromised.

According to *(Computerworld - Washington, 2004)* security researchers said that without voter - verifiable paper receipts, the 50 million Americans who will use E-Voting machines are uncertain that their votes will be recorded properly. Also the large and complexity of code base powering the systems allows manipulation of election results. Potential vendors influencing the elections, especially since some have taken active roles in operating polling stations and, in the case of Diebold Election Systems' CEO Walden O'Dell, stated publicly the intent to deliver election results to President George W. Bush. Unauthorized privilege escalation, incorrect use of cryptography, vulnerabilities to network threats, and poor software development processes (Stubblefield, A, 2004) Voters can cast unlimited votes without being detected by any mechanisms within the voting terminal software.

2.10.4 Accuracy in Capturing Voters' Intent

The possibility of an over voting (or making more selections than permissible) or under voting (when a voter makes fewer than the maximum number of permissible selections in a contest) also touch screen machines can misinterpret a voter's intent. For example, a voter might touch the part of the screen identified with his/her preferred candidate Jones, but candidate Mary’s box would light up instead.

2.10.5 E-Voting Recounting Issue

E-Voting offers myriad benefits—from multilingual operation to the prevention of over voting but to be trustworthy, a voting system must satisfy three main goals is to; Ensure the election’s integrity, Allow results Auditing Can be understandable and Trustable for both voters and politicians.

2.10.6 Security Issues

Security can be external issues due to voters and attackers, and internal issues such as system developing and administrating even just inheritance of some objects in the source code are unsuitable can cause the voting system crash.

2.10.7 Intruder Threats

Intruder threats can be, Invading the secrecy of the vote, data theft and unauthorized access to the platform, Selling or buying the votes, Confusing or Forcing voters to vote in a particular way or Computing or changing the election results. The intruder can be internal (who is a part of the E-Voting process and who can access the system in off and on mode), or external (who can access public information and is not part of the E-Voting system), another intruder type is malicious voter (who tries to cast more than one vote or sell his / her vote). *(Volkamer, M., 2009)*

2.10.8 Internet Security Issues

Internet voting is subject to potential risks due to the inherent insecurity of both the user's machine and the network connection by which it connects to the central server or tabulator. The users' machines may have many different forms of computer viruses, "worms", "spyware", or "Trojan horse" applications *(ACE, 2010a)*. Despite the widespread use of firewalls and anti-virus software to protect the user's machines and applications, another area is the connection to the network; in this area at least the correct use of public-key cryptography allows a degree of confidence in the integrity of this communication channel.

The SSL (Secure Sockets Layer) and TLS (Transport Layer Security) protocols were designed to prevent "man in the middle" attack (a network transmission is hijacked by an attacker who has managed to control the channel through the two end-points of the transaction that communicated with one another). *(ACE, 2010a)* Other types of attack are "denial of service" attacks or "spoofing" attacks. A denial of service attack is when the attacker, is able to prevent the communication from taking place, by overloading one or the other endpoint of the communication. A spoofing attack is when one of the communicating parties is tricked into opening a secure connection to a site controlled by an attacker. A "phishing" spoofing attack involves an email containing an obfuscated link to a site, which has been created to perfectly mimic the targeted website along with an urgent request to "re-enter" sensitive personal information (credit card numbers, passwords, etc.).

The security of Internet voting must be guaranteed, because in most constituencies no connection may be made between the voter and his or her vote. Secondly, discovery of anomalies or errors in the transmission or recording of votes cannot feasibly result in a correction of these results after the fact. It can only result in the invalidation affected votes; and would have disastrous effects in terms of public confidence in the legitimacy of the entire process *(ACE, 2010a).* Some of the major issues can be solve by TPM as indicated in Table (2.1) below:

Threats	Existing Solutions	Weaknesses	TPM Solutions
Data Theft	Data encryption (EFS, VPN, encrypted email.etc)	Encryption keys are stored on the hard disk, and they are susceptible to tampering	Protected storage of keys through hardware
Unauthorized access to platform	Username /Password Biometrics and external tokens for user authentication	Subject to dictionary attacks Biometrics can be spoofed Authentication credentials not bound to platform	Protection of authentication credentials by binding them to platform.
Unauthorized Access to network	Windows network logon, IEEE 802.1x	Can be bypassed Certificate can be spoofed Authentication data is stored on the hard disk, and is susceptible to tampering	PKI based method for Platform authentication Hardware protection of authentication data

Table (2.1) Threats and TPM solutions comparing with existing solutions (Bajikar, S. 2002)

2.11 Trusted Secure E-Voting System using TPM

As a suggested solution applying trusted platform module is recommended for insuring security and gaining peoples trust. The term "trusted computing" refers to applications that leverage hardware-based at the edge of the network and at the endpoints for higher assurance. The Trusted Platform Module can be implemented as a stand-alone or integrated component that enables trust in computing platforms *(TCG, 2009)* “*The acceptance of the TPM specification by ISO/IEC confirms the position of the Trusted Computing Group as the premier industry group for trusted computing and attests to the growing usage of the specification to secure data, systems and networks*,” according to Scott Rotondo, president of Trusted Computing Group.

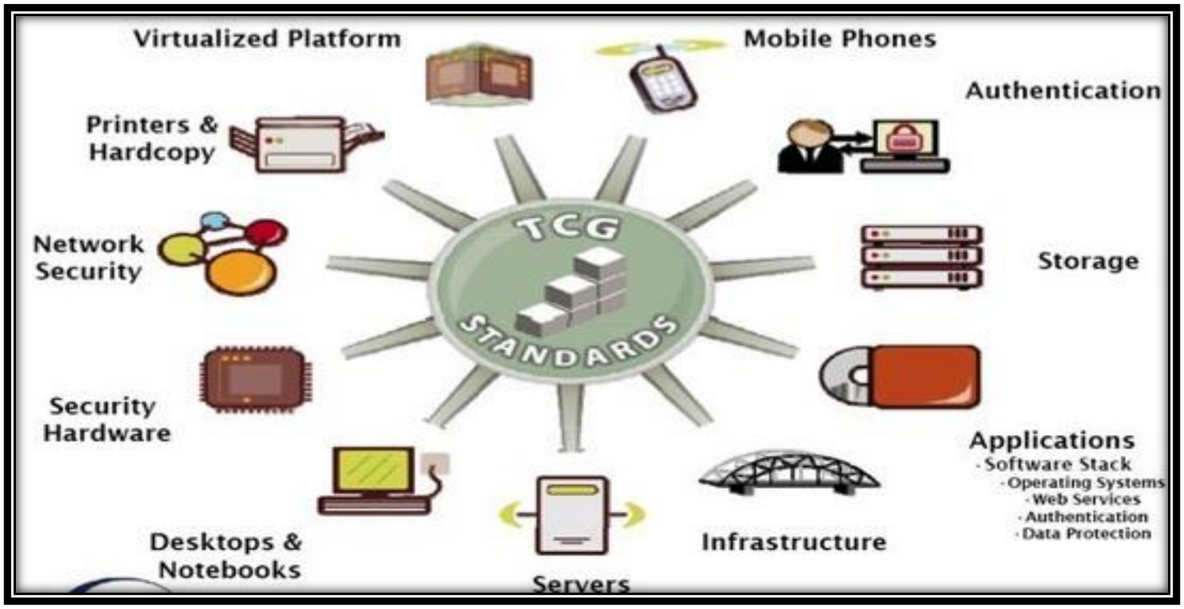


Figure (2.12) TCG Standards, (TCG, 2009)

According to TCG that TPM specification has been ISO standard accepted which reveals that deployment applications based on trusted computing infrastructure exhibit superior capabilities in security governance, risk management and compliance compared to other respondents. TPM is a microcontroller that can be installed on any computing device and can store keys, passwords and digital certificates. It is affixed to the motherboard of a device.

The chip also includes a random number generator and has an ability to perform certain cryptographic operations, such as the generation of new keys.TPM ensures that the information stored is more secure from external software attack and physical theft, security processes such as digital signature and key exchange, are protected through the secure TCG subsystem. Access to data and secrets in a platform could be denied if the boot sequence is not as expected. TPM can be integrated into other components in a system. TPM provides a group of crypto capabilities that allow certain crypto functions to be executed within the TPM hardware which can only provide input and output to TPM. It uses RSA built–in engine during digital signing and key wrapping operations. *(TCG, 2009)*

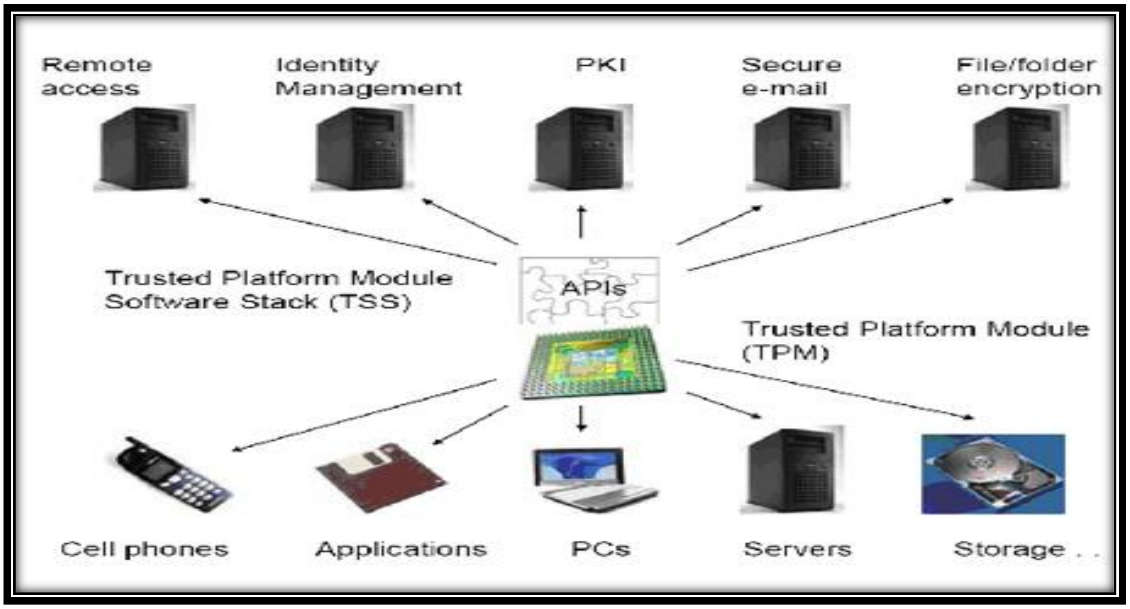


Figure (2.13) TPM Software Stack (TSS), (IT. Security Journal, 2008)

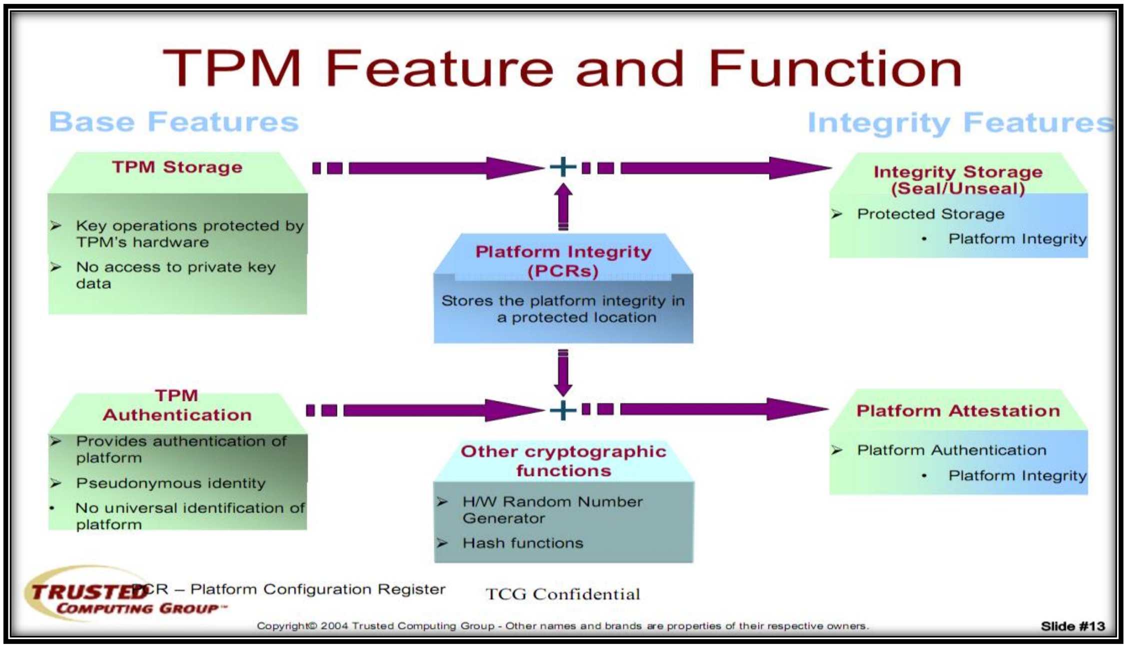
TPM Software Stack enables trust in network endpoints and secure network activities as shown in figure (2.13). TPM can use cryptographic means to accurately report its state anytime, which can be verified to determine the platform's integrity. By running on a TPM, each device in an E-Voting system operates in a verified environment, every device can attest to its state as for communicating devices can perform mutual attestation, to verify to each other that both devices are in a valid state before communicating. Using TPM approach, a trusted E-Voting system can accurately capture, count, and report the votes. *(IT Security Journal, 2008)*

TPM uses cryptographically to sign the log and bind data to this log, so the third party can have assurance that the machine only ran trusted software from the time it booted up until the time the measurement was taken. TPM forms the basis of a trusted computing platform by protecting against virtual and physical attacks. TPM ensures that the information stored is more secure from external software attack and physical theft, security processes such as digital signature and key exchange, are protected through the secure TCG subsystem.

TPM provides a group of crypto capabilities that allow certain crypto functions to be executed within the TPM hardware which can only provide input and output to TPM, it uses its built-in hash engine to compute hash values of small amount of data. Large amount of data are hashed outside of the TPM. Random Number Generator generates keys for various purposes *(TCG, 2009).* A trusted computing platform is defined by the TCG as a platform that is equipped with a

Trusted Platform Module. This TPM is a dedicated low cost hardware component that creates a chain Root of Trust. TPM chip performs certain cryptographic functions for platform authentication, secure storage registers for data, keys and attestation services. Every component (hardware, firmware or software) of the trusted platform has an associated hash value that represents its status and is distributed in a component validity certificate.

When the platform boots, measurement agents iteratively measure all the components of the platform and store the new values by concatenating them with the old values inside the Platform Configuration Registers (PCR) of the TPM chip. E-Voting system can benefit from all these security features such as TPM provides attestation device for the platform, Non-Volatile Secure Storage, Sealed Storage and Random Number Generator (RNG). *(TCG, 2009)* for securing its databases, servers, network, and voting channels.



TPM Feature and Function

Base Features

Integrity Features

TPM Storage

- Key operations protected by TPM's hardware
- No access to private key data

Platform Integrity (PCRs)

Stores the platform integrity in a protected location

Integrity Storage (Seal/Unseal)

- Protected Storage
  - Platform Integrity

TPM Authentication

- Provides authentication of platform
- Pseudonymous identity
- No universal identification of platform

Other cryptographic functions

- H/W Random Number Generator
- Hash functions

Platform Attestation

- Platform Authentication
  - Platform Integrity

PCR – Platform Configuration Register

TCG Confidential

Copyright© 2004 Trusted Computing Group - Other names and brands are properties of their respective owners.

Slide #13

Figure (2.14) TPM Features (TCG, 2009)

The Trusted Platform Module (TPM) is a piece of hardware or software that provides the ability to securely protect and store keys and data in general. It enables more secure storage of data by doing its asymmetric key operations on-chip (using its own hardware random number generator). It provides hardware-based protection of data because the private key used to protect the data is never exposed in the clear outside of the TPM's own internal memory area. Additionally, the key is only valid on the TPM on which it was created unless migrated by the user to a new TPM.

Platform Configuration Register (PC) is an area of memory inside a TPM that's used to store cryptographic hashes of data. Also an Attestation Identity Key (AIK) is a key created for use in attestation. However, data binding is data that has been encrypted by a TPM using a key that is part of its root of trust for storage. Every TPM has different root of trust of storage, the data can only be decrypted by the TPM that originally encrypted the data. Another feature also is data sealing, which is bound data that additionally records the values of selected PCRs at the time the data is encrypted. The only restriction that is associated with bound data, sealed data that they can only be decrypted when the selected PCRs have the same values they had at the time of encryption *(Fang, W., et al, 2009)*.

To enhance the security and protect information, the TPM effectively binds locks around the data. If keys or combinations are lost, the data cannot be accessible any more. The TPM provides two types of keys: Migratable keys that are designed to protect unencrypted data on more than one platform, and non Migratable keys. Least but not last, The TPM is a component on the desktop board that is specifically designed to enhance platform security by providing a protected space for key operations and other security critical tasks. By using both hardware and software, the TPM protects encryption and signature keys at their most vulnerable stages-operations when the keys are being used unencrypted in plain-text form. Trusted Platform Module (TPM), a hardware-based cryptography chip built into virtually every enterprise PC and notebook, and now installed in over 100 million PCs. *(Berger, B., 2008)*

2.12 Benefits and Weaknesses of Using TPM

There are many advantages of TPM technology as listed below:

2.12.1 Enhancing Personal Computer's (PC) data security

According to Rau, Director of PC semiconductor research at US market research company IDC. "As for client PCs and x86 servers, nearly 80 million of these systems shipped with a TPM in 2008," and by the end of 2009, predicting the number will approach 100 million systems." TPM Supports tailored security for the data that are stored on them and offer the right level of certified security that the respective application needs. *(Infineon, 2009)*

2.12.2 Memory curtaining

It refers to the isolation of PC's memory to prevent programs such as (virus's or malicious codes) from being able to alter PC's memory with TPM in the trusted computing design, even the operating system should not have access to curtained memory, to protect it from virus or hacker who gains control of the operating system interference with programs' secure memory.

2.12.3 Secure Input and Output (I/O)

TPM aims to defeat the threats posed by Key loggers and screen-grabbers (which are programs used by hackers to spy on computer users' activities). With secure I/O, no other software running on the same PC will be able to find out what the user typed, or how the application responded. At the same time, it allows programs to determine whether their input is provided by a physically present user, as distinct from another program impersonating a user. *(De Rossi, L., 2007)*

2.12.4 Remote attestation

TPM detects any unauthorized changes in the software that will protect the E-Voting system software from threats and attacks. *(De Rossi, L., 2007)*

2.12.5 Network Security

Trusted Network Connect (TCN) as a trusted platform specification provides standards for virtually endpoint security either published or in preliminary form. It provides a framework to achieve a multi-vendor network standard such as Platform-Authentication, Authorization, Access Policy, Assessment, Isolation, and Remediation which will enhance the E-Voting system network security *(IT Security Journal, 2008).*

2.12.6 Trusted Mobile Devices

TCG's Mobile Phone Work Group supports cell phones and other mobile products with the Mobile Trusted Module (MTM) specification. To meet the Trusted Platform's three requirements for roots of trust for memory, storage and reporting, the Integrity Management Model defines the infrastructure functions. Reference Integrity Measurements provide the building block elements for platform attestation. The mobile phone can now protect user data and identity information as well as device identity information. Mobile financial transactions such as payments, ticketing and voting can be conducted in confidence *(IT Security Journal, 2008).*

2.12.7 Trusted Data Storage

TPM addresses the inability of a PC to securely store passwords to prevent hacker's invasion, TPM generates passwords based in part on the identity of the software and device requesting to use them. If a program different from the program that originally encrypted, private data should attempt to decrypt, that data, the attempt is guaranteed to fail. TPM also secure storage systems including removable media drives, flash storage, and multiple storage device systems. For the highest convenience and ease of use as well as lowest cost, disc initialization, installation, and configuration are not required. The process uses partitioned, hidden memory, security firmware and hardware, trusted send/receive commands, and hidden memory assigned to applications. *(IT Security Journal, 2008)*

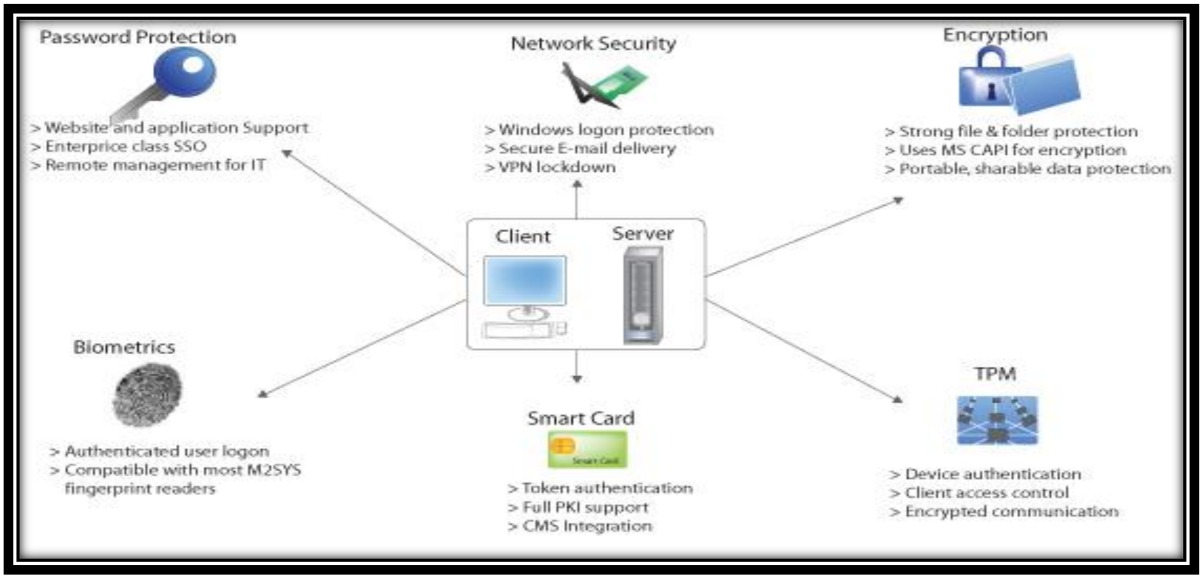

Password Protection
> Website and application Support
> Enterprice class SSO
> Remote management for IT
Network Security
> Windows logon protection
> Secure E-mail delivery
> VPN lockdown
Encryption
> Strong file & folder protection
> Uses MS CAPI for encryption
> Portable, sharable data protection
Client
Server
Biometrics
> Authenticated user logon
> Compatible with most M2SYS fingerprint readers
Smart Card
> Token authentication
> Full PKI support
> CMS Integration
TPM
> Device authentication
> Client access control
> Encrypted communication

Figure (2.15) Different methods for securing password, (M2SYS, 2010)

The strong need for password and data security management in the huge increasing number of organization data security breaches, the sharing or theft of user passwords is the basic concern to be secured. TPM is used with other solutions as shown in the figure (2.15) to authenticate the hardware, and to gain access control to the clients and to encrypt communication.

2.12.8 Reducing Cost

Any Remote access points without the appropriate authority are denied access to a TCG-TPM features protected network. With encrypted confidential data, unauthorized parties cannot access the data on computers, Mobiles or storage devices so a data breach disclosure is not required, which avoids extensive corrective action as well as cost. Provides a low cost protected environment and Ubiquitous security - at very low cost *(IT Security Journal, 2008)*

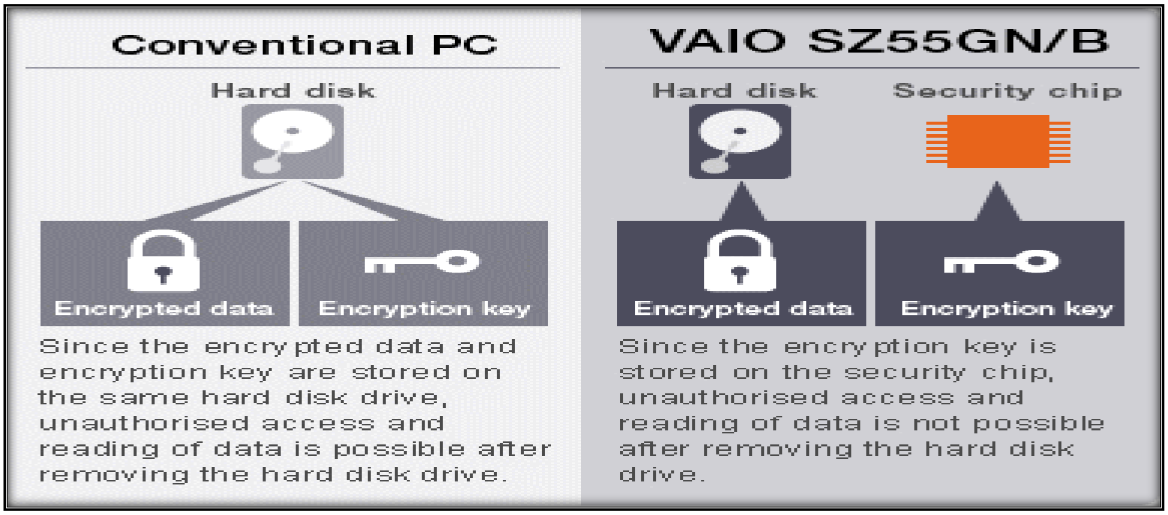
Weaknesses of TPM

TCG are trying to find solutions for information security. No one can stop the rapid technology evolving, in most countries internet is becoming a necessity for purchasing and doing transaction online, so all online and offline processes need to be highly secured. TPM 1.2 is now implemented in windows and many operating systems. TPM is designed with and Endorsement key and Endorsement Certificate from the manufacturer, which can be a weakness as the owner (manufacturer) should be trustable. Some authorities struggle to accept foreign-made cryptographic hardware modules as trustworthy for processing sensitive national data such as elections. Also it can't be directly used in common PC current in use. *(TCG, 2009)* these weaknesses do not match the huge benefits that TPM offers.

2.13 Success Cases Implemented TPM

SONY - VAIO implementing TPM security chip

VAIO SZ75GN/B provides secure encryption and decryption of files and folders with a built-in TCG - ver. 1.2 compliant TPM security chip and supplied software utility.



Since the encrypted data and encryption key are stored on the same hard disk drive, unauthorised access and reading of data is possible after removing the hard disk drive.

Since the encryption key is stored on the security chip, unauthorised access and reading of data is not possible after removing the hard disk drive.

Figure (2.16) VAIO _ TPM, (Sony VAIO, 2008)

TPM can be utilized with files such as email, the Encrypting File System in Windows Vista® operating system, and an encrypted part of the hard disk. This utility enables users to register TPM passwords that are stored and encrypted by the chip. *(Sony VAIO, 2008).*

Infineon Technologies AG, Neubiberg, Germany

According to Technology Media 2009 "*Infineon's TPM Security Chips Are First to Receive Global TCG and Common Criteria Certification and UK Government Approval; Showing World Trust in Infineon Security Expertise for PC and Data Network Protection*"

Infineon Technologies AG introduced the first semiconductor provider of TPM security chips that successfully passed security tests, the Infineon TPM, the SLB 9635 TT 1.2, offers hardware-based security features to authenticate computers and to store keys and passwords securely. Integrated onto the motherboard of a mobile or PC, TPM helps protect the stored data against unauthorized access, provides strong authentication and improves the system integrity. In government applications, TPM enables more secure data storage and secure online information exchange while protecting privacy *(Infineon, 2009)***.**

2.14 Critical success factors for E-Voting System

The basic issue in E-Voting System is Security and building people Trust to gain the success of E-Voting processes the principal axes of the approach are as follows: *(Manolopoulos, M., 2008)*

2.14.1 Proven technological excellence for the component of the system

The system should use strong technological tools and computer science primitives, preferably scientifically proven and standard-based to ensure the sound operation of the system and its robustness against potential attacks by implementing trustable security technologies such as TPM.

2.14.2 Usage of open source technologies and publicly available information

System development and operation should be based on open source technologies to allow independence from existing vendors and increase transparency.

2.14.3 Involve infield voter's assessment

After the end of the voting process, voters should be motivated to assess the system and the whole procedure, Voters feedback should be taken seriously into account for improving the system and the organization of the voting procedure.

2.14.4 Organize pre- and post- application information campaigns

Organizing an Information campaign before an e-Voting event improves Stakeholders' understanding of the usage of E-Voting system's capabilities and operation, while information gathered days after the E-Voting event helps them understand each other's views and propose improvements on the operation and usability of the system to reach an E-Voting System that will contribute to its improvements in order to face more demanding e-Voting procedures. In this way, E-Voting will be gradually established and trusted by citizens and the involved stakeholders.

2.15 Increasing E-Voting Voter Turnout

For increasing number of voter's participation the Author recommends including:
Young people, old people, people living abroad and blind / partially- sighted persons

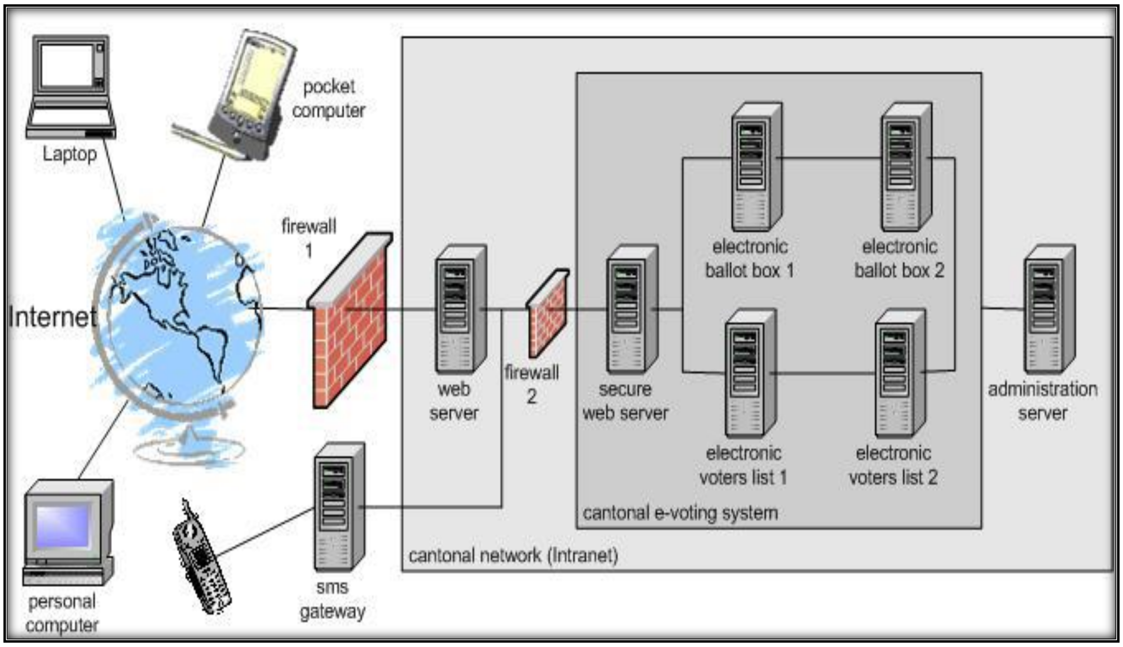


Figure (2.17) Risks / Security (Braun, N., Bundeskanzlei, BK, 2006)

As provided in figure risks such as interception, modification or loss of e-votes in the E-Voting process can be prevented by implementing several security layers encryption of each transaction as follows:

- Voter is prompted to check the digital finger print of the server certificate.
- System is redundant and protected by firewalls.
- Personal access and identification codes are altered for every Election Day.
- Frequent refresh of the domain name server during voting period.
- Special control devices and protocol filters for protection.
- Operators are alarmed and an emergency procedure is launched if any unexpected event happened.
- If the system stopped working the received e-ballots will be saved and the public will be informed to cast votes at polling stations (the voter gets a notice, that his vote has been cast but he/she must not be given a proof of its content else vote buying could take place.

2.16 E-Voting Future

Enfranchising Voters through new E-Voting channels

According to *(Scytl, 2009)* the Organization of American States and the Council of Europe**,** have established standards and guidelines on how to implement the internet voting in a secure and reliable manner to improve current E-Voting systems. Scytl collaborated with the Council of Europe in the security and audit standards set in September 2004.

Remote E-Voting (Internet Voting)

Internet voting is regarded by many governments as evolution of electoral processes because of its potential to increase voter turnout rates, facilitate the voting process and enfranchise voters such as overseas voters, military voters and voters with disabilities. Internet voting offers many advantages , including mobility and convenience for voters, greater speed and accuracy in the counting process, prevention of involuntary voting errors, better accessibility, lower costs, support of multiple languages and greater flexibility. Scytl's Internet voting solutions are based on the core security technology, Pnyx.core, ensuring the integrity, privacy and transparency of the election as follows:

Pnyx.Government

Pnyx.Government is an Internet voting platform for the public sector allowing all types of electoral processes (e.g., elections, consultations, surveys, referendums, etc.) to the organization through the Internet and other channels like mobile phones. *(Scytl, 2009)*

Secure & Cost-Effective Poll-Site E-Voting Technology

It consists of a comprehensive and modular platform that allows governments to introduce E-Voting in their electoral processes in a secure, reliable and cost-effective manner

Pnyx.DRE

Pnyx.DRE is an innovative poll-site E-Voting solution that turns a standard PC into a secure, accessible and reliable DRE E-Voting terminal. It can be used to carry out all types of electoral processes in a secure and convenient manner with the highest usability and accessibility standards. *(Scytl, 2009)*

Pnyx.VM

Pnyx.VM provides audit ability and redundancy to DREs through a secure and independent verification module, enabling voters to verify their votes before they are cast and recorded.

Pnyx.VVPAT

It is Voter-Verified Paper Audit Trail solution which cryptographically protects both the printed paper ballots and the corresponding digital votes.

Prime III

Prime III It is an electronic secure, open-source, multimodal electronic voting system that delivers the necessary system security, integrity and user satisfaction safeguards in a user friendly interface that accommodates all people regardless of ability. But it does not secure internet voting, and there is a physical separation between the user and the Prime III system as it is not located in the voting booth; it is in a separate partitioned area under guard. The user interacts with system through the touch screen and/or the headset. *(United States Election Assistance Commission, 2009)*

2.17 Summary / Conclusion

The idea of automating Traditional voting systems was to reduce the vote counting time, to insure that vote is being correctly accounted, to reduce fraud, to remove errors in filling out the ballots, and improve system usability for people with special needs. This approach raises several security issues, given that democratic principles depend on the electoral process's integrity. Beyond the traditional security properties (integrity, confidentiality, and availability), other properties need to be ensured. Some e-voting system requirements seem contradictory, like ensuring voter authenticity and vote anonymity, providing a vote-counting proof while preventing vote trade, allowing voting via the Internet but avoiding voter coercion, guaranteeing the uniqueness of the vote in decentralized voting, allowing vote automation while providing vote materialization, and ensuring audit ability in a software or hardware environment that could malfunction by implementing TPM as a security solution voters trust are gained which improves the voting process.

A widely available, inexpensive and easily used component on most devices. TPM is used to check PCs at start-up for any changes to the software used to run the computer and helps detect any suspicious code before the PC is booted and connected to the network. TPM stores keys, certificates and passwords securely and enables authentication and attestation, critical to trusted computing for E-Voting process. All voting systems rely on software for efficiency, usability, and accessibility, but software carries risk (including privacy) even for software independent verification systems, many E-voting systems cannot fully satisfy ease of administration, information assurance, and usability alone such as E2E systems. TCG increases privacy by ensuring the correct software is running. It enables excellent usability and accessibility by making it possible to build trustworthy electronic interfaces. And through implementing TPM (TCG) makes voting safer and Trust worthy for everyone at the cost of more complicated engineering design and key management. TCG specifications have been developed for many devices such as desktop and portable computers, mobile devices, storage devices, and the network itself, to ensure data protection, network security and protection against viruses, malware, and other attacks. This will ease the use of the multiple channels of E-Voting systems and increase the voter’s turnout.

Chapter- Three Research Methodology

3.1 Introduction

This chapter indicates the suitable research methodology and paradigm for conducting accurate data gathering and analysis to solve the problems of E-Voting system by suggesting a frame work based on the results of this chapter feedback. After conducting the literature review which has involved extensive search from secondary study such as journals, books and internet scholar website in general, the research gaps has been clearly identified. The next step in the sequence of the research is to define the research methodology and strategy.

3.2 Research Methodology Outlines

The research methodology to be followed for conducting this research is listed in figure (3.1).

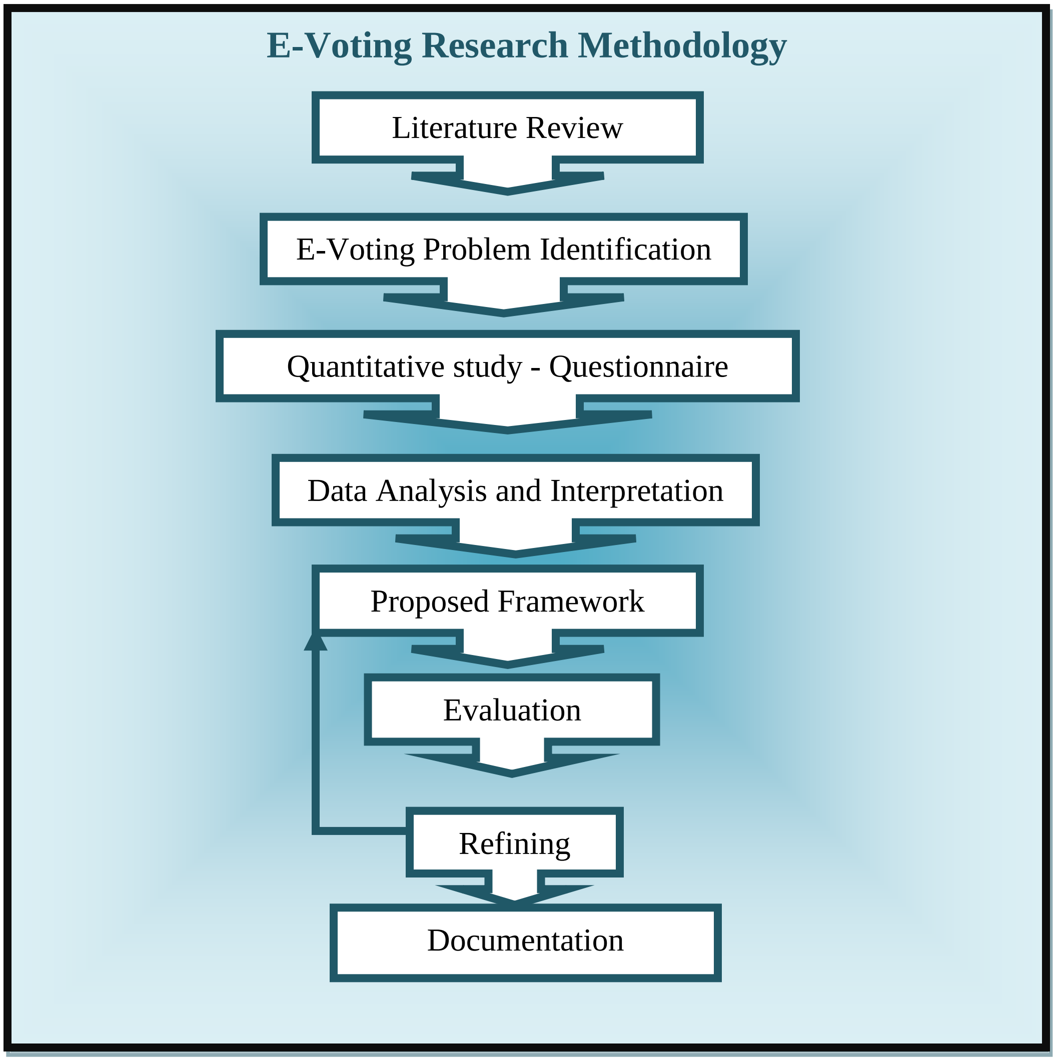

E-Voting Research Methodology
Literature Review
E-Voting Problem Identification
Quantitative study - Questionnaire
Data Analysis and Interpretation
Proposed Framework
Evaluation
Refining
Documentation

Figure (3.1) E-Voting Research Methodology

3.2.1 Literature Review Research Methodology

Data collection is the process of collecting data about the research. The objective of data collection is to collect data to identify the current status of E-voting system and the gaps to improve it. Based on the analysis of collected data framework will be produced and finally it will be tested by expert people to be approved. There are several data gathering techniques used to collect data such as interviews, survey, observation and focus group. The selection of data gathering techniques depends upon certain factors such as speed, time, cost, coverage and medium such as (internet, email based or physical paper based). In order to identify the selected area (Trustable E-Voting system) review of others work were conducted by:

Secondary Research Method that was achieved by gathering data according to existing information and related work done by others if the idea has been discussed before and if there is any documentation available from the organization or government documents. As long taken in consideration accuracy, consistency, credibility of secondary data and the methodology that used in secondary data collecting is from scholarly reliable resource. Secondary data are required to get information more accurate because would be support between actual statement, theories side and opinions. Secondary data can be collected from previous scholarly studies reports, surveys, from already done interviews, from literature, publications, internet, and broadcast media. Secondary research is much easier to gather than primary research but in this research both methods are used for making better decision.

Academic Research that was used to support primary and secondary research undertaken; it consists of Books, Journals and Internet. In this research most of the data was gathered through scholar websites such as *IEEExplore*, *ACM* and *Athens*.

3.2.2 Problem identification methods

The process of gathering data from a selected sample group on the basis of user profiling techniques to analyzed in order to prove the hypotheses. The designing research methods to be used are primary, secondary and academic research to get the accurate scholar information.

The Primary data collection method used to identify the research problems is questionnaire, because it is an easy approach to cover several people in a short time, it can be analyzed easily as it has close ended question, it is a quantitative method which can be interpreted into percentage, it saves time, as it can be delivered online or by paper and collected the same time or later which makes the respondent free to respond and relaxed, also the cost is low and can be distributed to large amount of people.

The sample selected was 10 expert people in the field of security and IT, as to evaluate the framework and the solution proposed based on their knowledge, and they preferred to have voting mechanism in their country. The objective of this research was to collect data from experts in security and IT fields. The expert people do not have time for large discussion interviews and they are difficult to locate. So through questionnaire data will be easily collected and it will consume less time. Another benefit of questionnaire is that the results are solid, because they produce quantitative result such as numbers that are easy to analyze. The process of questionnaire will be helpful in next chapter to analyze data. Interviewing is not selected as the process for data collection using this research because it is time consuming, and it is very difficult to locate expert people for large interval of time. Interviews produce qualitative results that are hard to analyze because in interviews people are free to give their ideas and opinions.

Observations also not selected as the data collection method for this research because this research is not related to any experimenting process or observation of any hypothesis. By considering the overall picture of data collection methods and undertaken research, Paper based Questionnaire is selected as the data collection method. The questionnaire will be forwarded to the expert people in form of paper; the answers will be collect to analyze the data.

3.2.3 Data Analysis and Interpretation Methods

In this chapter the feedback collected from questionnaire (1) will be prepared and analyzed, as the sample is small analyzing was done by EXCEL program, else it should be done by SPSS. The data was interpreted in tables, then pie and chart graphs. Percentage was provided for the quantitative data to illustrate it for better interpretation, then description of each graph, finally summary and findings of the analysis. This chapter is important to proceed with developing the proposed framework.

3.2.4 Proposed Framework

The methodology used for developing the proposed framework is based on analyzing the existing models of E-Voting system, in the literature review then finding the gaps to try to overcome it. The proposed framework will be described thoroughly in chapter (5).

3.2.5 Evaluation

The evaluation is very important step for testing the proposed framework, the method used for evaluation in this research, is by conducting another questionnaire for the same sample done in questionnaire one, second step is testing against the literature review existing modules, to be sure of the quality of the artifact and if it needs any improvement before final submission.

3.2.6 Refining

After doing the evaluation of the framework proposed, comparison between the objectives, deliverables and what has been achieved, if the result is matching then proceed with documentation, else improving and testing the framework again and so on.

3.2.7 Documentation

Final step after refining , evaluating and testing the framework , documenting the research is done under the guidelines of minimum requirements of research documentation of UCTI university, and the revision of the Master supervisor “ Mr., Ali Dehghantanha”, the referencing was based on Harvard referencing , Text Body font “Times New Roman (12), Headers “ Cambria” ranged from 13-16 . Finally graphs where either copied from online resources or drawn. This research is done as a partial fulfillment of the requirements of Staffordshire University for Master Degree in Information Technology Management.

3.3 Research approach

E-Voting system is a challenging approach for increasing Electronic Participation. However, lack of citizens' trust is the main obstacle that prevents its successful realization**.** Research approach can be two types deductive or inductive, selected approach is deductive as it has a general theory and based on that theory hypotheses will be formed to be tested in order to support the research theory, if the hypothesis is supported then the research theory is proved. It is an approach which starts from top to bottom. **Deductive** includes the quantitative data analysis that is easy to analyze as compared to inductive approach it supports qualitative analysis and it is not suitable because it is specific bottom to top approach which produces conclusions that are only probably true or false. The E-Voting system approach is based on these components:

3.3.1 The decomposition of E-Voting systems into "layers of trust" for reducing the complexity of managing trust issues in smaller manageable layers.

3.3.2 Identifying and documenting security critical aspects of the E-Voting system, and a cryptographically secure E-Voting protocol.

3.3.3 Defining and building people trust as positive attitude towards a system that performs its operations transparently.

3.3.4 E-Voting system must be usable by people regardless of their age, education, infirmity, or disability.

3.4 Research Philosophy -Paradigm

There are many research Paradigms (philosophies), each paradigm contains methodology that uses two or more methods of research to collect data. The research paradigm selected is **Positivism** because it is based on Evidence of formal proposition, Quantifiable measures and Hypothesis testing (*Bolan, C., Mende, D., 2004)*, however if comparing with other paradigms that are commonly used such as Interpretivist and critical paradigm, **Interpretivism** is not suitable for conducting the research because it depends on Ethnography study, observation method , interviews. It is a subjective inductive qualitative approach that is hard to measure, and the **Critical paradigm** depends on historical and field research.

3.5 Research Methodology

The research methodology selected is **Exploratory** because its informal unstructured research that aims to define and clarify the problem of the research conducted and to develop hypotheses which is what is needed to do the research, while the descriptive and causal approaches are not useful as **Descriptive** specifies a phenomena at a point of a time and the phenomena as they exist. In Descriptive methodology data is often quantitative and statistics applied. It is used to identify and obtain information on a particular problem or issue. **Causal** is to determine causality *(Cooper, D, Schindler, P 2003).*

3.6 Research Design

The research design focuses on trustable E-Voting management system, that includes online voting and electronic through devices voting. The proposed framework describes the electoral environment. Pre-voting, voting, and post-voting in terms of managerial and technological procedures with the implementation of TPM. The framework was developed based on literature review by searching scientific papers on the E-Voting systems, and on quantitative questionnaires from selected security experts to get their feedback.

3.7 Justification of research Paradigm and Methodology

The purpose of this research is to produce a "Trustable E-Voting system framework using TPM"; to achieve this aim accurate and reliable feedback should be collected based on primary and secondary research methods. Primary Research will be conducted using Questionnaire which will include Mono quantitative method. Qualitative research offers insights and understandings of participants, which is unobtainable by quantitative research. Qualitative methods can highlight key themes or patterns emerging in the project, are used to comprehend and manage data and used to develop and test hypothesizes.

There are weaknesses with qualitative research method that, their result is less easily generalized than with quantitative methods, which is much easier and accurate to analyze. Qualitative research involves the use of qualitative data such as interviews, direct observations, survey and analysis of documents and material. **Quantitative** Questionnaire and literature review are the research method used for developing Framework for trustable E-Voting system using TPM.

3.8 Time Horizon

In time horizon there are two types cross sectional and longitudinal, Cross sectional is a research that is done within a short period of time. The method used in this research is cross sectional because the feedback has to be collected from the experts in short period of time, first questionnaire is given to them to identify the current E-Voting problems and to analyze their acceptance of the suggested solution. Then a second questionnaire will be given to them to evaluate and test the framework suggested within the time limit. While Longitudinal is done in a long period and carried repeatable and for projects that needs to be evaluated multiple times in different times *(Cooper, D, Schindler, P 2003).*

3.9 Ethical Consideration

The research problem investigate does not involve physical or psychological harm or damage to human beings or organizations. The people's privacy is protected and not revealed, it is strictly confidential. The respondents were confirmed about the nature and purpose of the study, they are free to respond or refuse and to feel free to skip any question they dislike so the standard ethical principles are fulfilled such a (No harm to participants, Voluntary participation and Informed consent Anonymity; Confidentiality and No deceiving subjects).

3.10 Conclusion

This chapter has discussed various options available for the execution of the field of the research and the logic for the selection of the specific approach, strategy and methods applied in this research project. Upon it the research paradigm selected was positivism; Methodology was deductive, methods questionnaire, with longitudinal time horizon for best suitable processes in research design methodologies to proceed with data analysis.

CHAPTER-FOUR

DATA ANALYSIS

AND

INTERPRETATION

4.1 Introduction

Data analysis is considered as an important part of research; as to analyze the necessity of proposed Framework, to test the effectiveness of the proposed Framework by questionnaire the experts; and to evaluate the effectiveness of the proposed model. The initial step of this chapter begins from quantitative analysis part where the gathered data will be prepared and analyzed, and all diagrams will be presented by utilizing Microsoft Excel tools. Each diagram analysis and description will be shown. The method followed was through primary research (Questionnaire). The data analysis consists of two sections, first the sampling is done by selecting (10) experts in security and IT field, and questionnaire conducted, second is descriptive statistical analysis in order to proceed with delivering a Trustable E-Voting Management Framework using TPM.

4.2 Users Profiling-(Characteristics of the Respondents)

To fulfill the objective of this research, two questionnaires were conducted, first for problem identification, the second for suggested solution approval feedback. The aim was to involve the experts in the field of security and take their opinion on the current E-Voting system status, and to get their testing and approval of the project deliverable frame work.

The sample was selected from UCTI university as a win award university, and as it has many expert lecturers in the field of security from different countries, which is a benefit to enrich this research because of different culture and different usage of E-Voting channels , this will give depth in the results of data analysis. The sample was collected from ten (10) experts in the field of security and software engineering from different countries, and different education level but with working experience, working in UCTI University.

4.3 Questionnaire (1) Problem Finding

4.3.1 Question one (Education level)

Question one (*Kindly specify your education?*) aims to know the level of education as the sample is based on experts opinion. The figure below shows the percentage of experts who responded to questionnaire is as follows:

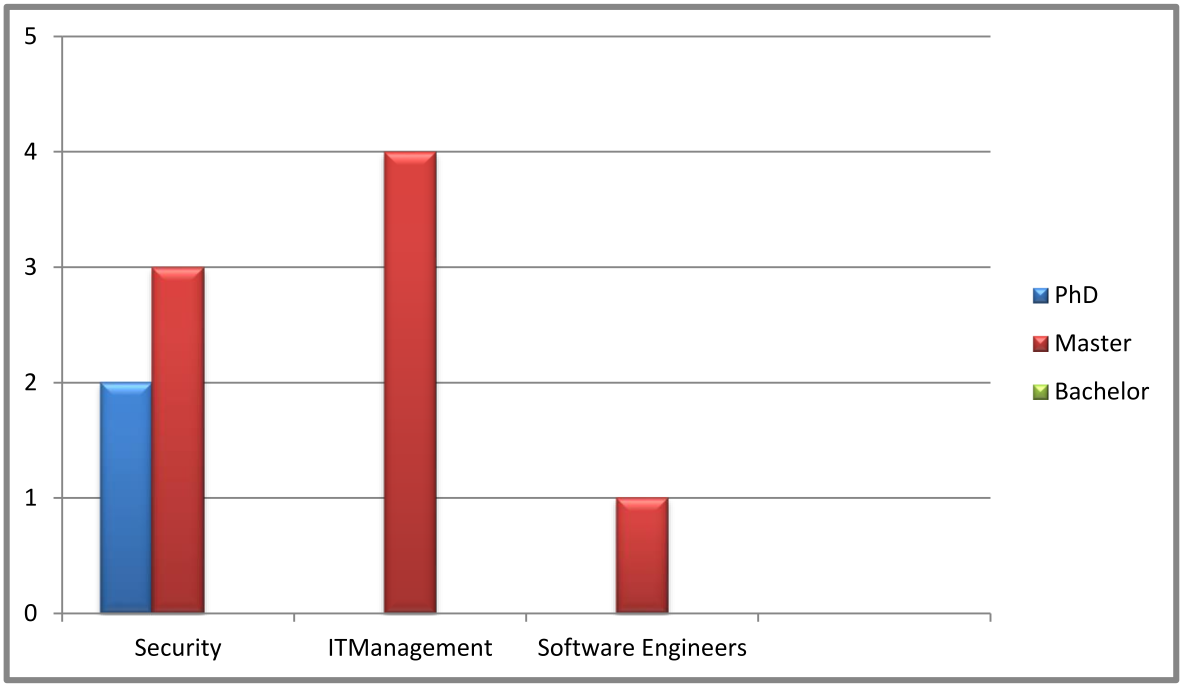


Figure (4.1) Education

Description

As indicated in the figure (4.1), the data analysis for (10) experts people education level was 20% PhD level and 30% Masters in Security field , 40% Masters in IT Management, and 10% in Software engineering to ensue the knowledge and depth of the research solution and testing the deliverable.

4.3.2 Question Two (Nationality)

Question two (*kindly specify your nationality?*) aims to know the nationality of the experts as it is important that they have knowledge about E-Voting Systems to be sure of the accuracy of their feedback.

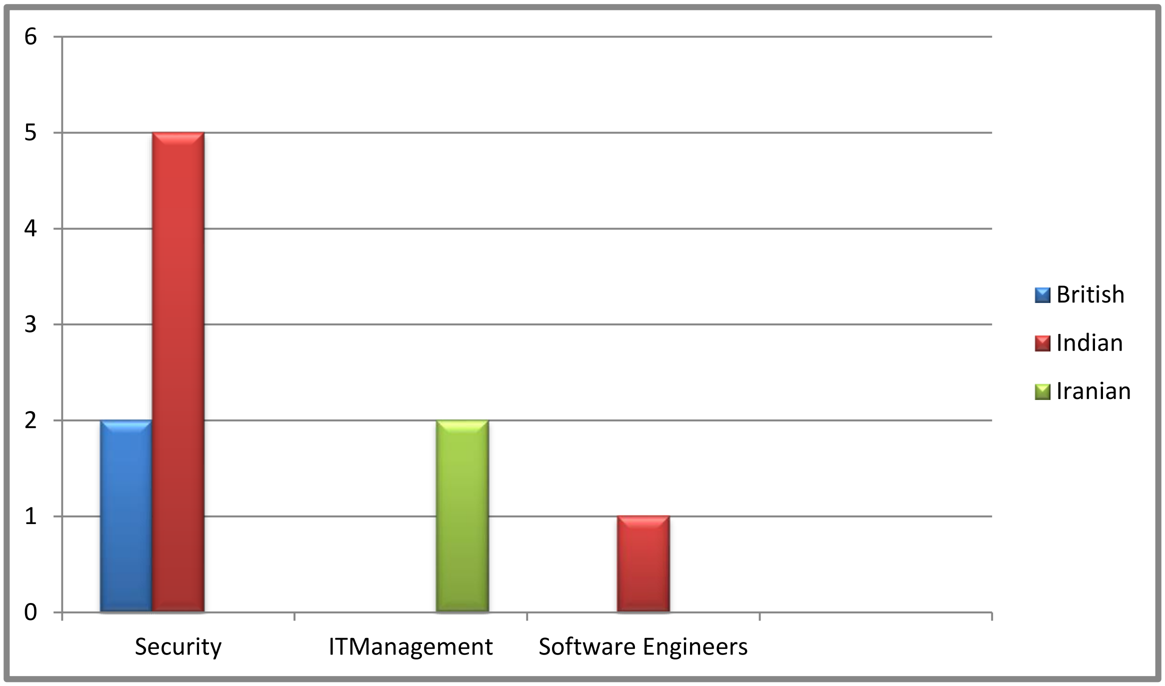


Figure (4.2) Nationality

Description

Different Nationality responded to the survey questionnaire which have experienced election in their countries, 20% from United Kingdom in the security field and PhD degree holders as indicated in the previous figure (4.1) , 60% were Indians and Master Degree Holders both fields (50% Masters in ITM and 10% Masters in Software Engineering) finally 20% are Iranian that have major issues in their election process so their feedback will be powerful for identifying the problems in E-voting System they were from the field of IT Management.

4.3.3 Question Three (E-Voting Channels)

Question three (*kindly circle and rate your preference of the existing E-Voting channels used for conducting election in your country?*) aims to know the E-Voting system methods that is used to cast votes, and which is mostly preferred and why? To proceed with finding the issues that is related to lacking of trust in the current system as was described in the literature review chapter 2

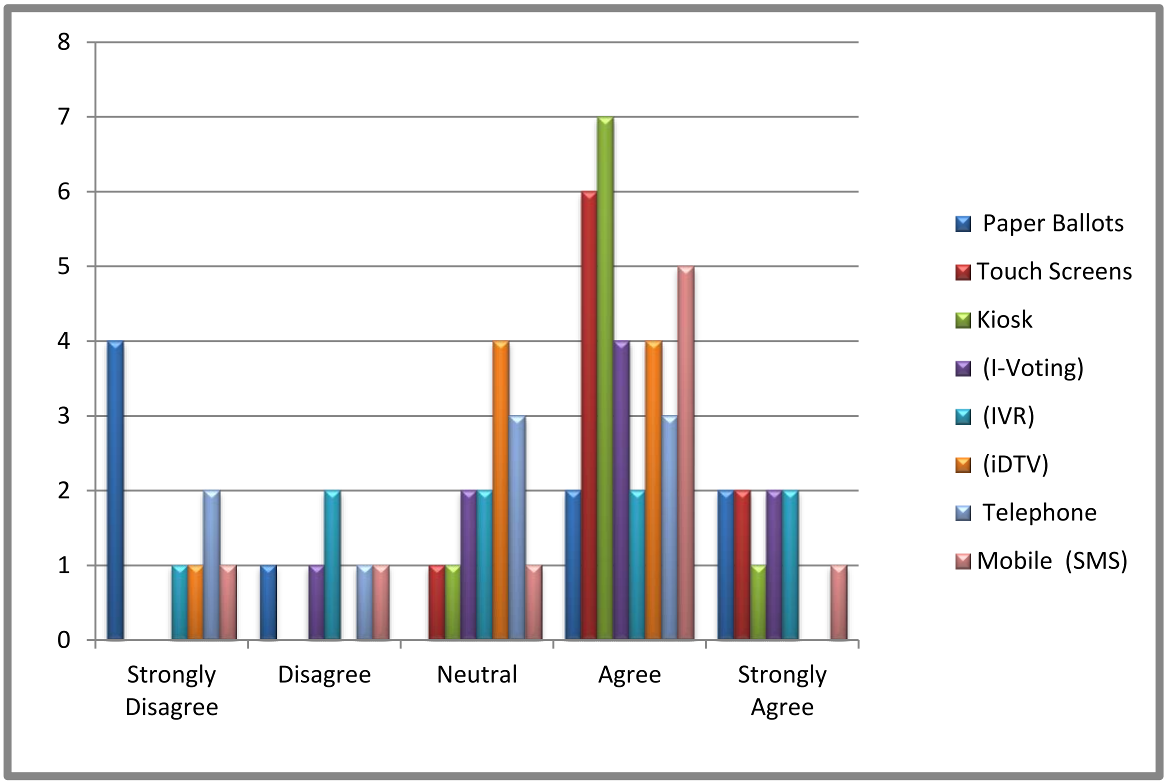


Figure (4.3) E-Voting Channels

Description

As for experts preference of voting methods the figure shows that mostly agreed on Kiosks and touch screens, which are conducted physically at the polling places , but for absentees or people who are not available for some reasons such as out of the country these methods are not suitable. They strongly disagreed on landline telephone, interactive digital TV (iDTV) and other channels that will be described individually below, but these channels are important for cases such as disabled people or unavailable people and their votes are needed so they cannot be ignored.

The following section will describe the E-voting channels in a pie figure for each channel from the figure in (4.3) to be analyzed.

Paper Ballots

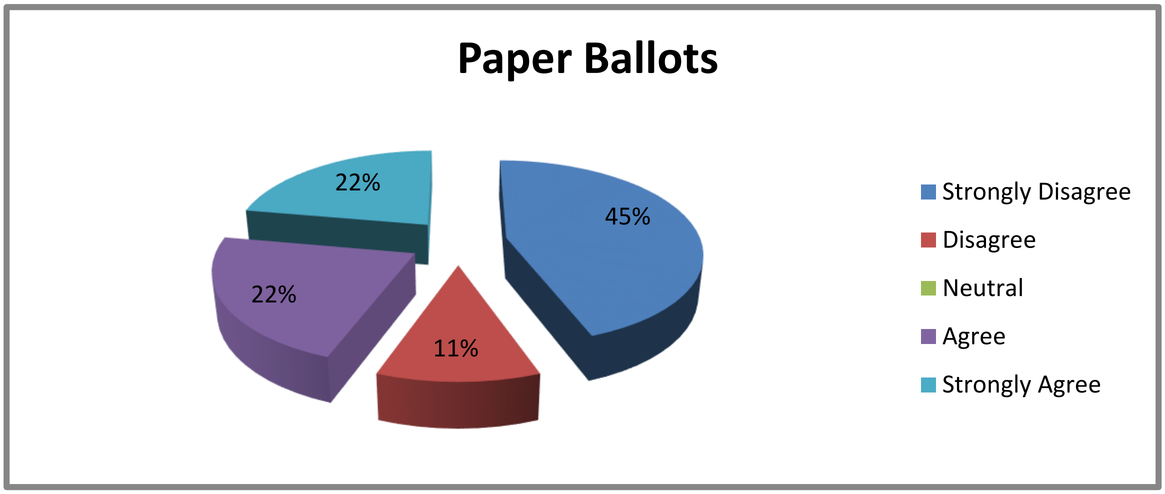


Figure (4.3.1) Paper Ballot

Description

In this figure 45% of experts strongly disagreed, 11% disagreed on the traditional paper ballot. While 22% strongly agreed, and 22% agreed on the usage of paper ballots.

Touch Screens

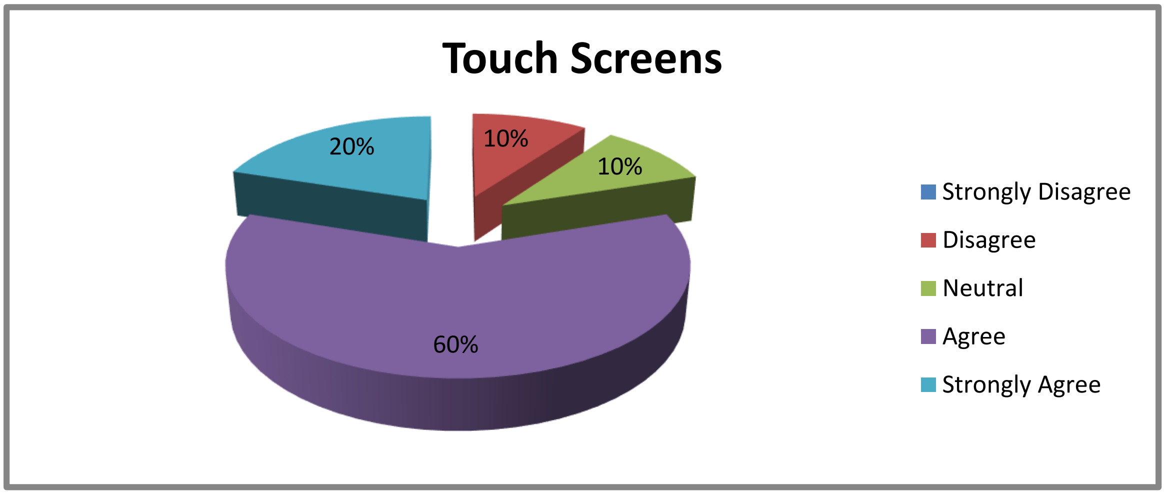


Figure (4.3.2) Touch Screens

Description

Most of the experts agreed 60% and strongly agreed 20%, which indicate that they prefer touch screen for casting votes, while 10% disagreed and 10% were neutral.

Kiosk

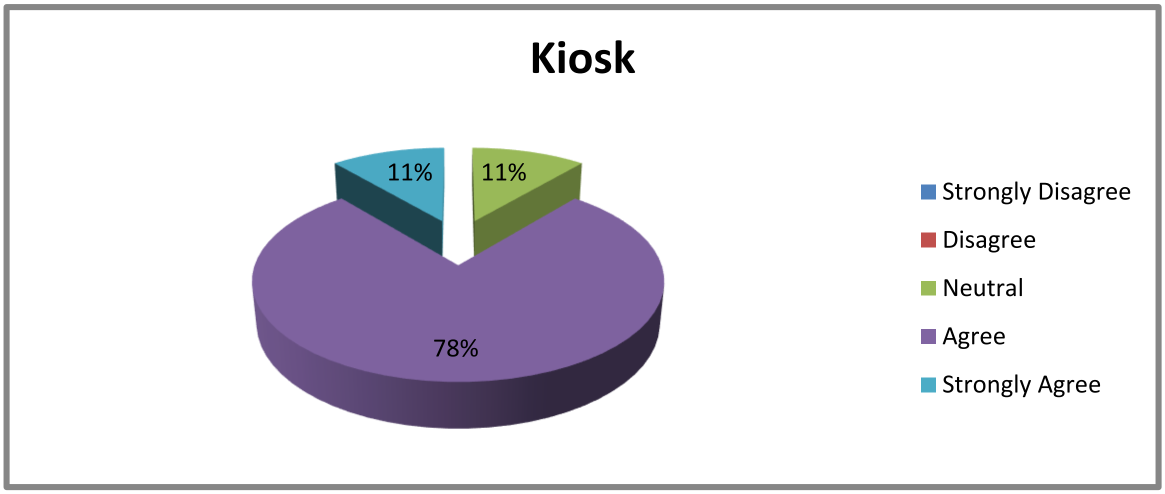


Figure (4.3.3) Kiosk

Description

Most of the experts agreed 78%, and strongly agreed 11%, which indicate that they prefer kiosk for casting votes, while 11% were neutral.

Internet Voting (I-Voting)

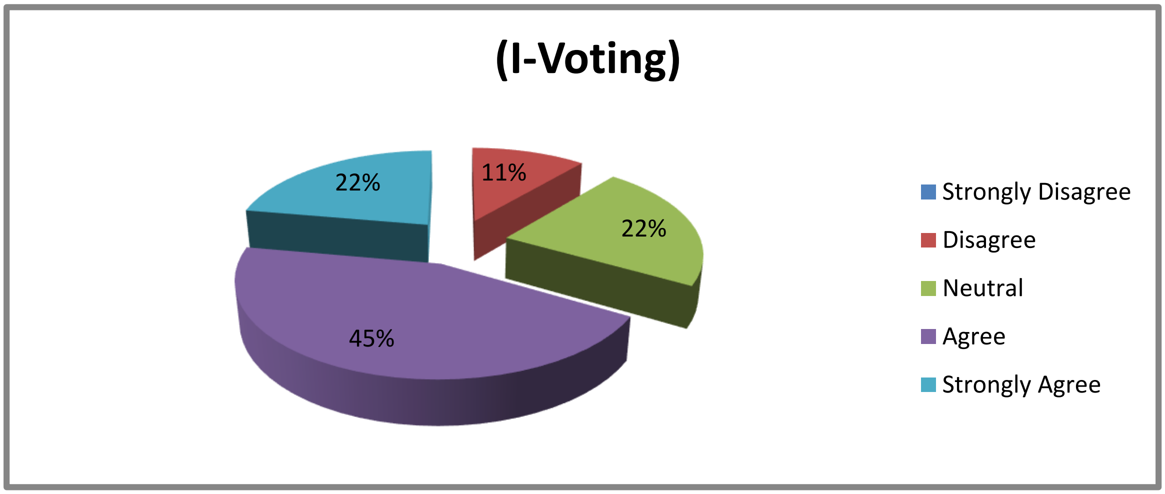


Figure (4.3.4) I-Voting

Description

Most of the experts agreed 45%, and strongly agreed 22%, which indicate that they prefer internet voting for casting votes, while 11% disagreed and 22% were neutral.

Interactive Response (IVR)

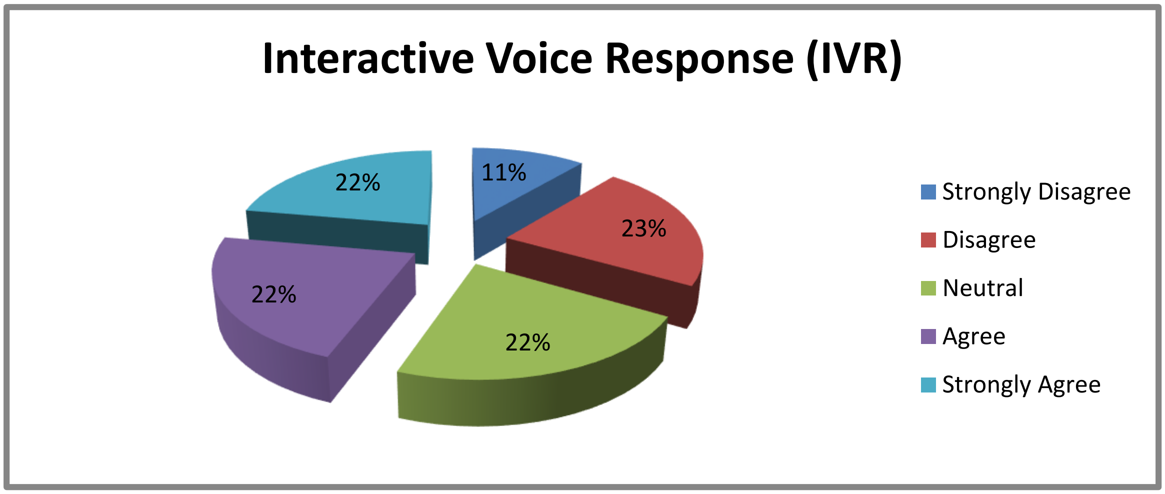


Figure (4.3.5) IVR

Description

Interactive Response (IVR) has 22% strongly agreed and 22% agreed, while 11% strongly disagreed and 23% disagreed, 22% remain neutral.

Interactive Digital TV (iDTV)

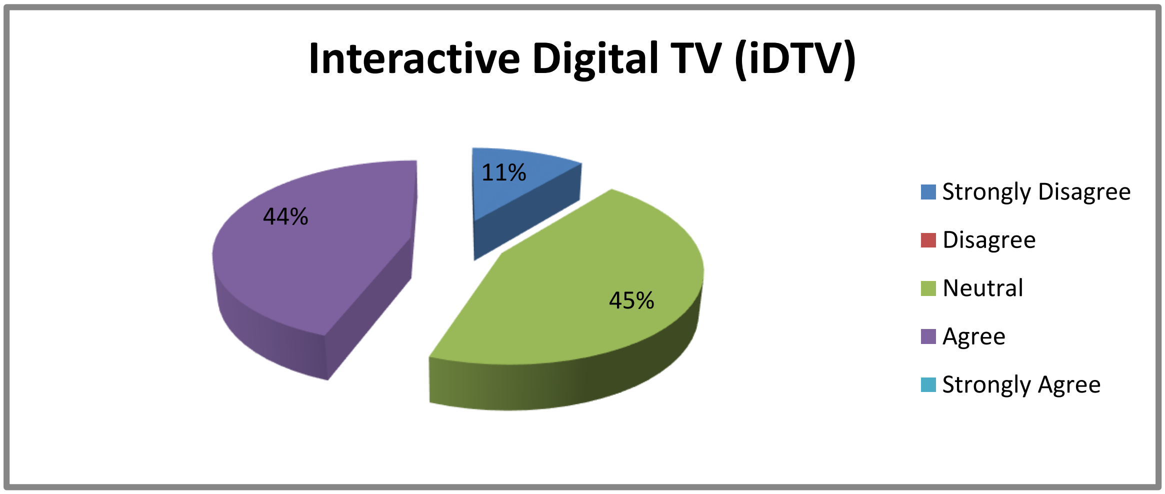


Figure (4.3.6) (iDTV)

Description

Interactive digital TV (iDTV) has 44% agreed, while 11% strongly disagreed, still 45% remain neutral.

Land line Telephone Voting

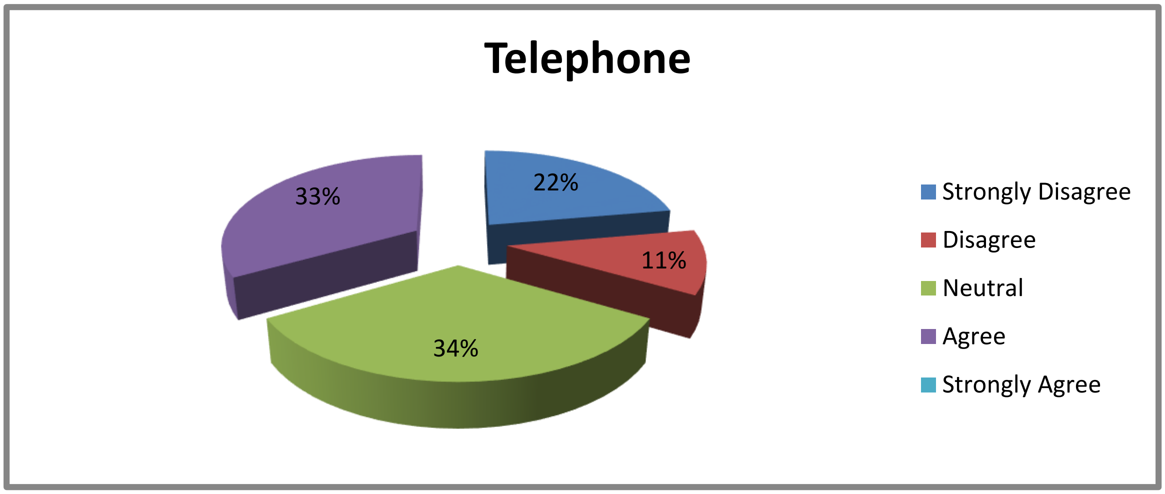


Figure (4.3.7) Telephone

Description

Landline Telephone Voting has 33% agreed, while 22% strongly disagreed and 11% disagreed, 34% remain neutral which shows telephone is not preferred.

Mobile Voting (SMS)

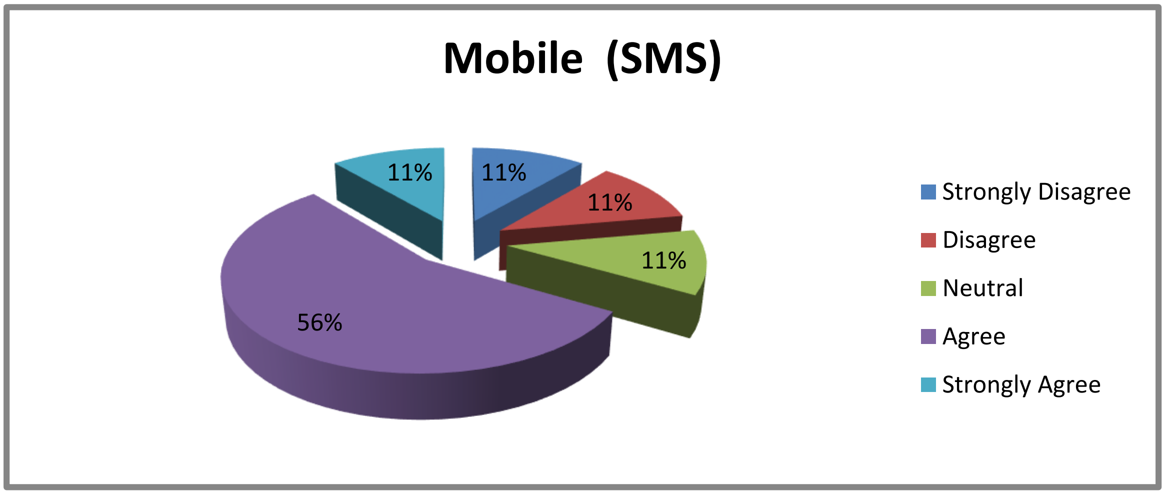


Figure (4.3.8) Mobile (SMS)

Description

Mobile Voting (SMS) has 11% strongly agreed and 56% agreed, while 11% strongly disagreed and 11% disagreed, 11% remain neutral which shows that Mobile voting via (SMS) is preferred.

4.3.4 Question Four (E-Voting Problems)

Question three (*kindly circle and rate the seriousness of the problems according to the existing E-Voting System?*) aims to know the E-Voting system problems that affects the voting turn out and decreases the level of voters trust .

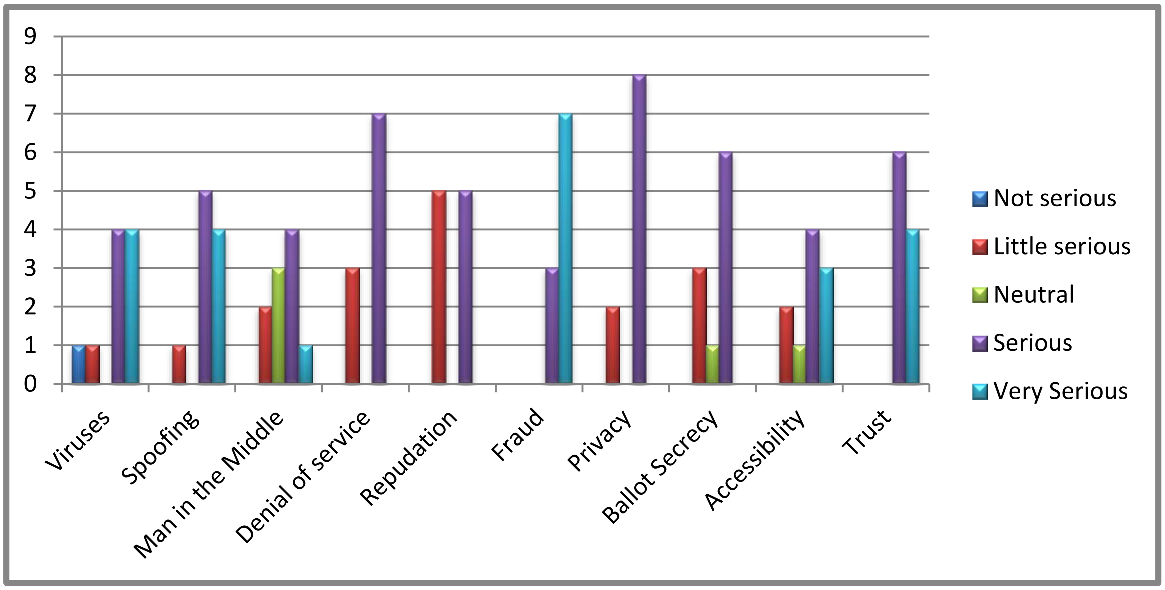


Figure (4.4) E-Voting Problem

Description

In this figure fraud is shown as a very serious problem (70%), then viruses, spoofing and trust (40%), while accessibility (30%) and man-in-the-middle (10%). The serious issues were privacy with percentage of (80%), Denial of service (70%), trust and ballot secrecy (60%), repudiation (50%), while accessibility, man-in-the-middle and viruses were with percentage of (40%). Percentage of respondent who claimed that repudiation is little serious were (50%), ballot secrecy and denial of service (30%), man-in-the-middle, privacy and accessibility (20%), while spoofing and viruses with percentage of (10%).finally (10%) responded that trust is not serious problem. The following section will describe the E-voting channels in a pie figure for each problem from the figure in (4.4) to be analyzed.

Viruses, Key Logger and Hacking

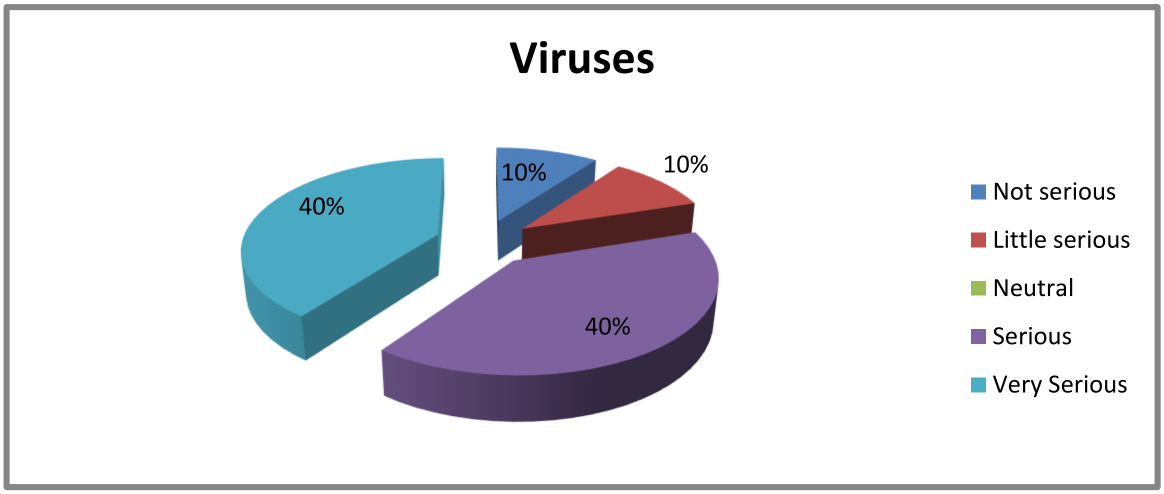


Figure (4.4.1) Viruses (Hacking)

Description

40% of experts indicated viruses, key loggers and hacking are very serious problems, 40% serious, while 10% responded as little serious, 10% declared that they are not serious problems.

User Spoofing

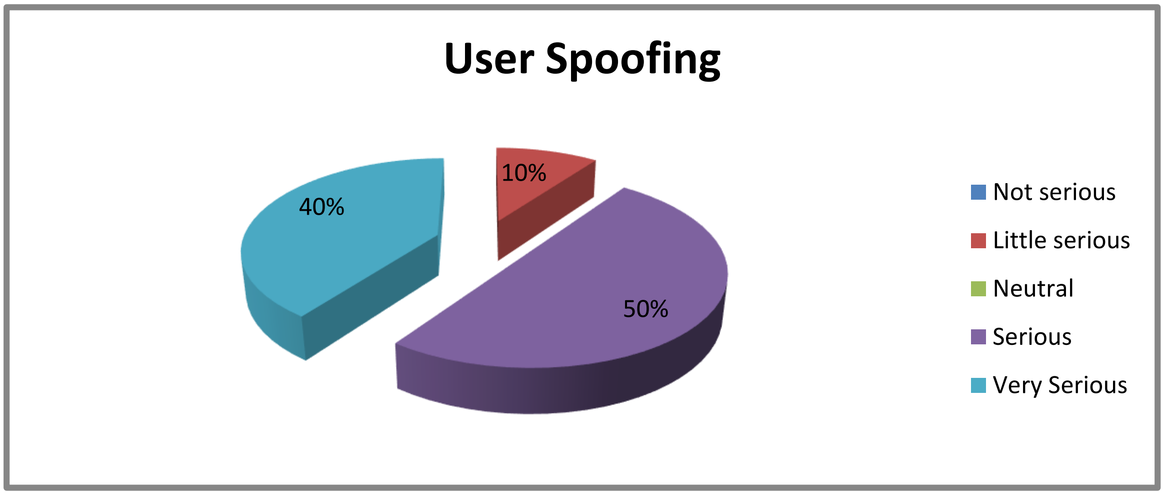


Figure (4.4.2) User Spoofing

Description

40% of experts indicated user spoofing is very serious problem, 50% serious, while 10% responded as little serious.

Man- In –The- Middle

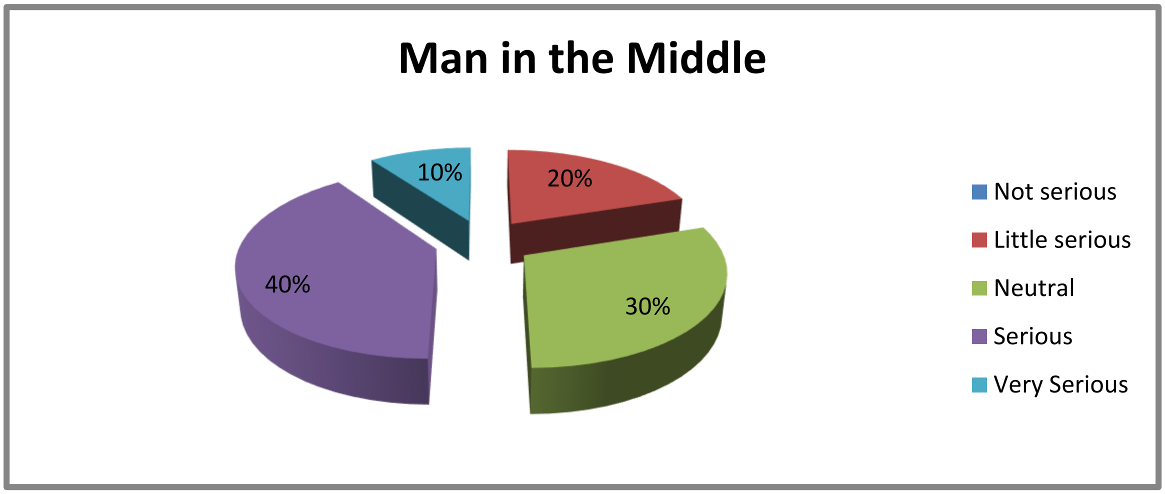


Figure (4.4.3) Man-in- the- Middle

Description

Man in the middle attack is a serious issue because it steals the data without noticing especially for internet voting. 10% selected very serious and 40% selected serious, 20% little serious, while 30% were neutral.

Denial of Service

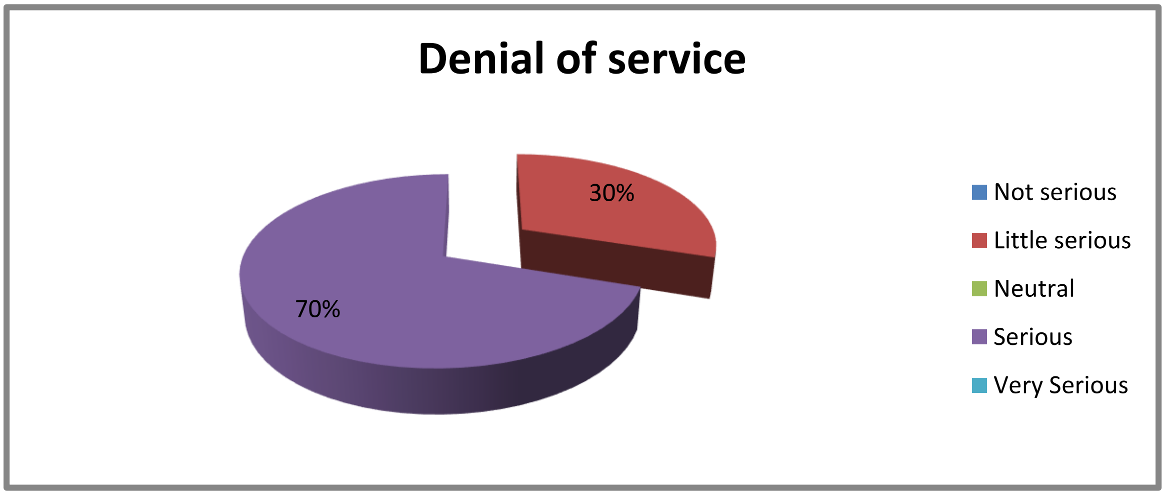


Figure (4.4.4) Denial of service

Description

70% experts declared that Denial of service is serious problem and 30% was little serious which makes it serious factor to be prevented.

Repudiation

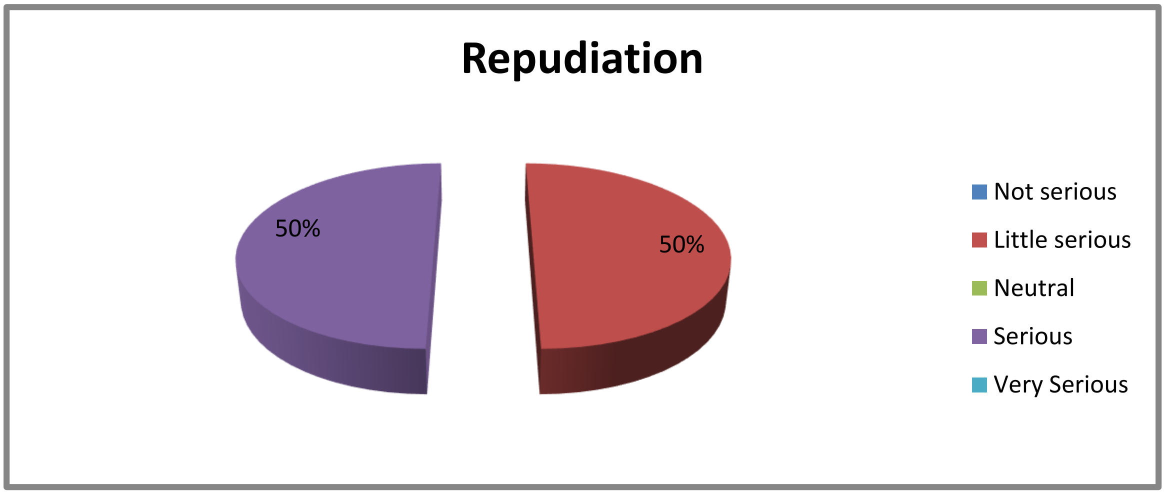


Figure (4.4.5) Repudiation

Description

50% experts declared that repudiation is serious problem, 50% responded that it is little serious.

Fraud

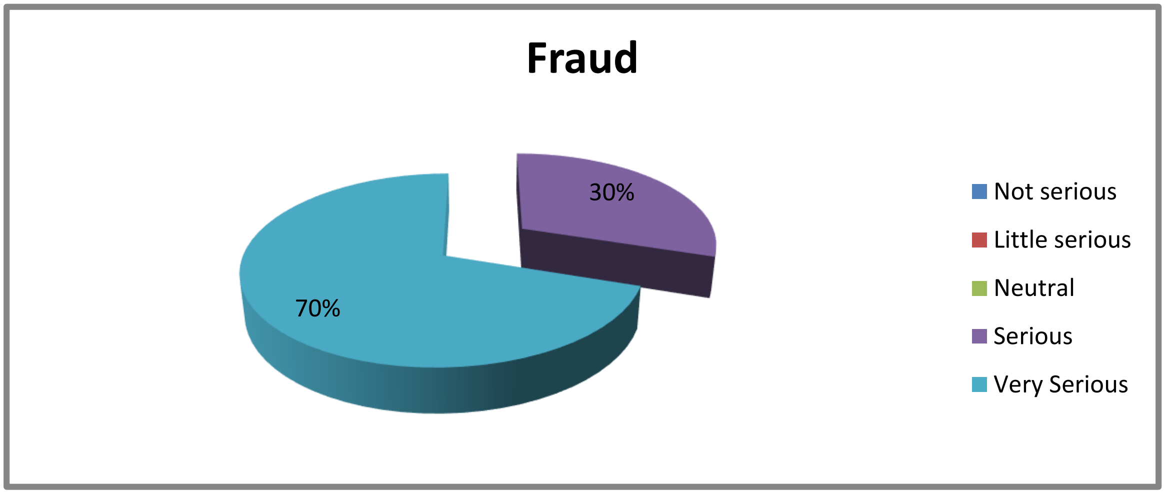


Figure (4.4.6) Fraud

Description

Fraud is a very serious problem even 70% from the experts declared that it is very serious issue, and 30% selected serious which makes it 100% serious factor to be avoided for the success of E-Voting system.

Privacy

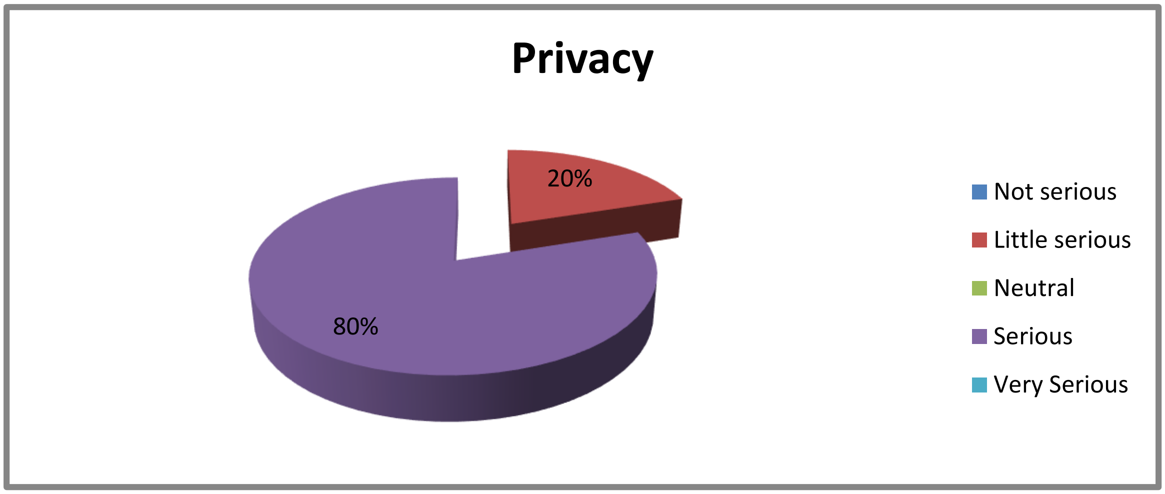


Figure (4.4.7) Privacy

Description

Privacy issue is declared serious problem with percentage of 80% and 20% little serious which shows that privacy is an important factor to achieve in E-Voting system.

Ballot Secrecy

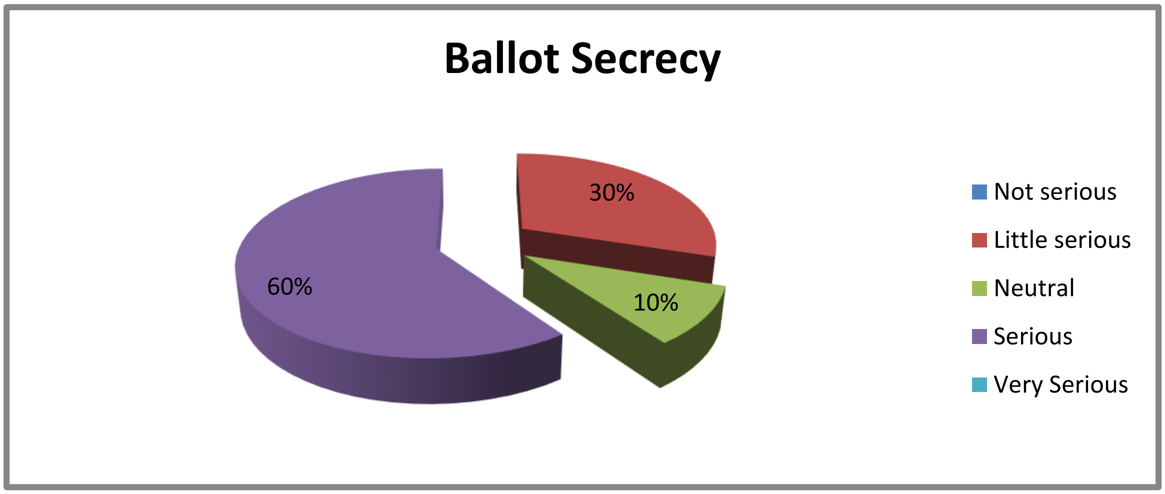


Figure (4.4.8) Ballot secrecy

Description

Ballot secrecy issue is declared as serious problem with percentage of 60% and 30% little serious which shows that ballot secrecy is an important factor to achieve in E-Voting system. While 10% were neutral.

Accessibility

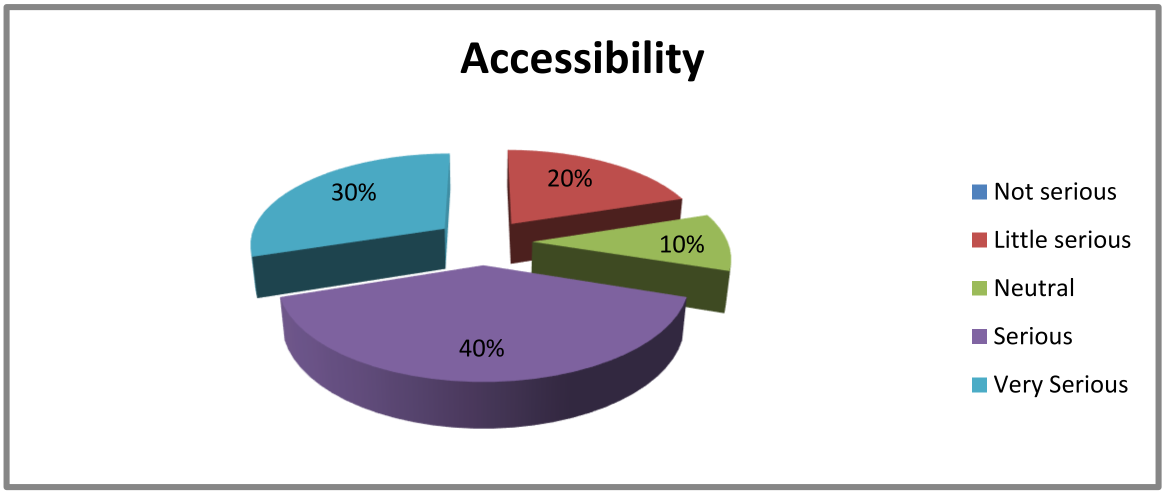


Figure (4.4.9) Accessibility

Description

Accessibility issue is declared serious problem with percentage of 40%, and 30% very serious. While 20% responded little serious and 10% were neutral.

Trust

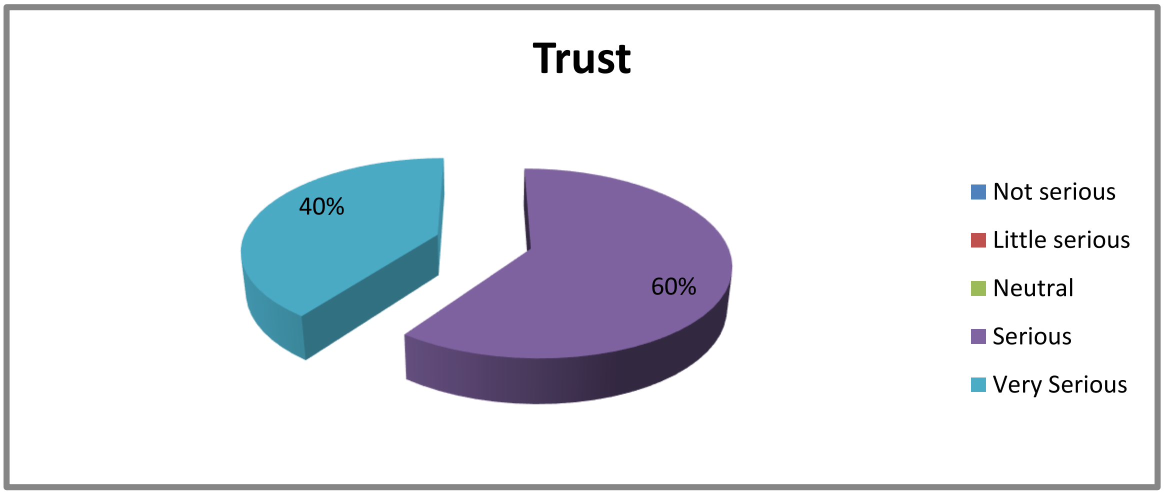


Figure (4.4.10) Trust

Description

Almost 100% declared that trust is a serious issue but the level of seriousness varies as 40% declared it is very serious issue the rest 60% answered it is serious issue**.**

4.3.5 Question Five (TPM Proposed Solution)

Question five (*kindly circle and rate the level of your preference in implementing Trusted Platform Module (TPM) to enhance the security and increase voters trust in the election process?*) aims to know the experts acceptance of TPM to be implemented in the E-Voting system framework to optimize the security in a cost effective way .

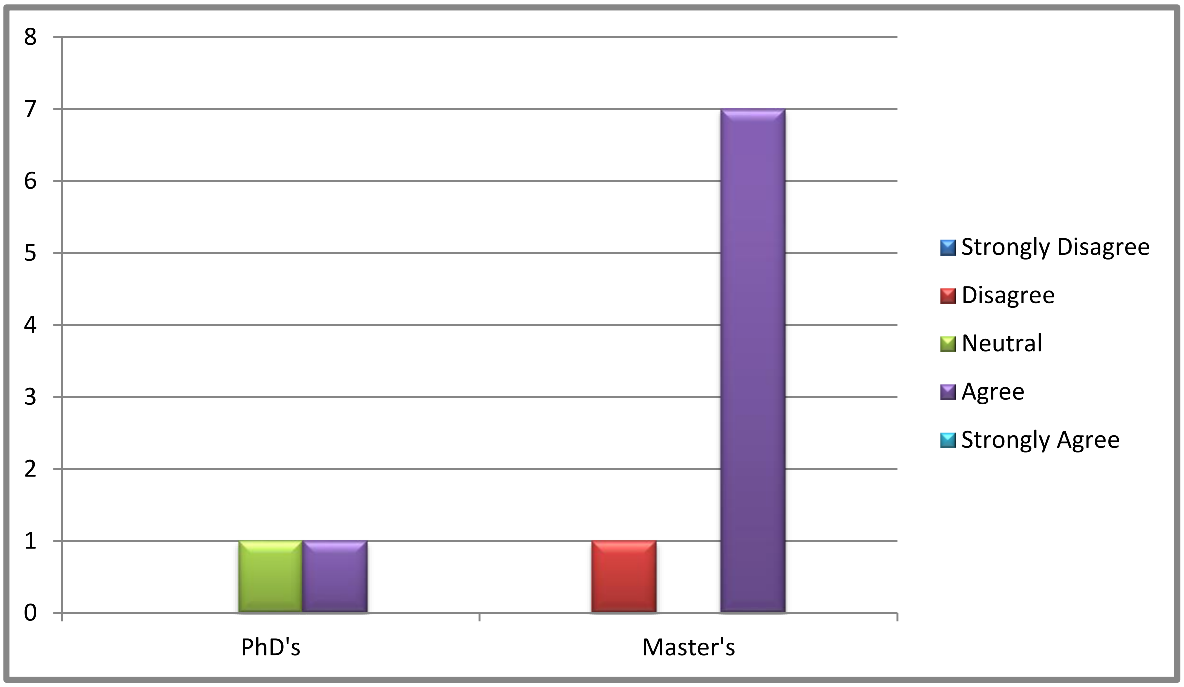


Figure (4.5) TPM – Solution

Description

As shown in the figure (4.5), 10% PhD experts and 80% Master Degree experts agreed on the usage of TPM in E-Voting system; as a trusted platform tool to enhance the system security, while 10% Master Degree security experts disagreed, the rest 10% PhD degree security experts were neutral.

4.4 Summary of Data Analysis _ E-Voting Questionnaire

In the table below a description of each question analysis and conclusion is provided in order to proceed to developing the deliverable framework to fulfill the aim of this research. Table (4.1)

E-Voting Channels		
Channel	**Percentage of preference**	**Conclusion**
Paper Ballot	44%	Touch screen and kiosk are highly preferred as voting channel , next are internet voting and mobile (SMS), the rest ranged between 33%-44% which indicates that kiosk, touch screens and internet voting channels are important and should be considered when developing the proposed framework.
Touch screen	80%	
Kiosk	89%	
Internet voting (I-Voting)	67%	
Interactive Voice Response	44%	
Interactive Digital TV	44%	
Telephone	33%	
Mobile (SMS)	67%	
E-Voting Problems		
Problem	**Percentage of seriousness**	**Conclusion**
Viruses ,Key logger	80%	All the problem are considered serious as the percentage declared the most important problems were fraud and trust that effect the voting process, then comes the issues of user spoofing , viruses and privacy, the rest are ranging between 50% and 70% which indicates the seriousness of these issues for the need to optimize the security to overcome these problems.
User spoofing	90%	
Man in the Middle	50%	
Denial of service	70%	
Repudiation	50%	
Fraud	100%	
Privacy	80%	
Ballot secrecy	60%	
Accessibility	70%	
Trust	100%	
Experts approval for TPM solution		
Degree	**Percentage of preference**	**Conclusion**
TPM	69%	High acceptance for TPM usage.

4.5 Findings of the analysis

The quantitative questionnaire analysis finding that there are serious problems in the E-Voting system. Security issues are vital to the election process, lack of trust because of insecure hardware and software E-Voting system, the vulnerability to threats and attacks will decrease the voter's turnout that will affect the voting results negatively. The touch screen and kiosk is favorable channel for voting as it serves wide range of people, disabled, young citizens, old people, any voter who is attending physically at the polling place, because of their usability and ease of use. While the internet and mobiles also were with high preferred methods as voters can access from anywhere any time which will increase the voting turnout. However the issues of security prevents or decrease voters acceptance to vote because the voter does not trust the system, so the proposed solution was to enhance the security with usage of trusted platform from trusted computing group with highest standards with low-cost. The majority experts agreed on the TPM solution proposed.

4.6 Conclusion

To fulfill the objective of research literature review was conducted, methodology of study was selected and questionnaire was done, the data analysis and interpretation is very important to measure the feedback and proceed on developing the project artifact deliverable. This chapter presented the complete data analysis with illustration of tables and graph's.

CHAPTER-FIVE

FRAMEWORK

5.1 Introduction

In order to proceed with developing the research deliverable framework there will be some points to consider, First consideration time and space, as the E-Voting process is bounded with limited time and the location which voters should be available physically at the polling station, also according to culture some countries differentiate between men and female in the polling place these points are indirectly effecting the framework because managing a trustable E-Voting system includes all participants so , there have to be many channels managed and secured to overcome these issues. These channels can be internet voting from a computer, voting by SMS on a mobile telephone, voting by telephone using the telephone keypad, voting by means of interactive television, or Interactive Voice Response. To gain high voting turnout and client trust the E-Voting system must be highly secured and usable.

Based on the literature review done (chapter two) many security issues were found and still E-Voting systems needs to be optimized according to their usability and security. Suggested solution was implementing TPM. Following table will be a brief description about related work of implementing TPM and the weaknesses that should be overcome.

5.2 Benefits of Data Analysis and Interpretation

The data analysis is very important to get feedback about the actual current E-Voting status. In this research problem in E-Voting systems were identified, by searching and reviewing secondary scholar resources, to find the gaps and the problems identified by others, also what is the current status for E-Voting systems. After that a quantitative study by questionnaire was done to get the feedback about the problems found. By analyzing the feedback many problems related to security was found serious, the suggested solution TPM as a trusted platform to optimize the security and solve the E-Voting problem was highly accepted by experts, which helps in proceeding with developing the Framework artifact.

5.3 Use of Literature Review in creating artifacts

The evidence on the importance of the existence of secured trustable E-Voting system is presented by the literature review done in chapter two, through the review of work done by others, the different protocols and methods used for developing secure E-Voting system. The gaps were identified; a discussion on related work was made only on the implementation of TPM to find the gaps and to proceed on developing the proposed framework for trustable E-Voting management system. The proposed framework addresses the issues that were highlighted in the literature review, such as security issues that effects voters trust and decreases the E-Voting systems turnout. The proposed framework recommends the implementation of trusted platform module as a solution to optimize the E-Voting system security.

5.4 E-Voting Management Framework Security Requirements

E-Voting system process is achieved in three stages that have to be managed from every perspective in efficient effective way with highest quality of service, as it is a vital operation that costs money, effort, time and the result of this process if not accurate will be a disaster, as it is a decision on nations preferred leader. Millions of legal citizens have to vote, but the trust is a critical success factor for the voters to cast their votes. Achieving trust in the system and the technology is hard issue, because E-Voting is socio-technical that means it is a system that is based on humans and technology integrated together. A lot of fraud and hacking is found for many reasons and for the benefit of many people politics or regular illegal people.

The basic security requirements have to be implemented in the proposed E-Voting system. These security requirements are set as security objectives in order to gain the highest level of secure trustable system, as listed below: *(Xenakis, A., Macintosh, A ,2004).*

5.4.1 Effective voter registration: permission is granted to good faith people and systems.

5.4.2 Effective voter authenticity: services are only available to those eligible to vote.

5.4.3 Effective voter anonymity: Identity of the voter cannot be established with the exception of the ability to warrant under law votes cast.

5.4.4 Effective vote confidentiality: E-Voting must guarantee the confidentiality of the vote until it is counted.

5.4.5 Effective system identification and authentication: Accountable E-Voting service processes are only accessible to authorized people and systems.

5.4.6 Effective system access control: Access granted to E-Voting application and assets is the minimum necessary for the identified user to obtain services required.

5.4.7 Information integrity: Ensuring that the voter’s vote is received and counted as intended.

5.4.8 Service availability: Ensuring access to the E-Voting service as and when required.

5.4.9 Information availability: Ensuring continued access to E-Voting data assets as and when required.

5.4.10 Service protection: Ensuring protection of E-Voting service implementation and associated assets from external interference and penetration.

5.4.11 Operator integrity: The employees who are administrating the E-Voting service should be of an unquestionable record of behavior.

5.4.12 Open auditing and accounting: The E-Voting service must keep a proper record of significant transactions and the integrity of audit information must be assured.

5.4.13 Third party system authentication: Third party systems, used by any E-Voting service, must demonstrate to the voter that they are authorized E-Voting agents.

5.4.14 Public verifiability: The E-Voting service must be publicly verifiable.

5.5 Assumptions Requirements of the Proposed Framework

The proposed framework is based on the assumptions that:

5.5.1 There is a consultant from TCG for managing and supporting the security of the election processes, which includes hardware, software and communication.

5.5.2 The devices which are used are secured with TPM.

5.5.3 The employees are well trained, and the administration is well educated.

5.5.4 There are helpdesk for any information inquiry or assistant.

5.5.5 The interfaces of the E-Voting system are highly accessible, user friendly and usable for different types of users from novice to experts, also for disabled people.

5.5.6 The E-Voting system supports many languages, and has speech audio facility.

5.5.7 There is a prototype dummy simulation of the E-Voting system outside the voting area, so voters can try before the actual casting of votes to gain their confidence and satisfaction that they are comfortable using the E-Voting system.

5.5.8 The system should be able to identify the casted votes online, and permit it from happing again in the polling places for the same person to avoid over voting.

5.5.9 The E-Voting system should be able achieve all the standards such as; election and Ballot integrity, ballot secrecy, voter anonymity and authentication, receipts and coercion resistance, anonymous channels, Privacy, Verifiability and Transparency.

5.5.10 The system should be able to achieve the requirements that were discussed in the previous section such as; Effective voter registration, authenticity, anonymity, and Effective vote confidentiality…etc.

5.6Toward Trustable E-Voting Management System Framework

The main propose of developing the research proposed framework is to manage a secure trustworthy E-Voting system, by securing each and every perspective of the system from its initial stage till the documentation and feedback for the next election preparation and improvement. This will include securing; data, network, servers, communication channels, storage devices and user devices. All of this securing will be achieved; by implementing TPM as chain of trust that combines hardware and software security to provide trusted client device. This TPM chip provides Protected Capabilities, Integrity Measurement and Storage as Roots of Trust, Integrity Reporting and Attestation. *(TCG, 2009)*

The current technology methods of E-Voting systems is the usage of electrical or electro mechanical operations, such as Scanners, DREs and Ballot Marking Devices (Auto Mark). The security of those technologies will be considered in the proposed framework. E-Voting system consists of two types that have to be managed. As shown in the framework figure (5.1), there are many channels for voting including all the types that will be discussed as follows. One type is Distance voting which is done through the internet. The other one is presence voting which is done at a polling station under the supervision of the election's administration.

The main tasks in the proposed framework are as follows; In preparation for the voting process (Pre-voting) registration of the voters in a list or registry; then identification, authentication, and authorization of users; when casting vote process the electronic ballot is displayed and may be cast anonymously by a citizen; Post-voting collecting of votes by an urn server; finally votes are processed and an election result is calculated and presented. These stages of E-Voting processes will be described thoroughly in the next section.

The proposed solution that have been implemented in the framework; has many benefits that provides chain of trust from every perspective such as, TPM trusted set (TS) delivers Root of Trust for Measurement (RTM): The measurement capabilities. Root of Trust for Reporting (RTR): The reporting capabilities. And Root of Trust for Storage (RTS): The storage capabilities

(Ericson, P., 2004). The proposed framework was developed after identifying the problems and issues in the current E-voting system, based on the literature review and questionnaire as shown in Figure (5.1) below:

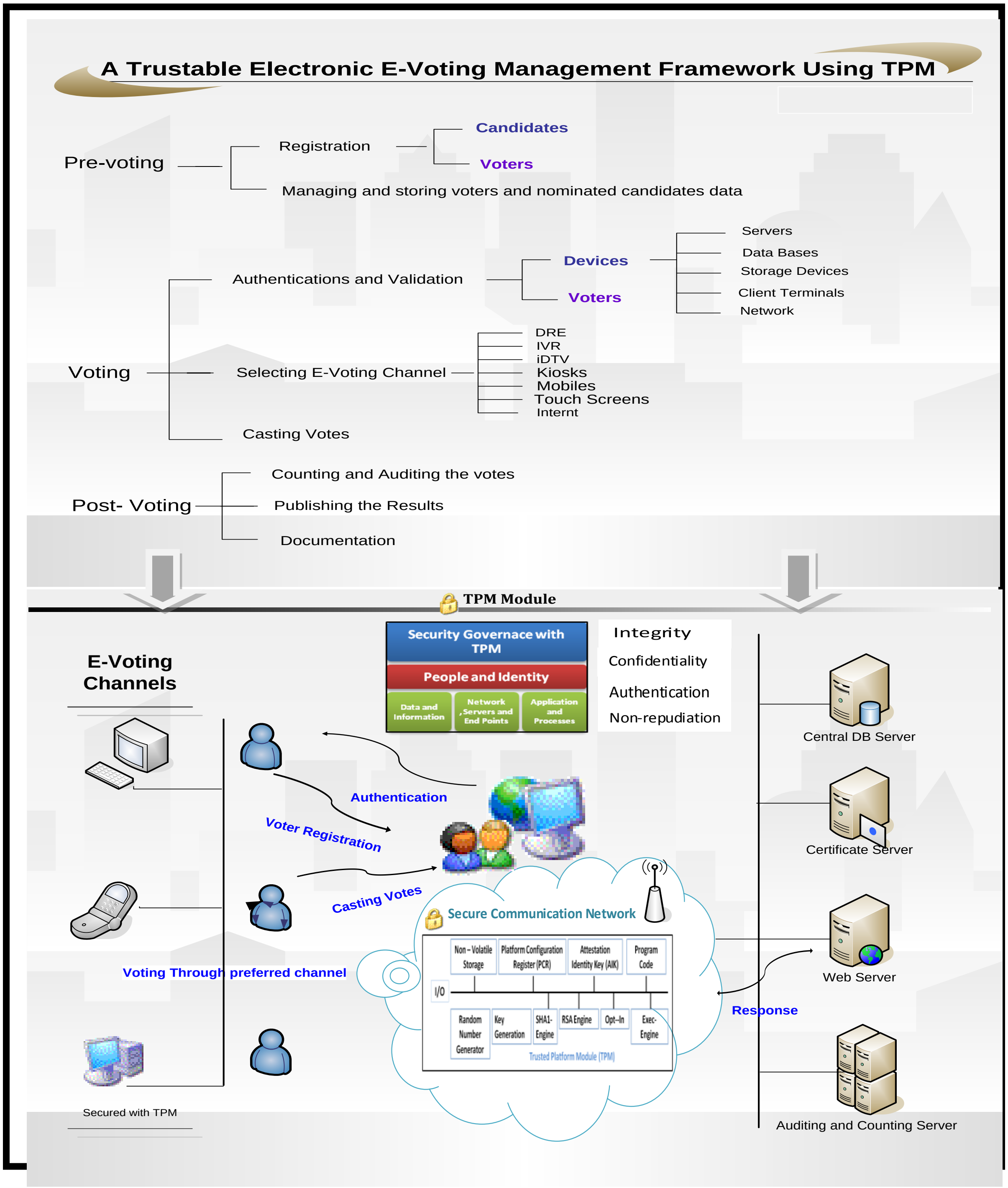
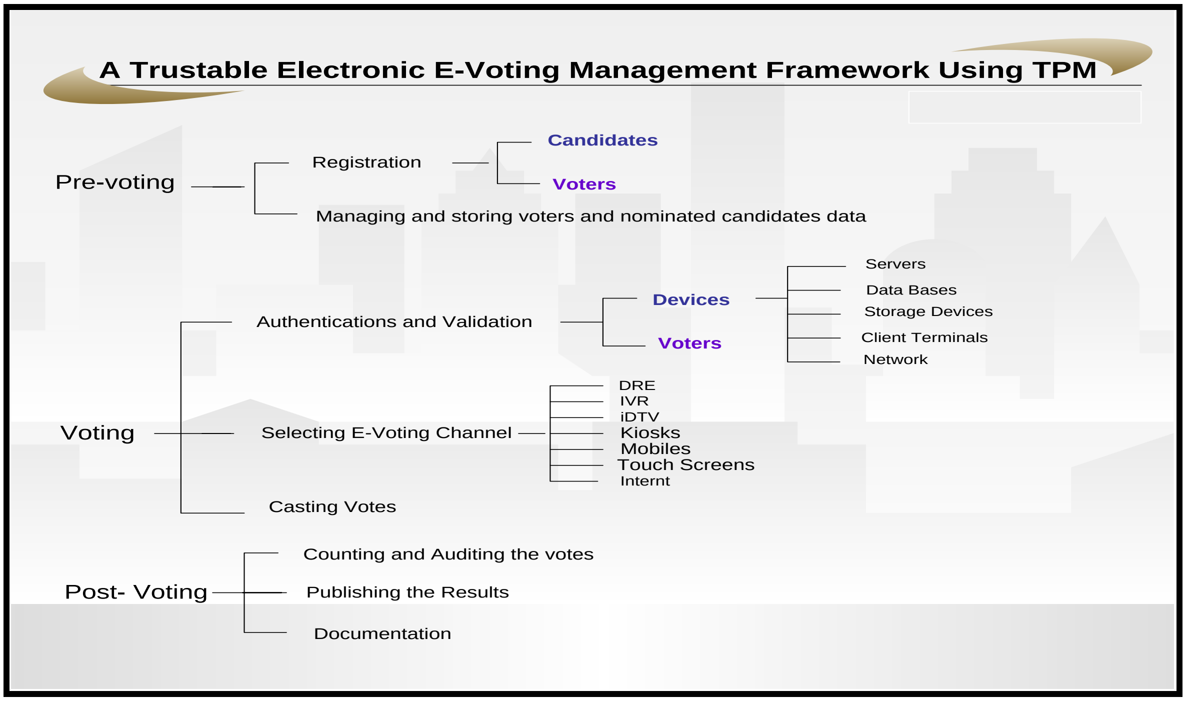


Figure (5.1) Proposed Framework

The proposed framework consist of two parts, the first part concerns the E-Voting processes. The second part consists of TPM implementation in the whole operation of E-Voting processes. These two parts will be explained as follows:

Part One - E-Voting Management Process

Preparation for the election considers: Human factors such as voters, candidates, employees, Technology Factors such as the devices, operating systems, application and networks. The figure below show the first part of the framework proposed.



A Trustable Electronic E-Voting Management Framework Using TPM

Pre-voting
Registration
Candidates
Voters
Managing and storing voters and nominated candidates data

Voting
Authentications and Validation
Devices
Servers
Data Bases
Storage Devices
Client Terminals
Network
Voters
Selecting E-Voting Channel
DRE
IVR
iDTV
Kiosks
Mobiles
Touch Screens
Internt
Casting Votes

Post- Voting
Counting and Auditing the votes
Publishing the Results
Documentation

Figure (5.2) Proposed Framework Part one

The main tasks of e-voting systems as shown in the proposed framework are as follows; registration of the voters and candidates in a list or registry; identification, authentication, and authorization of users, candidates and voters; managing all their data, then casting of votes: the electronic ballot is displayed and may be cast anonymously by a citizen after choosing the channel of E-voting system; then collecting of votes by an urn server; auditing and processing of votes, finally election result is calculated and presented. Each of these processes will be described in the next section.

Pre – voting

At the beginning of the election the organizers of the election campaign; will announce the information and the duration time of the E-Government Voting process, then they determine who is eligible to vote at the permitted time, after that ballot preparation and distribution this phase includes election information , candidates and the voters identification. Managing the election campaign through the method and media available for conducting the E-Voting campaign such as, local newspapers, radio stations, TV, Text message (SMS) through mobile phones, the official website can have the details and photos of all the candidates, and the information on the voting process.

In addition to the **awareness campaign**, there should be **training** for the employees on the election process including the use of the E-Voting system. The training can be done through full simulations of the E-Voting process before the actual election date. It is costly and time consuming, but the benefits are huge as it will reduce the errors of misusing the system, and it will reduce time of gaining knowledge of the technology and much more so training is preferred as it serves as an audit of the E-Voting system. The administrative and technical personnel should be trained on the ethical, business and technical issues before the elections.

As for managing the election process there should be three teams that are supervised by technical team as follows: *First*; the **Electorate Registration** System: for building the official database of voters. *Second*; The **Candidates Registration** System: for managing and updating Candidate‘s information and verifying their eligibility to run in the election. *Third;* the **Voter's Identity Verification** System: for ensuring the authentication of voters' identities using an ID card or a passport. The Voter identification and registration is used to identify the person either male or female, for the purpose of registering has a right to vote, thus identifying legitimate voters.

This will be done through authenticating the identity of the legal person allowed to vote in a contest, and to authenticate each person's voting rights. Voter identification and registration ensures that only legitimate voters are allowed to register for voting. Successful voter registration will ensure the authenticity and anonymity of the voter, and will result in legitimate voters being given a means of proving their right to vote to the voting system in a contest. Depending on national requirements or specific voting

Validation of E-Voting channels, as for the internet voting method validation**.** There must be some consideration taken when voting by internet, that voters are voting on different operating systems, and on different devices which provide the necessity for the websites to be usable, user friendly and secured. E-Voting system must be adapted to the different systems used by users, such as, for example, internet navigators. The other thing E-Voting system must check upon the voters if they voted online they will not vote again physically at the polling place, to avoid over voting not to mention checking the identity of the voter who is voting online to avoid dead people vote or redundancy of voting. Other channels such as mobiles, DRE's …etc also must be validated for the accuracy of votes results. After validating the channels also maintenance and validation of the system devices as they should be ready for the voting operation next step.

Voting

The **Vote Casting System**: This system includes the e-voting channels and devices, such as touch screens, kiosks, voting websites, the voting database, the encryption system, the vote counting system and results presentation system. The primary function of E-Voting system is to capture voter preferences reliably, and report them accurately. The critical process is between capturing the voter vote and voting on an e-voting system (machine), as the system should be able to prove that a voter's choice is captured correctly and anonymously from his/her selected voting method, and that the vote is not subject to tampering. Voters can choose between casting their votes physically at the election place (poll site), remotely by internet voting (online / email) or by Mobile SMS according to the different channel voters preference, after authenticating and authorizing themselves by providing identification to a trusted official workers, for preventing over or under votes administrators validates the credentials of those attempting to vote when the election process begins.

Post – voting

After voters have casted their votes, the administrators collect the votes, then votes are processed and an election result is audited calculated and presented. Audit is the process by which the election authority representatives can examine the process used by which the vote is collected and counted to prove the authenticity of the result. Their tasks are to count all the ballots, as for the ballots issues, they should match the total of ballots cast, spoiled and unused. Prove that voted ballots received are secure from any alteration, they should allow a recount when result is contest, and allow for multiple observers to witness all the process. Then publishing the final results and documenting all the E-Voting process, machines and employee's performance, everything has to be documented for improving the system in the next election. The system provides a facility to perform recount if there is any complaint about the results.

Part Two - Implementing TPM on E-Voting System

This technical part should be done according to the security requirements mentioned earlier in (5.4). TPM functions create a chain of trust that is most needed for enhancing the security of E-Voting system; the research aim is to deliver a Trustable Electronic Government Voting Management Framework using TPM, which is what the project artifact is based on. The following section will illustrate the second part of the framework after implementing TPM.

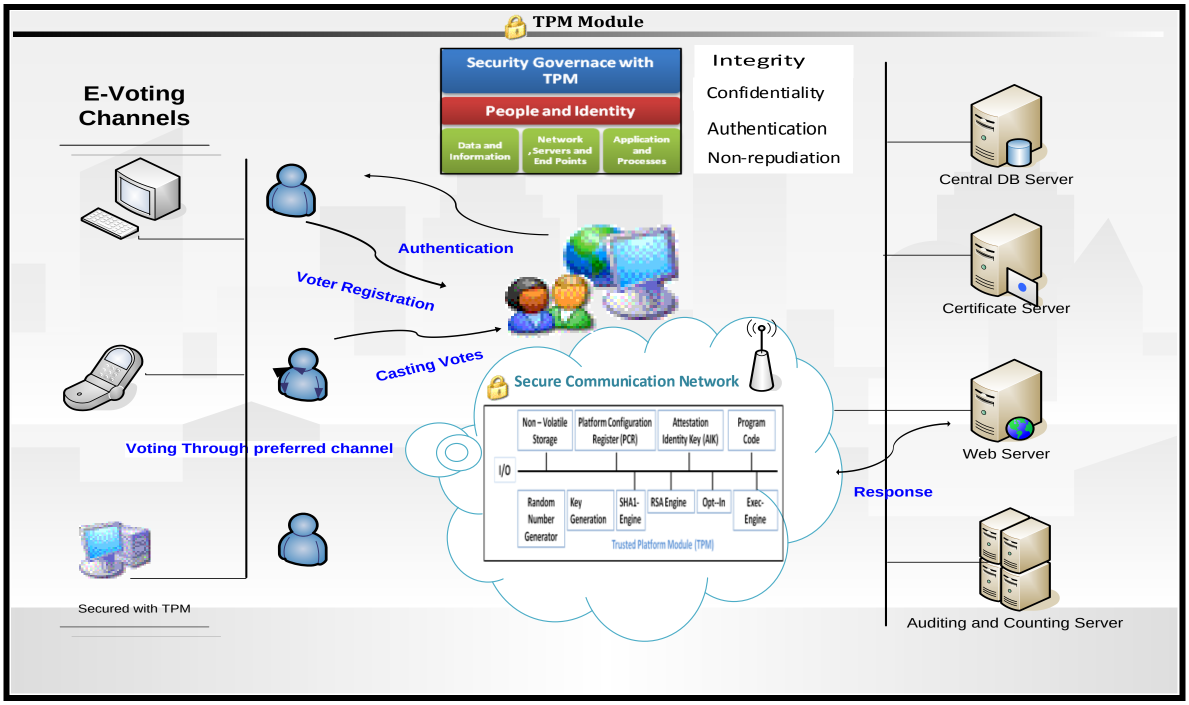


Figure (5.3) Proposed Framework Part Two

The Architecture of the E-Voting proposed framework part 2 is as follows;

The entities are Voters: Anyone who has once registered can vote over the voting channels within reasonable time (according to election duration), Candidates, Authorities, Servers: Admin, Web, CA, DB, and Counter. E-Voting channels: IVR, Mobile, Internet, kiosks, Touch screens, DRE…etc, Network, TPM.

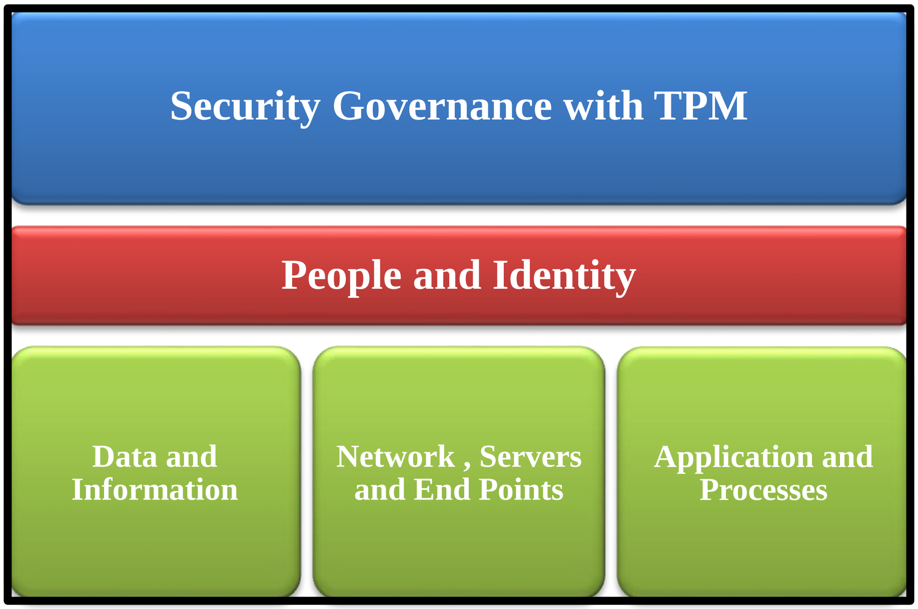

Security Governance with TPM
People and Identity
Data and Information
Network , Servers and End Points
Application and Processes

Figure (5.3.1) Proposed Framework Part Two TPM

In this TPM framework Rather than implementing security on top of system elements, the security is built in so the system infrastructure will be fundamentally secure. By implementing TPM secure cryptographic chip in E-Voting System, it provides a hardware-based approach to managing voter's authentication, network access, and data protection, including everything from multi-factor authentication and machine binding for removable media, to irrevocable digital signatures and full-disk encryption. TPM has many features such as the chip includes the RTR (root of trust reporting) and RTS (root of trust storage) functions, The TPM also supports other functions such as cryptographic key generation, and data sealing and binding *(Fang, W., et al, 2009)*. TPM can benefit enhancing the security of the **E-Voting system** as follows:

Multi-factor authentication: TPM provides one factor in a multi-factor authentication model. For example, adding digital certificates (PKI) tied to a TPM to biometrics, eliminate passwords and create stronger authentication models for wired, wireless, and VPN access. **Strong login authentication:** TPM ensures that only authenticated users access the network **Machine binding:** TPM Encrypts all data stored on removable media and limit access based on identity. **Digital signatures:** A TPM enables tamper-resistant digital document signing, to reduce fraud. **Trusted audit trail:** TPM helps to create the required irrevocable audit trail. **Password vaults:** Even if the PC is lost or stolen, passwords are protected by the TPM. **File and folder encryption:** TPM will encrypt files and folders, and controls access to those files and verifies their integrity. **Strong client/server authentication:** TPM provides key management tools including key escrow, backup, and recovery capabilities.

Network access control: In the Trusted Network Connect (TNC) framework. TPM attests to the identity and even health of a PC state before it is granted network access, or shunted into network quarantine. **Endpoint integrity:** The TPM can hash state information prior to a hard drive shutdown, to report to a host that the machine and its software have not been tampered with when it boots. Also it can monitor all applications in the trusted application stack to report they are not tampered with while running. Finally **Trusted client/server security**: as an example IBM, among others, has begun shipping trusted servers with a built-in TPM to create even more secure client/server relationships and computing environments. *(Berger, B., 2008)*

As indicated above all these TPM features can benefit the E-Voting system: first securing the database storage then the voters and candidates information are secured and cannot be altered, which means the first step of registration is done successfully. Second the authentication of the devices and voters, which mitigate the privacy issue and prevent the man-in-the-middle attacks. Also it provides integrity, confidentiality and non repudiation which are the main elements of successful secure trustable E-Voting system. As for the network communication input and output as indicated before that TPM Software Stack enables trust in network endpoints and secure network activities. TNC provides Platform-Authentication, Authorization, Access Policy, Assessment, Isolation, and Remediation which will enhance the E-Voting system network security *(IT Security Journal, 2008).*

By running on a TPM, each device in an E-Voting system operates in a verified environment, every device can attest to its state as for communicating devices can perform mutual attestation, to verify to each other that both devices are in a valid state before communicating. Using TPM approach, a trusted E-Voting system can accurately capture, count, and report the votes.

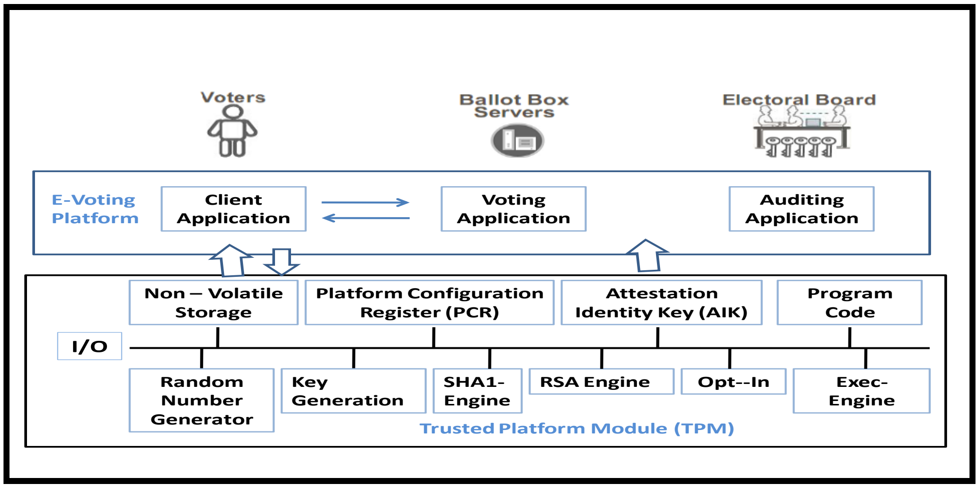


Figure (5.3.2) Proposed Framework Part Two TPM

Phase 1: System initialization to check the integrity of the electoral roll before the poll opens, and to make sure that the virtual urn is empty and that the vote counters are set to zero, also securing the devices with TPM by sealing the storage, and the electronic devices.

Phase 2: Registering all the legible voters and storing their information in a secured database (secured by TPM), Verifying and authenticating the voters and the candidates. The voter must prove his/her identity to the manager of the electoral roll. The procedure used may range from the use of an identifier combined with a PIN code to use of a smartcard, in this proposed framework usage of TPM key generation for better security.

Phase 3: Securing E-Voting channels and devices by TPM, for an example as voting by the internet (I-Voting) protecting the voters passwords with a TPM, so that the servers on the other end can be assured who the user really is as the password is backed with the guaranteed identity from the TPM, and the user can be assured that access to the services can only be made from the computer with the TPM installed.

Phase 4: If the voter is authenticated, he/she is credited with a random number, giving him/her the right to vote. The voter then makes, from his/her virtual polling station, the selection, or selections, appertaining to the poll. Next is validation of the vote (check to ensure the voter has not already voted).

Phase 5: After casting the votes, and when the poll closes, the managers analyze the vote's then audit and count them, finally publishing the results and the documentation, if needed recount.

Chapter-Six

Framework Evaluation

6.1 Introduction

Testing and evaluating the artifact is very important for the development process of the targeted project deliverable, as to improve it for final documentation. The evaluation was done through second questionnaire to the research sample selected “security experts” that was questioned before. Through the next section there will be data analysis and interpretation for the evaluation results. Testing and evaluation is complex and time consuming task, but it is necessary because of many reasons such as; the security testing of E-Voting systems must be well documented to create a realistic E-Voting systems, secondly The proposed framework must be evaluated and refined to be well developed , finally utilizing reverse engineering experience to expose vulnerabilities in the proposed framework of E-Voting system components that have been analysed, and gain a deeper understanding than would be possible otherwise. The evaluation methods conducted in this research have been done through primary through questionnaire, and secondary based on the literature review evaluation methods.

A brief introduction to the TPM module was given in the evaluation questionnaire (2) to give an idea on the proposed solution as follows” Trusted Computing Group is not-for-profit organization that consists of about 140 member companies their focus was on developing, defining, and promoting open standards for trusted computing which will benefit users. They introduced a hardware chip called trusted platform module (TPM), that provides chain of trust for information and communication security.

The framework proposed aims to manage the E-Voting process from the initial pre-voting stage through voting until the post- voting, and to enhance the security to gain voters and users trust in E-Voting systems. It is about implementing TPM in all the process from authentication of the voter, securing voting channels (internet, kiosks, Mobiles…etc) to the network and storage devices in order to gain chain of trust of the E-Voting system. TPM addresses the inability of a PC to securely store passwords to prevent hacker’s invasion. It provides Authentication, Authorization, Access Policy, Assessment, Isolation, and Remediation which will enhance the E-Voting system network security”. Then the questions were introduced as will be discussed and analyzed next section through the primary evaluation.

6.2 Primary Evaluation Questionnaire Feedback

Evaluation and testing of the proposed framework will be done through analysing the experts feedback taken from the second questionnaire conducted as follows;

6.2.1 Question one (Education)

Question one (*Kindly specify your education?*) aims to know the level of education as the sample is based on experts opinion. The figure below shows the percentage of experts who responded to questionnaire is as follows:

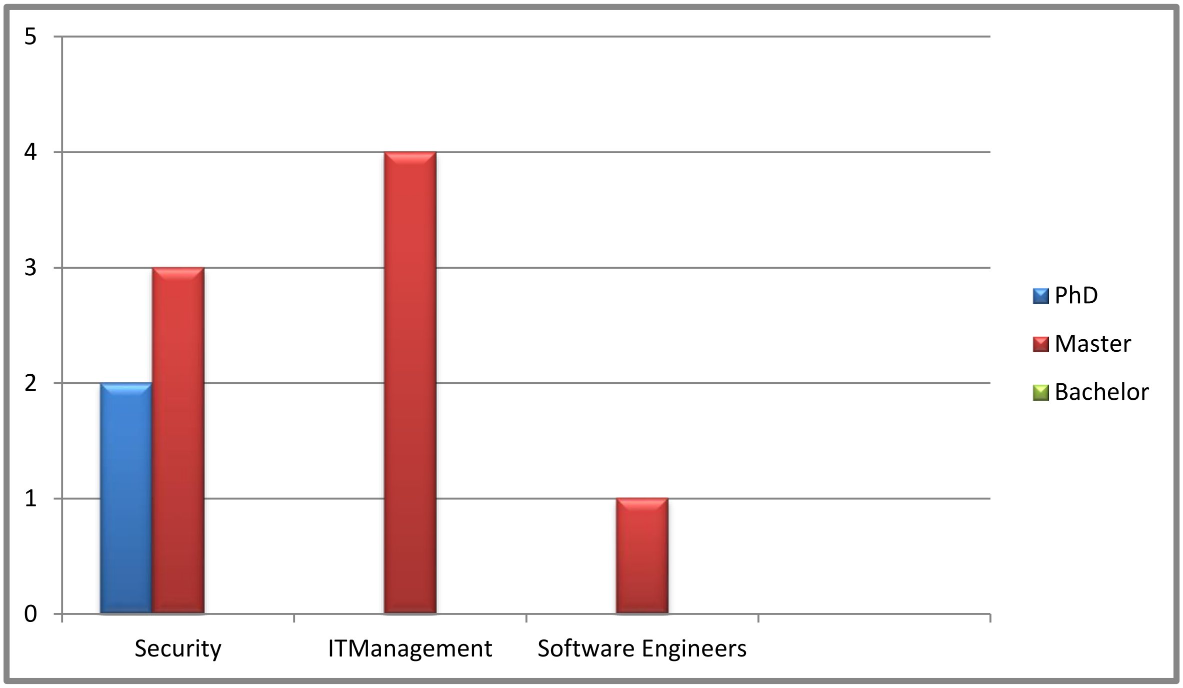


Figure (6.1) Education

Description

As indicated in the figure (6.1), the data analysis for (10) experts people education level was 20% PhD level and 30% Masters in Security field , 40% Masters in IT Management, and 10% in Software engineering to ensue the knowledge and depth of the research solution and testing the deliverable.

6.2.2 Question Two (Nationality)

Question two (*kindly specify your nationality?*) aims to know the nationality of the experts as it is important that they have knowledge about E-Voting Systems to be sure of the accuracy of their feedback.

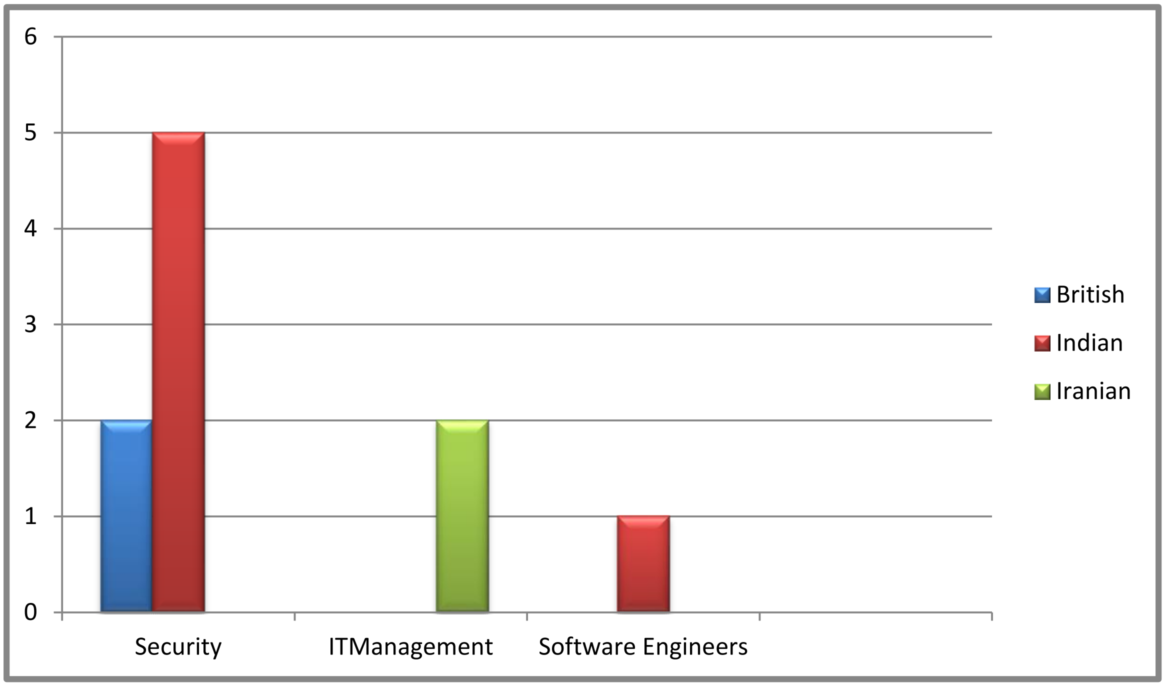


Figure (6.2) Nationality

Description

Different Nationality responded to the survey questionnaire which have experienced election in their countries, 20% from United Kingdom in the security field and PhD degree holders as indicated in the previous figure (6.2) , 60% were Indians and Master Degree Holders both fields (50% Masters in ITM and 10% Masters in Software Engineering) finally 20% are Iranian that have major issues in their election process so their feedback will be powerful for identifying the problems in E-voting System they were from the field of IT Management.

6.2.3 Question Three (E-Voting Framework with TPM)

Question three *(Do you consider the security of E-Voting system is enhanced in this proposed framework by using TPM)* aims to Evaluate the E-Voting system proposed framework to refine it and documented.

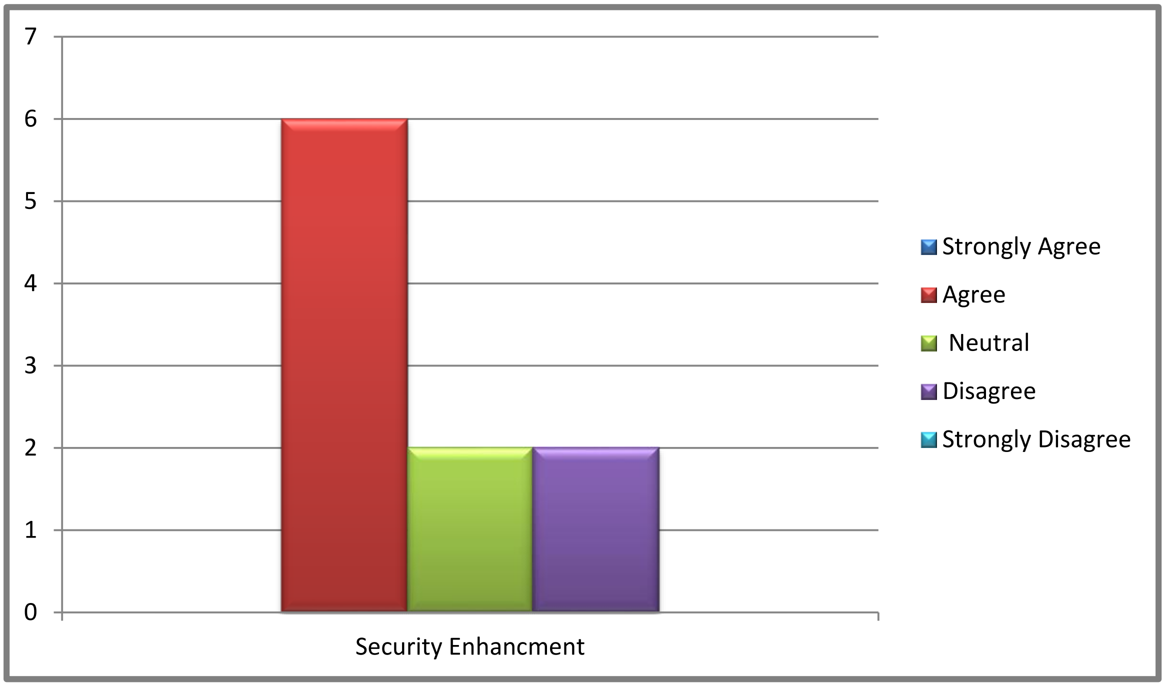


Figure (6.3) Framework Security Enhancement

Description

Different opinion was given, 60% experts agreed on the TPM usage can enhance the security of E-Voting system, and 20% disagreed, while 20% remained neutral.

6.2.4 Question Four (E-Voting channels with TPM)

Question three *(Do you consider the security of E-Voting system channels are enhanced in this proposed framework by using TPM)* aims to Evaluate the TPM usage for securing E-Voting channels.

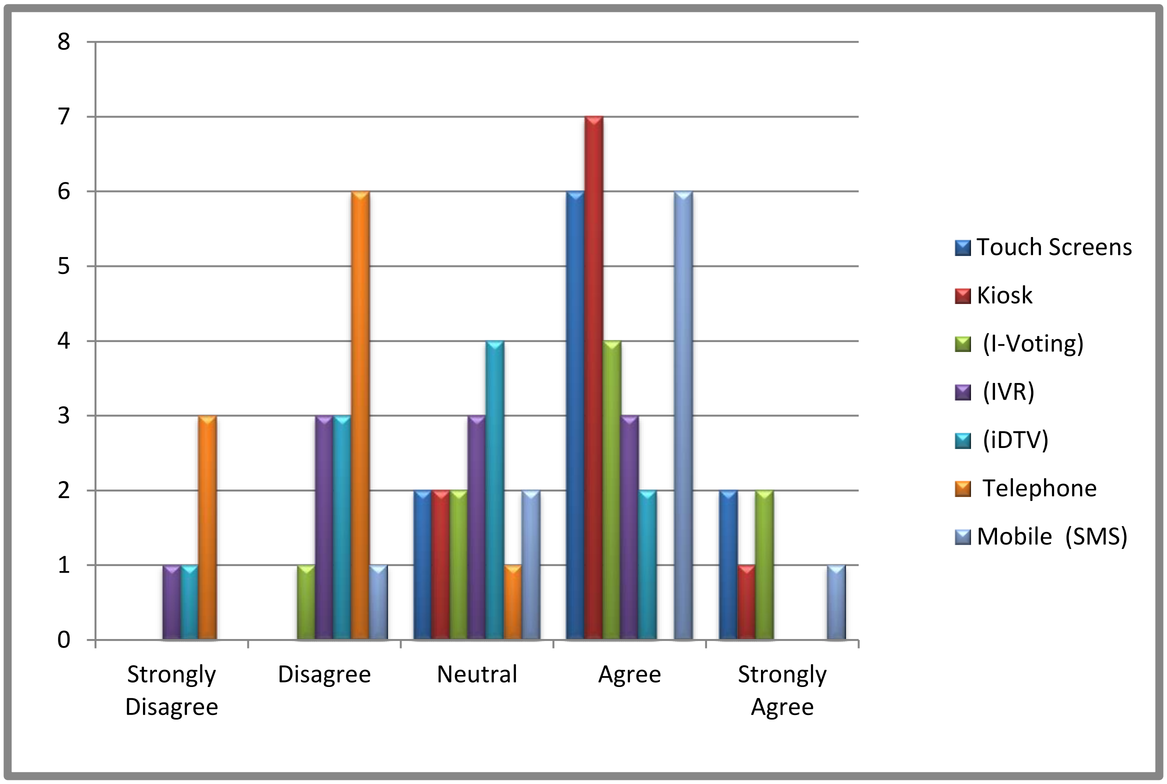


Figure (6.4) E-Voting Channels with TPM

Description

As for experts consideration of TPM ability to enhance the security of E-Voting system channels, the figure shows that mostly agreed on Kiosks 70%, and touch screens 60%. They disagreed on landline telephone 60%, interactive digital TV (iDTV) 30%, and other channels that will be described individually below. The following section will describe the expert level of acceptance that TPM enhances security of E-voting channels, in a pie figure for each channel from the figure in (6.4) to be analyzed.

Touch Screens

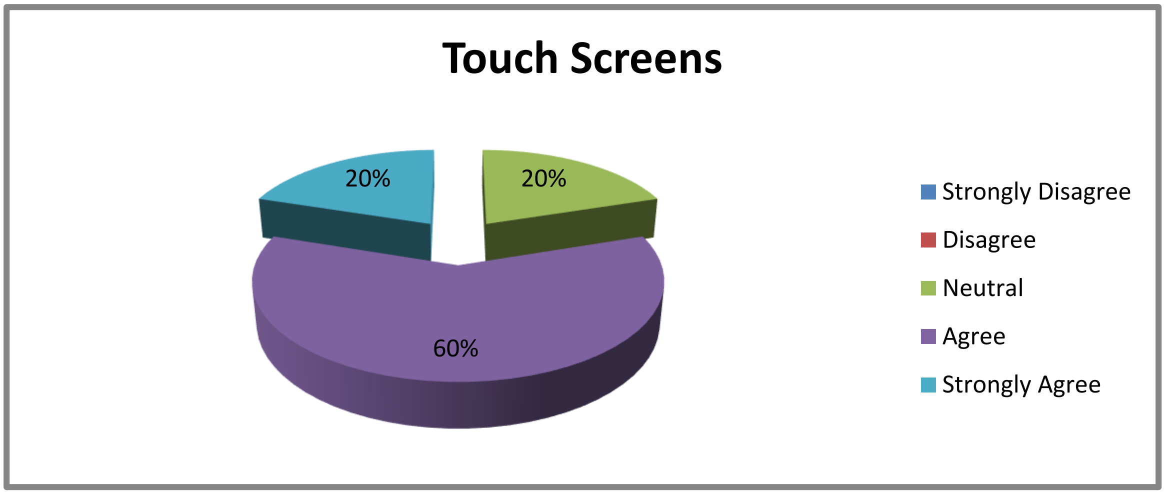


Figure (6.4.1) Touch Screens

Description

Most of the experts agreed 60% and 20% strongly agreed on TPM enhancing security of touch screens, while 20 % were neutral.

Kiosk

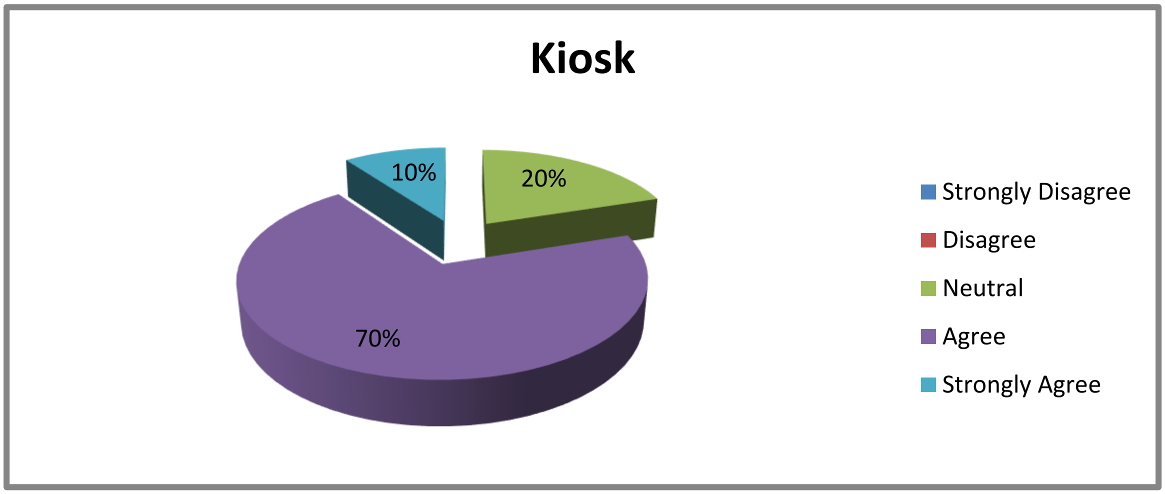


Figure (6.4.2) Kiosk

Description

Most of the experts agreed 70% and 10% strongly agreed, which indicate that they prefer kiosk for casting votes, while 20% were neutral about TPM enhancing security of kiosks.

Internet Voting (I-Voting)

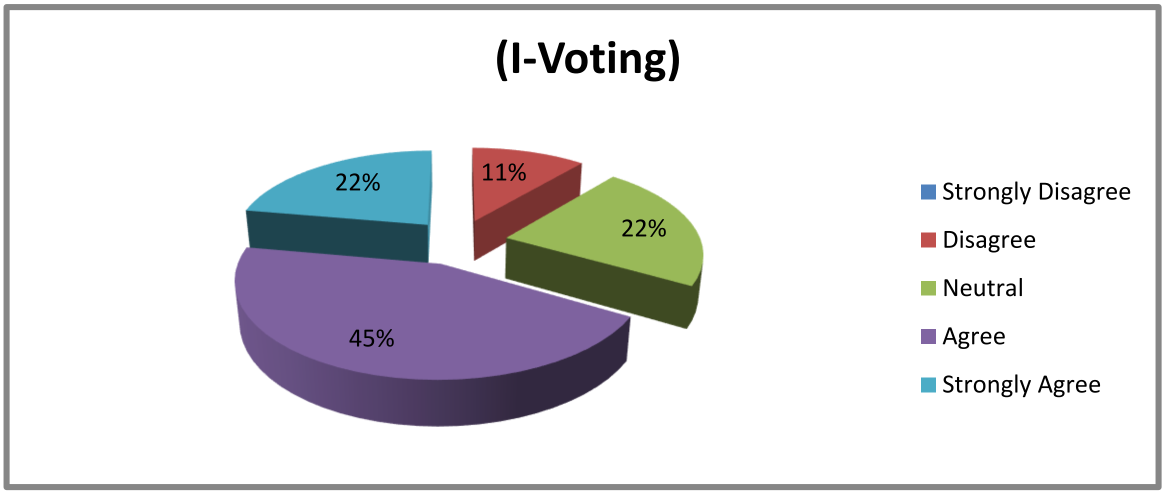


Figure (6.4.3) I-Voting

Description

45% of experts agreed and 22% strongly agreed, while 11% disagreed, however 22% remain neutral on TPM enhancing security of I-Voting.

Interactive Response (IVR)

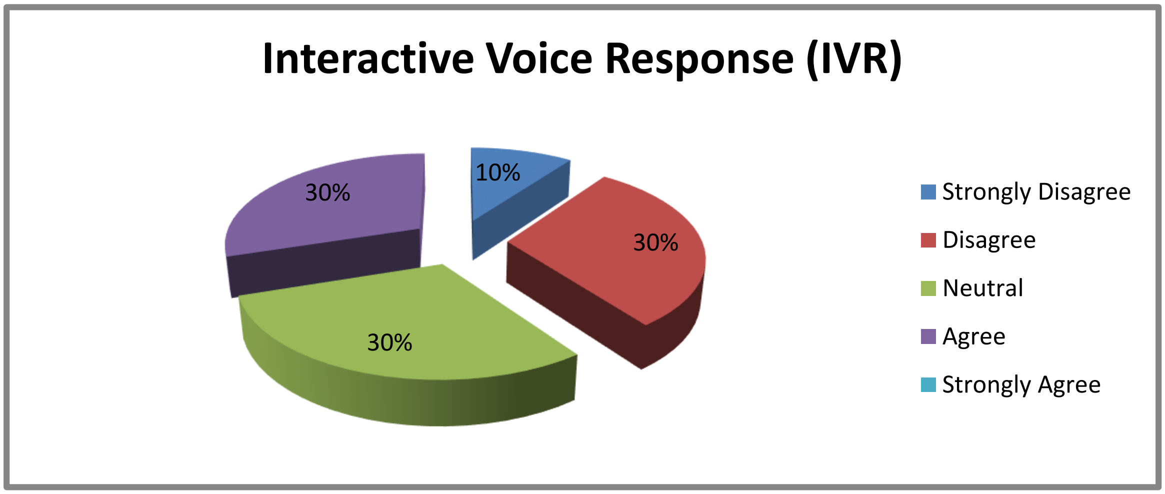


Figure (6.4.4) IVR

Description

10% strongly agreed and 30% agreed, while 30% disagreed, 30% remain neutral on TPM enhancing security of Interactive Response (IVR) voting.

Interactive Digital TV (iDTV)

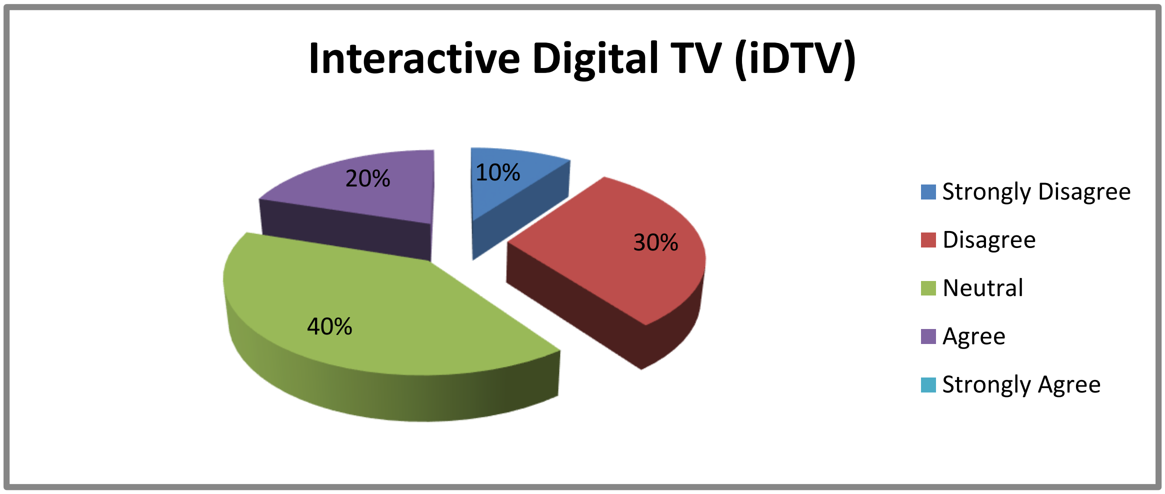


Figure (6.4.5) (iDTV)

Description

Interactive digital TV (iDTV) has 20% agreed, while 10% strongly disagreed, and 30% disagreed, still 40% remain neutral on TPM enhancing security of (iDTV) Voting.

Landline Telephone Voting

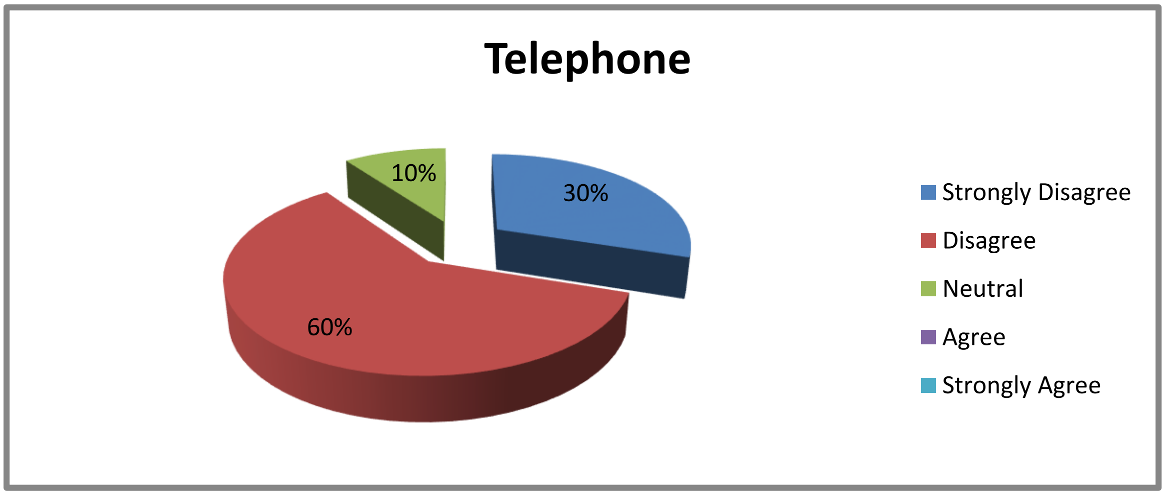


Figure (6.4.6) Telephone

Description

Landline Telephone voting has 30% strongly disagreed and 60% disagreed, while 10% remain neutral on TPM enhancing security of Telephone Voting.

Mobile Voting (SMS)

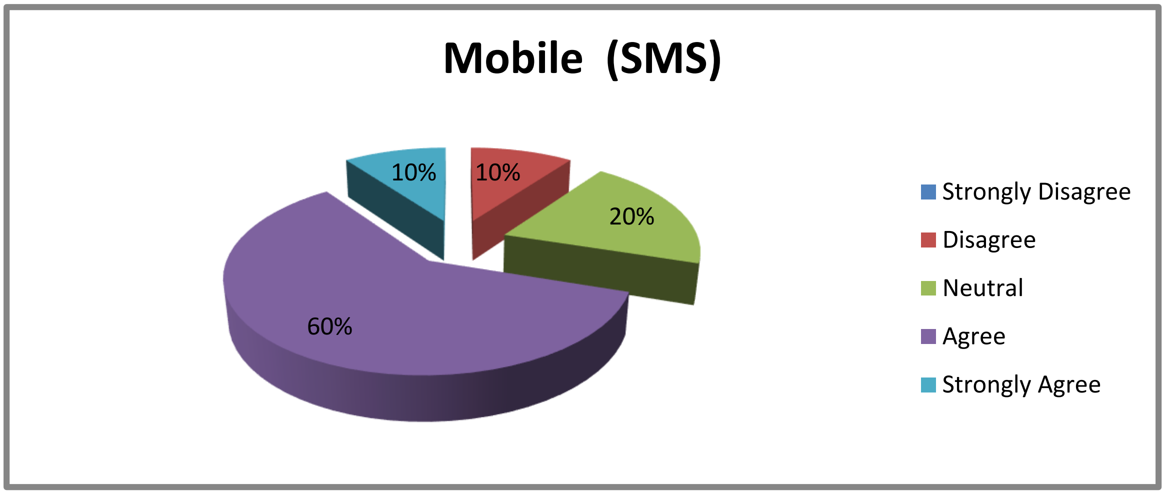


Figure (6.4.7) Mobile (SMS)

Description

Mobile Voting (SMS) has 10 % strongly agreed and 60% agreed, while 10% disagreed, and 20% remain neutral which shows that acceptance of TPM module can secure Mobile voting.

Summary of question (6.2.4)

Table (6.2.4) below indicates experts acceptance of TPM usage to enhance the security of E-Voting channels. The percentage is the total of strongly agree and agree.

E-Voting Channels		
Channel	**Percentage of preference**	**Conclusion**
Touch screen	80%	As shown that experts agreed on TPM can enhance the security of touch screens and kiosks with the percentage of 80%., and the security of internet 67% but for telephone they indicated zero, while mobile phone 70%, which gave it positive evaluation and TPM is good to be used.
Kiosk	80%	
Internet voting (I-Voting)	67%	
Interactive Voice Response	40%	
Interactive Digital TV	20%	
Telephone	0%	
Mobile (SMS)	70%	

6.2.5 Question Five (E-Voting attacks mitigated by TPM)

Question three *(Do you consider the security of E-Voting system are enhanced in this proposed framework by using TPM to mitigate the following E-Voting systems attacks and threats.)* aims to Evaluate the usage of TPM to mitigate the possible attacks on e-voting system.

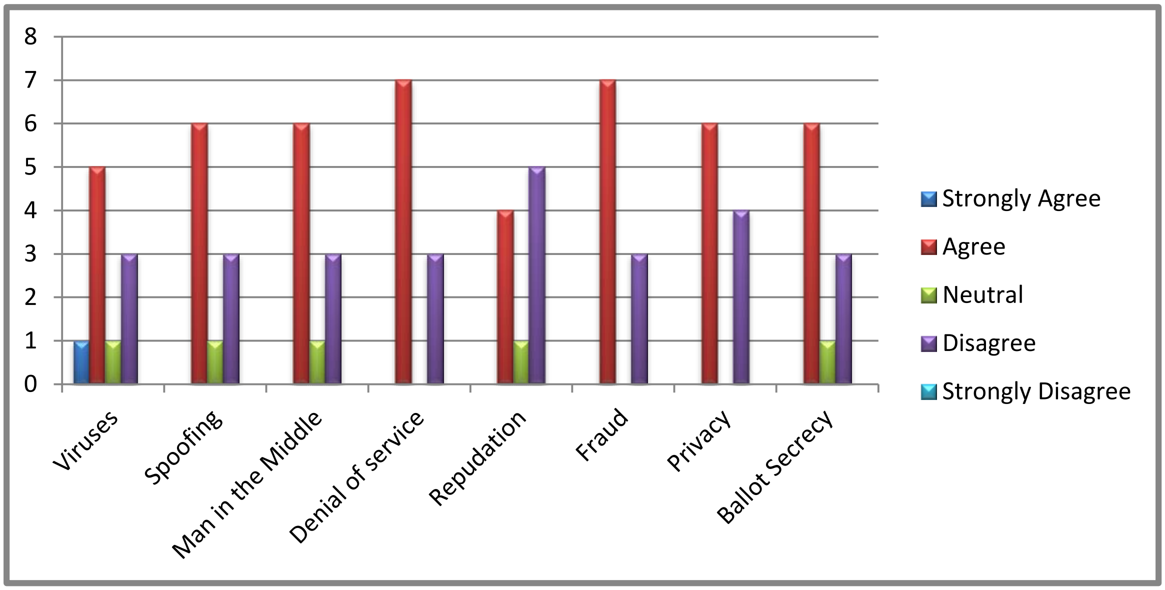


Figure (6.5) E-Voting Attacks

Description

In this chart figure experts agreed that TPM can mitigate fraud (70%) and denial of service (70%), then spoofing, man-in-the-middle, privacy, ballot secrecy, strongly agreed on viruses (10%), and disagreed on repudiation (50%) and all other threats with equal percentage (30%), While (10%) remained neutral on viruses, spoofing, man-in-the-middle, repudiation and ballot secrecy. The following section will describe expert’s consideration on TPM mitigating E-Voting system potential threats and attacks in a pie figure for each problem from the figure in (6.5) to be analyzed.

Viruses, Key Logger and Hacking

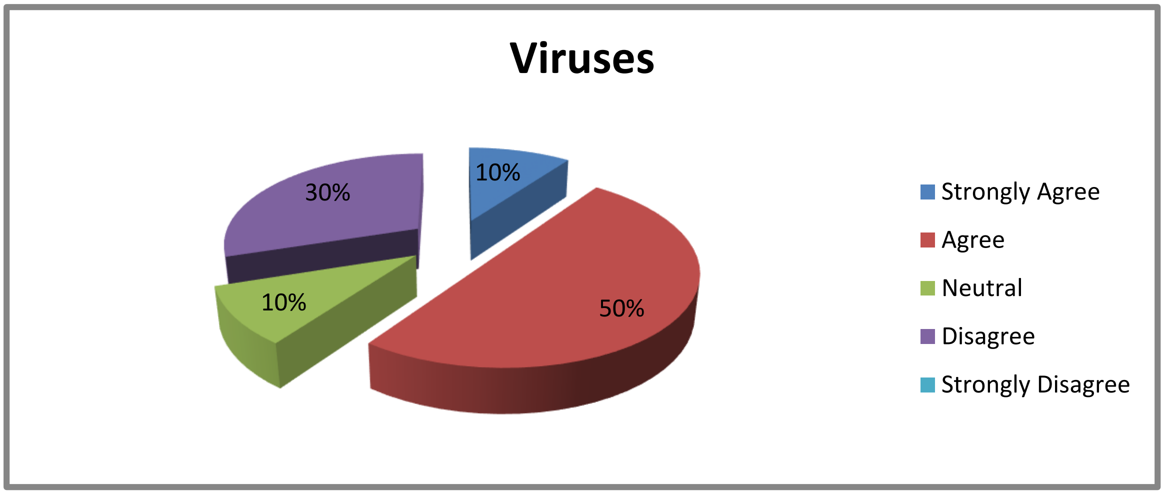


Figure (6.5.1) Viruses, Key Logger and Hacking

Description

50% expert agreed and 10% strongly agreed that TPM can mitigate these attacks, while 30% disagreed and 10% remained neutral.

User Spoofing

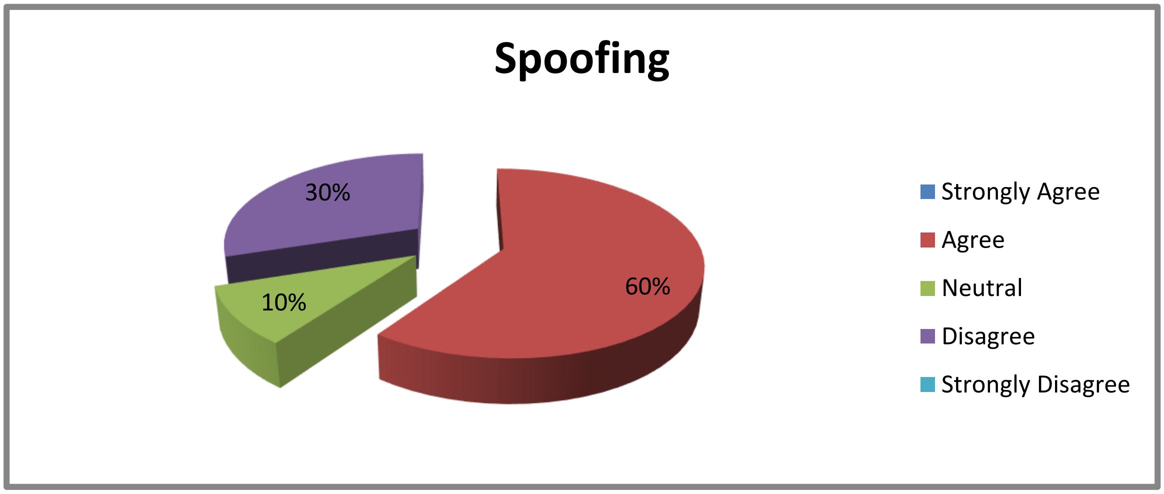


Figure (6.5.2) User Spoofing

Description

60% expert agreed that TPM can mitigate user spoofing attack, while 30% disagreed and 10% remained neutral.

Man- In –The- Middle

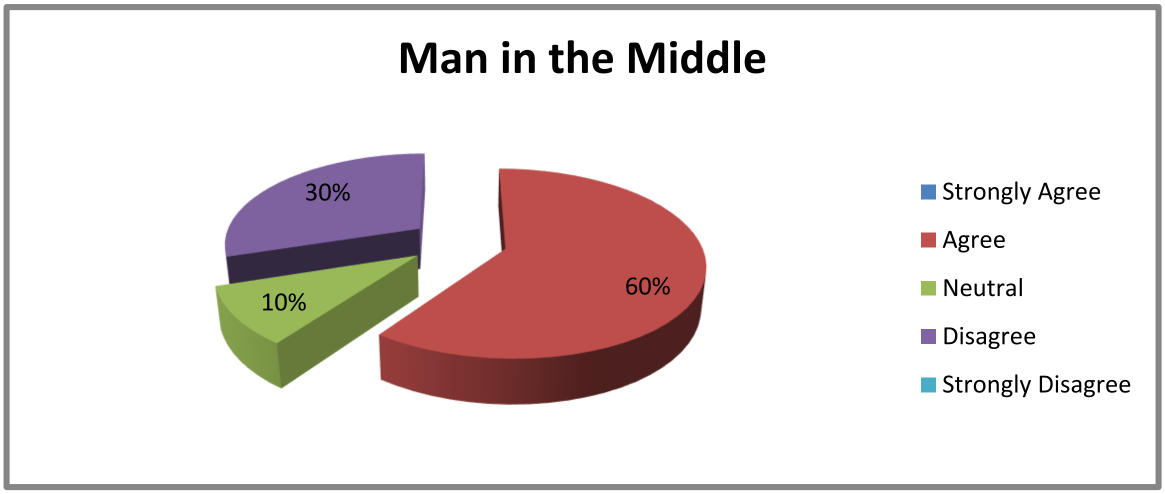


Figure (6.5.3) Man-in- the- Middle

Description

60% expert agreed that TPM can mitigate Man-in- the- Middle attack, while 30% disagreed and 10% remained neutral.

Denial of Service

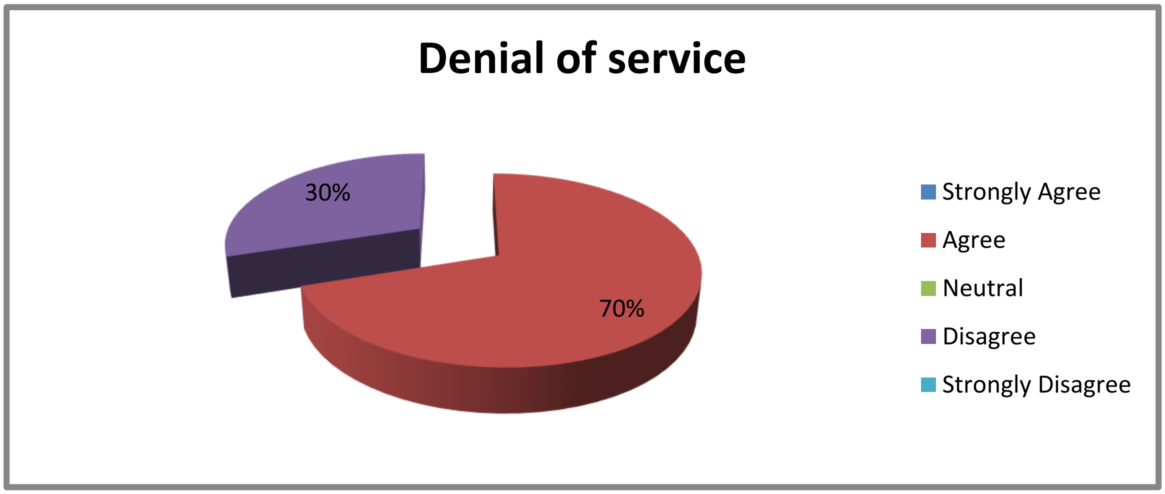


Figure (6.5.4) Denial of service

Description

70% expert agreed that TPM can mitigate Denial of service attack, while 30% disagreed.

Repudiation

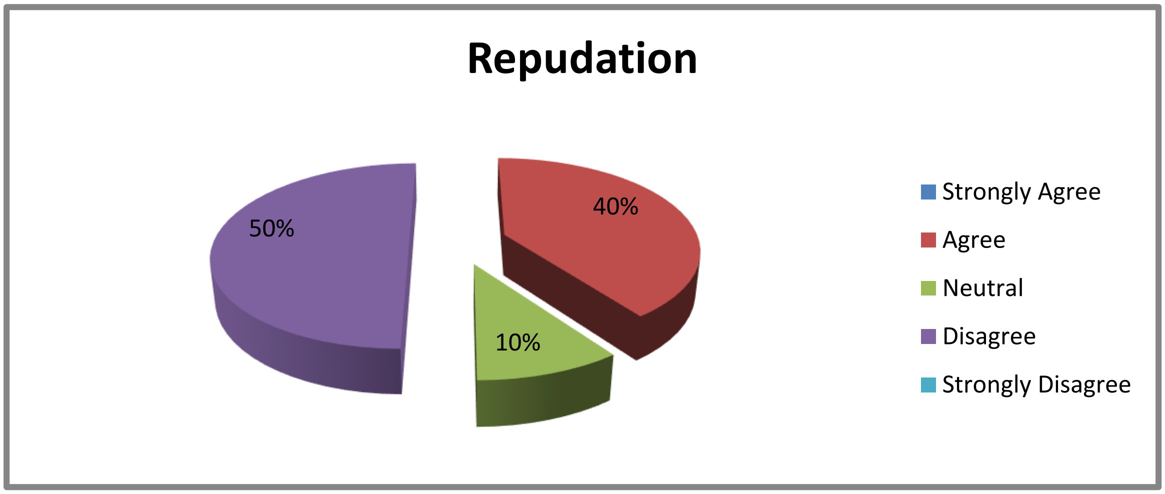


Figure (6.5.5) Repudiation

Description

40% expert agreed that TPM can mitigate Repudiation, while 50% disagreed and 10% remain neutral.

Fraud

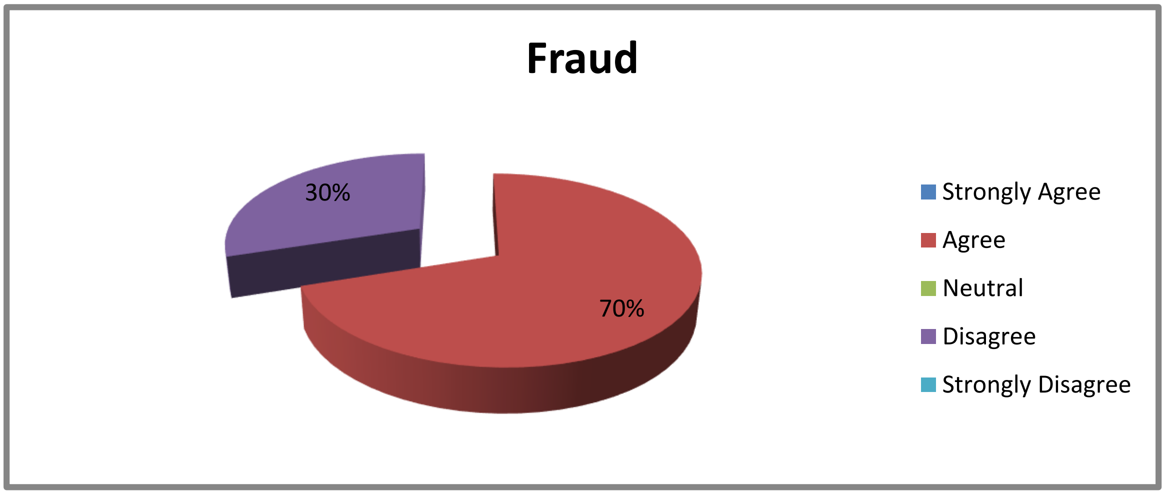


Figure (6.5.6) Fraud

Description

70% expert agreed that TPM can mitigate Fraud, while 30% disagreed.

Privacy

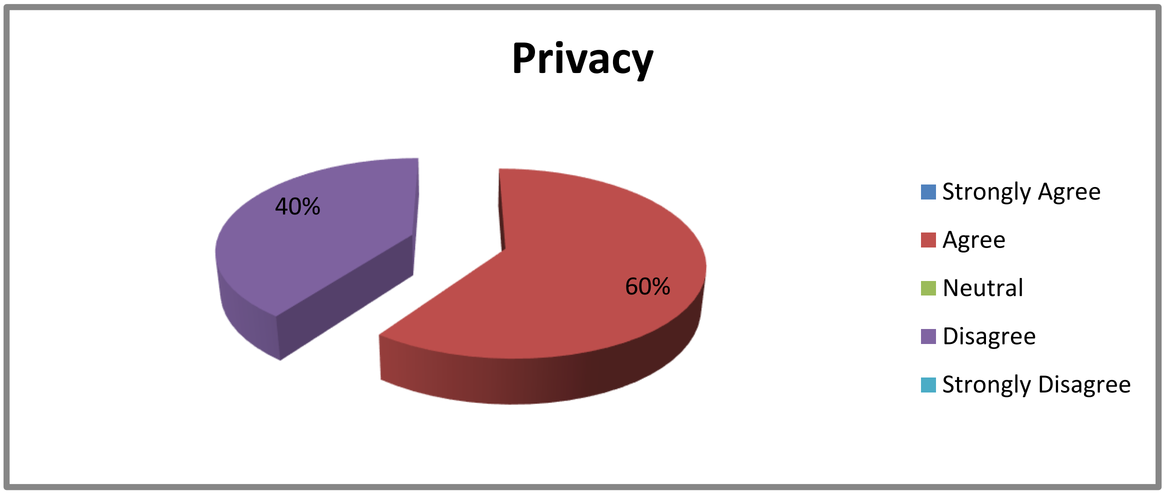


Figure (6.5.7) Privacy

Description

60% expert agreed that TPM can mitigate privacy attack, while 40% disagreed.

Ballot Secrecy

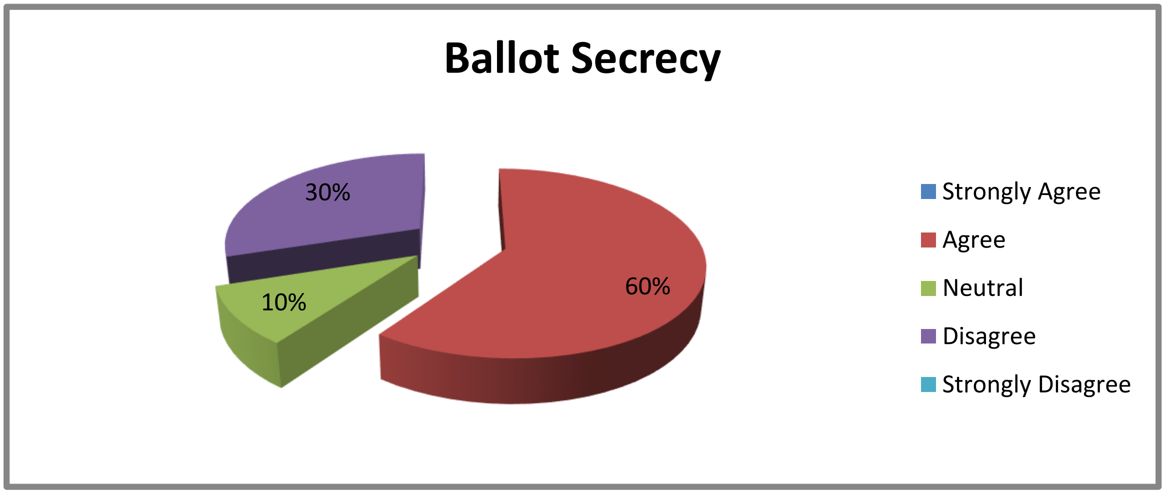


Figure (6.5.8) Ballot secrecy

Description

60% expert agreed that TPM can mitigate ballot secrecy attack, while 30% disagreed and 10% remain neutral.

Summary of question (6.2.5)

Table (6.2.5) below indicates experts acceptance of TPM ability to enhance the security of E-Voting to mitigate the attacks. The percentage is the total of strongly agree and agree.

E-Voting Problems		
Problem	**Percentage of preference**	**Conclusion**
Viruses, Key logger and Hacking	60%	As shown that experts agreed that TPM can enhance the security, and mitigate the E-Voting system attacks. Most of the opinions agreed on TPM ability to mitigate fraud and denial of service. The rest was the same percentage of 60% agreed on the ability of TPM to mitigate man-in-the-middle attack, viruses, key logger, hacking, and user spoofing.
User spoofing	60%	
Man in the Middle	60%	
Denial of service	70%	
Repudiation	40%	
Fraud	70%	
Privacy	60%	
Ballot secrecy	60%	

6.3 Findings of the Evaluation Analysis

The quantitative questionnaire (2) feedback analysis finding that the framework proposed is accepted with the percentage of 60%. And they agreed on the ability of TPM can enhance the security of E-Voting channels, such as touch screens and kiosks with the percentage of 80%., and the security of internet 67%, while mobile phone 70%, which gave it positive evaluation and TPM is good to be used. Also the experts agreed that TPM can enhance the security, and mitigate the E-Voting systems attacks. Most of the opinions agreed on TPM ability to mitigate the E-Voting system threats. Most of the opinions agreed on TPM ability to mitigate fraud (70%) and denial of service (70%). The rest was the same percentage of 60% agreed on the ability of TPM to mitigate man-in-the-middle attack, privacy, viruses, key logger, hacking, and user spoofing. The evaluation feedback was in the favor of the proposed framework next is the secondary evaluation.

6.4 Secondary Framework Evaluation

The secondary evaluation will be done based on the literature review. As far with discussion made in chapter (2) **E2E** E-Voting systems were good, but had some issues such as they cannot meet every voting system requirement without using software to achieve greater efficiency, this software can be untrustworthy, In addition poor usability and accessibility, also it leads to disclosure of voter privacy or integrity even in software independent verifiable systems. As in Scantegrity II *(Fink, R., Sherman, A., 2009)* malicious printer software could expose ballot codes and destroy voter's privacy. Malicious scanner software could identify voters with stray marks, enabling coercion. E2E voting systems are not immune to privacy attacks, and they are not quick at catching integrity problems. While in the proposed framework of trustable E-Voting management system using TPM ensures the correct software is running, manages the cryptographic keys securely, enhance privacy, and detects problems at the early stages, high assurance of electronic accessibility interfaces. TPM assures the election authority of the integrity of the software and ballot data during voting, and the integrity of the vote data during storage and transmittal, increasing the security of the election. TPM also allows vote collection only during the election duration time. This led to the conclusion of TPM can enhance the security of E2E systems, and the proposed framework is able to overcome E2E issues.

DRE E-Voting systems has many benefits, such as good usability and accessibility, support of multiple ballots and languages, and elimination of over votes and under votes, but they have bad security engineering, TPM critical cryptographic operations reduces risk of the DRE systems while preserving their advantages. The research framework offers a secure trustworthy system by applying high-assurance computing techniques to voting technology, through implementing TPM that secures data with private signature keys (platform vote ballots (PVB) that prevents unauthorized vote modification, insertion, or deletion), stores measurements of booted software, and manages onboard nonvolatile memory, in the proposed framework, TPM verify the signatures of both the individual votes and the storage area using the PVB public key. Verification ensures that the DREs booted the correct software, voters used the correct ballots, and the votes were not modified, omitted, or illegally inserted or deleted. This led that the proposed framework can overcome the issues of DRE, when implementing the suggested solution TPM for more security of E-Voting systems.

The **Scytl** architecture suggests using a hardware security module to protect chained digital signatures but not signature keys, and uses light-weight voting software booted from a CD-ROM to eliminate reliance on preinstalled software and hardware, which makes it vulnerable to attacks and replacement of media *(Fink, R., Sherman, A., 2009)*. The research proposed framework with TPM stores and uses private keys only in tamper-resistant hardware, preventing attacks or unauthorized disclosure of the keys.

As for others who implanted **TPM** on E-voting System, Arbaugh suggested using TPMs in voting by outlining an on-line protocol for attesting systems through a central server, but omit key design details. Rössler, *et al.* proposed using hardware security modules in postal-voting where each voter submits a ballot encrypted with a public key to the tallying server. Also omit key design details. Paul and Tanenbaum sketched a voting system architecture incorporating TPMs, but the TPMs' role assures only correct software, the platform state is not bound to the cast ballot. Feldman, *et al.* suggested using trusted computing technology, cautioning that this technology could not prevent malicious code from changing future votes by altering data before it is sent to the storage device *(Fink, R., Sherman, A., 2009).* In the proposed framework hardware and correct software are used to develop chain of trust. TPM signs each cast ballot, so it detects any malicious software before modifying a vote.

The proposed framework gives integrity assurance to the voter in the polling location, and offers security assurance to the election authority that the correct software was installed, that voters used the correct ballot, and that votes were securely stored and transmitted to the central tallying location, detecting any malicious installed software in the polling booth early.

6.5 Conclusion

As for the evaluation result of primary and secondary testing of the proposed framework, the findings were high acceptance of TPM as a proposed solution for enhancing the security of E-Voting system. The other finding from the questionnaire (2) feedback, that the proposed frame work can enhance the security of E-Voting system channels, and can mitigate the E-Voting systems attacks. The second evaluation which was based on the literature review findings that the framework proposed through implementing TPM, can overcome the issues with the existing E-Voting systems such as, DRE, E2E, Scytl and some of E-Voting systems that implemented TPM. Finally the results of the evaluation were in the favor of the proposed framework.

CHAPTER-SEVEN

CONCLUSION

7.1 Introduction

Many countries nowadays dismissed and discarded E-Voting and returned to paper ballot voting such as Germany *(European Digital Rights, 2009)*, which cost large amount of money loss and wasted materials, plus jobless people. All of this happened because of insecure system and machine malfunction.The lost and uncounted large amount of votes associated with paper ballots voting could very well be contributing to biased political decisions. Populations are increasing millions of votes have to dealt with , let alone the information technology invasion, every day with new invention in technology and communication that will lead to conclusion that time cannot go back means we have to cope with technology. Electronic voting holds great promise for keeping democracy vibrant in the modern age. The usage of DRE voting systems is easy and less confusing than older paper ballot or punched-card methods. For instance, DRE systems often use touch screens so the voter does not need facility with keyboard and mouse. DRE voting machines can display pictures for voters who have difficulty reading, and can provide aural cues for the blind. Casting votes over the Internet, if secured, would make voting more convenient and enable shut-ins or those in remote areas to vote without absentee ballots. It could even usher in a new form of democracy with more frequent and direct voting on issues directly relevant to the citizens.

Voting in every method or channel is becoming very important nowadays, as it interact with people's daily live. For an example (iDTV) voting "American Idol" program which people vote their preference in real time, in education field choosing the leader, in governmental field choosing the nation's leader and so on, the solution is not to abandon technology but to cope with it and enhance it. Through this research suggested solution for enhancing the security through applying trusted computing standard , that a huge companies grouped together to solve the critical issues of information technology such as security by introducing trusted platform, to be applied on different electronic devices such as Pc's and mobiles maximize the security and gain people's confidence.

7.2 E-Voting and Information Technology Management

Technology is used, for example, to compile voter lists, to draw electoral boundaries, to manage and train staff, to print ballots, to conduct voter education campaigns, to record cast votes, to count and consolidate vote results and to publish election results. The appropriate information technology to elections can increase administrative efficiency, reduce long-term costs and enhance political transparency. Technologies used for elections can include software programs and electronic equipment, such as computers, PDAs, mobiles, printers and bar code readers. Other new materials such as cardboard, fiber glass and plastic used in polling equipment, printing presses, ball point pens, manual typewriters, electronic calculators and radios, or newer technologies like optical scanners, digital mapping and the Internet. *(ACE, 2010)*

The use of technology in elections is not an end in itself, but it assists in electoral management. For example, E-Voting process includes database management systems that can be used in several components of the election process, such as voter lists, material inventories, personnel management, payroll, election results dissemination and statistics.

The main focus is in this thesis is the information technology management of E-Voting technologies, that are currently in use around the world and framework for the implementation and enhancing of security platform within cost effectiveness, usability and application boundaries to gain trust and confidence in this vital electoral system in a cost effective and efficient way . There were many methods of enhancing the security of E-Voting system such as including external components (smart cards, biometrics) which requires more cost for the equipment itself, managing, maintaining, auditing and training additional cost. If comparing the implementing TPM with other trusted solution like implementing biometrics, implementing TPM is almost cost free as it is imbedded in many operating system software and hardware.

7.3 Conclusion related to the research Questionnaire – Problem

The selected methodology for this research was questionnaire over many methods for it benefits, such as simplicity, low cost and most important factor is that the security expert's which are the targeted sample time is limited and they cannot be located according to their busy schedule, so the questionnaire was given to them and collected later. The aim of the first questionnaire was to find the most preferred channel for voting, the serious problems in E-Voting system and the level of acceptance of the proposed solution (TPM). And the preference was that Touch screen are highly preferred as voting channel, next are internet voting and mobile (SMS), then (iDTV) and (IVR), although the telephone method and paper ballots were not preferred. The security issues found in E-Voting system were fraud and trust that effect the voting process, then issues of user spoofing, viruses and privacy, which indicates the seriousness of these issues for the need to optimize the security to overcome these problems.

All voting systems depends on software for efficiency, usability, and accessibility, but they carries risks including privacy even for software independent verification systems such as E2E, that cannot fully satisfy ease of administration, information assurance, and usability alone. TPM increases privacy by ensuring the correct software is running. It enables excellent usability and accessibility building trustworthy electronic interfaces. And helps voters catch problems in the polling location, to ensure secure system the cost of more complicated engineering design and key management *(Fink, R., and Sherman, A., 2009).*

The second questionnaire was conducted to the same sample to evaluate the proposed framework; and the results were, high acceptance of TPM as a proposed solution, for enhancing the security of E-Voting systems and voting channels. In addition the proposed framework can mitigate the E-Voting systems attacks to provide a trustworthy E-Voting system, and to increase voter's turnout. Finally the **Deliverables** of the project were met

Evaluating and reviewing the current E-Voting System Management Framework, and identify the gaps which are in the current E-Voting Management Framework to be targeted by TPM, and producing Trustable E-Voting System Management Framework using TPM.

7.4 Recommendation / suggestion

To protect the accuracy and impartiality of the E-Voting process, the following recommendations are suggested:

7.4.1 All E-Voting systems must embody careful engineering, strong safeguards, and rigorous testing in both their design and operation.

7.4.2 Voting systems should have inspection of a physical record to verify voters vote has been accurately cast and to serve as an independent check on the result produced and stored by the system. Making those records permanent (i.e., not only based in device memory) provides a means by which an accurate recount may be conducted.

7.4.3 E-Voting system can include Biometric voter verification for ensuring the reliability, security, and verifiability of public elections E-Voting system.

7.4.4 Poll workers should be sufficiently trained and voters educated.

7.4.5 E-Voting system must ensure the reliability, usability, security, and verifiability of public elections is fundamental to a stable democracy Convenience and speed of vote counting are no substitute for accuracy of results and trust in the process by the electorate.

7.4.6 E-Voting system must have Validation and Verification processes to assure the security and reliability of the E-Voting protocols and systems.

7.4.7 There should be well documentation and feedback on all the election process to prevent the mistakes happened and to improve the process for next election.

7.4.8 E-Voting system must be accessible to people who speak different languages, have a wide range of handicaps, or may be serving overseas.

7.5 Limitation of the Study

7.4.9 One of the main limitations that this research faces is difficult to arrange a meeting for an interview with the expert personnel; it took a long time to fulfill the survey procedure.

7.4.10 The study faced one of the biggest challenges of obtaining genuine information from secondary data as for limited resources and access.

7.6 Self Review

This research faced a lot of challenges, first adoption to the new environment in Malaysia, as it has different weather and culture, affected the first period of the study, in such a way that the three first months took only three modules out of four, the next three months starting the RMP with four modules, was very hard especially with health limitation because of the Dengue fever that infected me during the second semester. Starting the literature review and proceeding with my final dissertation was accompanied with HCI last module, made me expand my project submission till July to fulfill the Master degree requirements. The limitation of time, and collection information from primary and secondary resources was another challenge that faced me during my studies. Evaluating and testing the framework was the hardest task because of the effort and time given to locate the security expert people.   Cooperation from the program leader Miss Geetha and my Supervisor Mr. Ali were great on helping me to finish my thesis with quality documentation.

The modules that were taken during the master, assisted in gaining deep knowledge of how to conduct the research based on information technology, to contribute with providing dissertation that benefits the society.

Time management was effected because of uncontrolled circumstances especially with the failure of my laptop and stolen hardware, so I started my project all over again in April 2010 and managed to finish in June 29, 2010, also for the VISA limitation and family circumstances.

7.7 Future Direction

The research study can be extended to implementation and development of the trustable electronic government framework management system using trusted platform module (TPM), also can be extended in the design stage, as considering the usability and human computer interaction (HCI) part, not to mention voters education, and the increasing information technology awareness all over the world, in addition the new trends in green computing.

7.8 Conclusion

E-Voting systems are becoming very important governmental service portal to many modern democracies. National governments and local administrations are continuously searching ways of how to streamline the voting process and increase voter participation and voting turnout. The use of information technology and computer-based systems to collect and tally votes seems to be a logical and effective way to accomplish these goals. Unfortunately, real-world implementations of E-Voting systems have series of issues that worry both technologists and the general public.

Cost and security are the most two important factors along with usability and quality of service to the success of E-Voting systems. In this research the security related procedures that are required for the successful development and deployment of E-Voting in legally-binding government elections was explored, the research was initiated on theoretical basis, which justifies the necessity for security in deploying E-Voting Systems, the problem question was explored of who and what should be safeguarded in the course of the e-electoral process and what is the effect of using TPM as TCG standard for optimizing the security level. Based on the research study, the security in E-Voting has two aspects, the technical and the procedural one. As from the technical perspective further research is necessary to ensure full and complete voter authentication and voting security to enable an e-election. However, security can also be enhanced through providing procedural security measures at specific points in the e-electoral process through implementing TPM.

The analysis of the experts feedback from the survey conducted on E-Voting security issues confirmed past cases of procedural security issues. The need to further exploration on the re-design of the electoral process and consider procedural security in view of the increased complexity of the E-Voting processes, which can involve multi-channel E-Voting options, and the increase in the number of agents involved in the administration of elections. Security is a problem because, to date, the commercially available technology does not provide a completely secure e-transaction environment. It is not the aim of this research to address the future technical advances of security in E-Voting, but rather, how to improve the level of security of the E-Voting procedures, within the limitations of technology available. The proposed framework addresses all these issues through providing TPM as a solution to develop trustable E-Voting system.

References

ACE, 2010a, *Electronic Voting Systems*, [online] Available on http://aceproject.org/ace-en/topics/et/eth/eth02/eth02b/onePage [Accessed on June19, 2010]

ACE, 2010, *Overview of Elections and Technology*, [online] Available on http://aceproject.org/ace-en/topics/et/et10 [Accessed on April 7, 2010]

Ahmad, T. , et al, 2009, *An Efficient Mobile Voting System Security Scheme Based on Elliptic Curve Cryptography* , Third International Conference on Network and System Security, 2009. NSS '09, pp. 474-479.

Bajikar, S. 2002, Mobile Platforms Group Intel Corporation, *Trusted Platform Module (TPM) based Security on Notebook PCs - White Paper* [online], Available on http://www.intel.com/design/mobile/platform/downloads/Trusted_Platform_Module_White_Paper.pdf [Accessed on June 28, 2010]

Balzarotti, D. et al., 2009, *An Experience in Testing the Security of Real-World Electronic Voting Systems*, Software Engineering, IEEE Transactions on, PP (99), 1.

Berger, B., 2008, *Crypto chip: How the TPM bolsters enterprise security* [online], Available on http://www.securecomputing.net.au/Feature/115566,crypto-chip-how-the-tpm-bolsters-enterprise-security.aspx [Accessed on June 28, 2010]

Bolan, C., Mende, D., 2004, *Computer Security Research: Approaches and Assumptions*, [online] Available on http://scissec.scis.ecu.edu.au/proceedings/2004/aism/Bolan-Mende.pdf [Accessed on June 7, 2010]

Borras, J., 2004, *Overview of the work on e-voting technical standards*, [online] Available on https://ssl.bnt.com/idealliance/papers/xmle02/dx_xmle02/papers/04-04-01/04-04-01.pdf [Accessed on June 5, 2010].

Borchuck, J., 2007,*from $3,150 each to practically worthless Six counties still owe $33-million on obsolete voting machines*, St. Petersburg Times [online] Available onhttp://www.sptimes.com/2007/07/12/State/From_3_150_each_to_pr.shtml [Accessed on June 16, 2010].

Braun, N., Bundeskanzlei, BK, 2006, Electronic Voting 2006 Conference Bregenz, *Swiss E-Voting Pilot Projects Evaluation, Situation Analysis and How to Proceed* [online] Available on http://www.e-voting.cc/static/evoting/files/Swiss_Experiences.pdf [Accessed on June 28, 2010]

Cetinkaya, O., 2008 , *Analysis of Security Requirements for Cryptographic Voting Protocols (Extended Abstract),* ARES '08: Proceedings of the 2008 Third International Conference on Availability, Reliability and Security - Volume 00, IEEE Computer Society [online] Available on http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4529515&isnumber=4529303 [Accessed on March 18, 2010].

Cetinkaya and D. Cetinkaya, 2007, *Verification and Validation Issues in Electronic Voting* [online] Available on http://www.ejeg.com/volume-5/vol5iss2/Cetinkaya%20and%20Cetinkaya.pdf [Accessed on June 2, 2010].

Chaum, D. et al., 2008. *Scantegrity: End-to-End Voter-Verifiable Optical- Scan Voting.* Security & Privacy, IEEE, 6(3), 40-46.

Cooper, D, Schindler, P, 2003, *Business Research Methods*, Eighth Edition, Publisher McGraw Hill, PP (149).1

Clos, A., 2008, *Secure Client Platforms for Remote Internet Voting,*[online] Available on http://www.cdc.informatik.tu-darmstadt.de/reports/reports/Johannes_Clos.diplom.pdf [Accessed on June 17, 2010]

Council of Europe, 2003, *Questionnaire on Security Solutions in the EML Process Model* [online] Available on http://www.coe.int/t/dgap/democracy/activities/ggis/evoting/work_of_evoting_committee/03_background_documents/06Security_Questionnaire_en.asp [Accessed on May 28, 2010].

Cyllah, A., IFES, 2010, *Democracy and Election in Africa: Almami Cyllah's Testimony to Congress* [online] Available onhttp://www.ifes.org/Content/Videos/2010/Democracy-and-Election-in-Africa-Almami-Cyllahs-Testimony-to-Congress.aspx [Accessed on June 20, 2010]

De Rossi, L., 2007, *Computer Security: Trusted Computing Initiative Sets You As Your Own Computer Worst Threat - Protection Or Menace?*, [online], Available on http://www.masternewmedia.org/news/2007/02/02/computer_security_trusted_computing_initiative.htm#ixzz0pi667DiE [Accessed on June 2, 2010].

European Digital Rights, 2009, *No e-voting in Germany* [online] Available on http://www.edri.org/edri-gram/number7.5/no-evoting-germany [Accessed on June 29, 2010].

EJEG Electronic Journal of E- Government, 2005, *Bringing Confidence to Electronic Voting*, Paper1 Issue 1, [online] Available on http://www.ejeg.com/volume-1/volume1-issue-1/issue1-art5.htm [Accessed on May 28, 2010].

Ekberg, N., Zeglen, R., 2009, *Security Challenges of Electronic Voting Systems (NYSTEC)*, [online] Available on http://www.cscic.state.ny.us/security/conferences/security/2009/documents/Challenges-of-Electronic-Voting-Systems.pdf [Accessed on June 28, 2010].
Ericson, P., 2004, *TCPA/TCG and NGSCB: Benefits and Risks for Users* [online] Available on *http://pericson.com/files/tcpa-tcg-and-ngscb-benefits-and-risks-for-users.pdf* [Accessed on June 26, 2010]

Fang, W., et al, 2009 , *Research and application of trusted computing platform based on portable TPM , iccsit, pp.506-509, 2009 2nd IEEE International Conference on Computer Science and Information Technology, 2009* [online] Available on http://www.computer.org/portal/web/csdl/doi/10.1109/ICCSIT.2009.5234829 [Accessed on June 28, 2010]

Feng, Q. et al., 2009. *Voting Systems with Trust Mechanisms in Cyberspace: Vulnerabilities and Defences*, Knowledge and Data Engineering, IEEE Transactions on, PP (99), 1

Chaum, D. et al., 2008. *Scantegrity: End-to-End Voter-Verifiable Optical- Scan Voting. Security & Privacy,* IEEE, 6(3), 40-46.

Fink, R. et al, 2009. *TPM Meets DRE: Reducing the Trust Base for Electronic Voting Using Trusted Platform Modules*. Information Forensics and Security, IEEE Transactions on, 4(4), 628-637.

Fink, R., et al, 2009, *TPM Meets DRE: Reducing the Trust Base for Electronic Voting Using Trusted Platform Modules,*

Fink, R., Sherman , *A., 2009, Combining End-To-End Voting With Trustworthy Computing for Greater Privacy, Trust, Accessibility, and Usability* [online] Available on http://csrc.nist.gov/groups/ST/e2evoting/documents/papers/SHERMAN_trustworthye2e-NISTrevised9-25-09a.pdf [Accessed on May 31, 2010].

Infineon, 2009, *Technology Media*, [online], Available on http://www.infineon.com/cms/en/corporate/press/news/releases/2009/INFCCS200912-015.html [Accessed on June 1, 2010].

IT Security Journal, 2008, *Guide to Trusted computing*, [online], Available on http://www.itsecurityjournal.com/index.php/Latest/Guide-to-Trusted-Computing.html[Accessed on June 2, 2010].

Kelsey, J., et al, 2009, *Attacking Paper-Based E2E Voting Systems,* [online], Available on http://csrc.nist.gov/staff/jkelsey/attacking-e2e-voting-systems.pdf [Accessed on June 5, 2010].

Lee, Y. et al, 2010. *Towards trustworthy e-voting using paper receipts* [online] Available on http://www.sciencedirect.com/science/journal/09205489[Accessed on April 28, 2010].

Manolopoulos ,M., et al., 2008 ,ACM International Conference Proceeding Series; Vol. 351 Proceedings of the 2nd International Conference on Theory and Practice of Electronic Governance*A Step-Wise Refinement Approach for Enhancing e-Voting Acceptance* [online] Available on http://portal.acm.org/citation.cfm?id=1509096.1509153 [Accessed on June 26, 2010]

Monnoyer, S., 2005, *Challenge citizenship* [online] Available on http://www.evoting.cc/static/evoting/files/monnoyer-smith [Accessed on March 20, 2010].

Monnoyer, S., 2005, *how e-voting technology challenges traditional concepts of citizenship: an analysis of French voting rituals*, [online], Available on http://www.evoting.cc/static/evoting/files/monnoyersmith_challenge_citizenship_61-68.pdf [Accessed on December 4, 2009].

Moynihan, D, 2004, *Building Secure Elections: E-Voting, Security, and Systems Theory* [online] Available on http://catedras.fsoc.uba.ar/rusailh/Unidad%204/Moynihan%202004%20Building%20secure%20elections%20y%20e%20voting.pdf [Accessed on January 14, 2010].

M2SYS, 2010, *Biometric Secure Single Sign-On Software* [online] Available on http://www.m2sys.com/EBS.htm[Accessed June 6, 2010]

Ondrisek, B., 2009, Proceedings of the 42nd Hawaii International Conference on System Sciences - 2009, *E-Voting System Security Optimization* [online] Available on http://electrobabe.files.wordpress.com/2009/01/ondrisek_e-voting-system-security-optimization_05-02-02.pdf [Accessed on June 28, 2010].

Öksüzo˘gluy, E., Wallach, D., 2009, *Vote Box Nano: A Smaller, Stronger FPGA-based Voting Machine (Short Paper)* [online] Available on http://www.usenix.org/event/evtwote09/tech/full_papers/oksuzoglu.pdf [Accessed on June, 16, 2010]

ProCon.org, 2009, *Historical Timeline Electronic Voting Machines and Related Voting Technology,* [online] Available on http://votingmachines.procon.org/viewresource.asp?resourceID=273#1975 [Accessed on June 20, 2010]

Prosser, A., Krimmer, R., 2004, *The Dimensions of Electronic Voting Technology, Law, Politics and Society,* [online] Available on http://subs.emis.de/LNI/Proceedings/Proceedings47/Proceeding.GI.47-3.pdf [Accessed on June 20, 2010]

Ryan, P. et al., 2009. *PrÊt À Voter: a Voter-Verifiable Voting System*. Information Forensics and Security, IEEE Transactions on, 4(4), 662-673.

Qi Yao et al., 2009. *A trust and risk based dispute settlement mechanism in e-voting. In Machine Learning and Cybernetics,* 2009 International Conference on. Machine Learning and Cybernetics, 2009 International Conference on. pp. 2775-2780. Available at: 10.1109/ICMLC.2009.5212648.

Rusinek, D., Ksiezopolski, B, 2009, *Voter non-repudiation oriented scheme for the medium scale e-voting protocol*, Proceedings of the International Multi conference on Computer Science and Information Technology pp. 325–330 [online] Available on http://www.proceedings2009.imcsit.org/pliks/137.pdf [Accessed on May 29, 2010].

Security Focus, 2009, *U.S. issues revised e-voting standards,* [online], Available on http://www.securityfocus.com/brief/968 [Accessed on June 20, 2010]

Sony VAIO, 2008, Reliable Mobility, [online] Available on http://vaio-online.sony.com/prod_info/vgn-sz75gn_b/reliable_mobility.html [Accessed on June 1, 2010].

Singleton, K. 2008, *Many Shades of Green: AMSN to Implement Electronic Voting*. Med - Surg Matters, January 1, 9, [online] Available on http://www.proquest.com/ [Accessed on March 27, 2010].

Social Studies, n.d, *History of Voting Machines* [online], Available on *http://www.glencoe.com/sec/socialstudies/btt/election_day/history.shtml* [Accessed on June, 16, 2010]

Stubblefield, A, 2004., *Analysis of an Electronic Voting System***,** IEEE Symposium on Security and Privacy 2004 [online], Available on http://avirubin.com/vote.pdf [Accessed on June 28, 2010]

Sturton,C., et al , 2009, *On Voting Machine Design for Verification and Testability,* Conference on Computer and Communications Security
Proceedings of the 16th ACM conference on Computer and communications security, [online] Available on http://portal.acm.org/citation.cfm?id=1653662.1653719&coll=GUIDE&dl=GUIDE&CFID=71128634&CFTOKEN=19221839 [Accessed May 4, 2010]

Saunders, M., et al, 2007, Research Methods for Business Students, Fourth Edition, Publisher Pearson [online] Available on http://wps.pearsoned.co.uk/ema_uk_he_saunders_resmethbus_4/51/13274/3398341.cw/index.html [Accessed on May 20, 2010]

Trusted Computing Group, 2009 [online] Available on http://www.trustedcomputinggroup.org/ [Accessed on June 11, 2010].

United States Election Assistance Commission, 2009, *Current and Future Trends in Election Technology* [online] Available on http://www2.sbe.virginia.gov/GRDocs/Training/2009%20Annual%20Training/070109%20The%20Future%20of%20Voting%20Equipment%20Brian%20Hancock.ppt [Accessed on June 26, 2010]

Verton, D., 2004, *Computer World Government*, *E-voting system security, integrity under fire* [online] Available from http://www.computerworld.com/s/article/92950/E_voting_system_security_integrity_under_fire?taxonomyId=70&pageNumber=2 [Accessed June 26, 2010]

Vijayan, J., 2009, *E-voting system lets voters verify their ballots are counted*, Computerworld [online] Available on http://www.computerworld.com/s/article/9140285/E_voting_system_lets_voters_verify_their_ballots_are_counted [Accessed on June 16, 2010].

Volkamer, M., 2009, *Evaluation of Electronic Voting: Requirements and Evaluation Procedures to Support Responsible Election Authorities*, Publisher Springer, 2009.

Word press, 2009, *OAV Internet Voting and OFW representation – Hoping for the best* [online] Available on http://ofwempowerment.wordpress.com/2009/11/ [Accessed on June 19, 2010]

Wright, J., 2004, *MIRROR OF THE NATION'S MINDAustralia's Electoral Experiments* [online] Available on http://home.vicnet.net.au/~prsa/history/mirrornm.htm [Accessed on June 16, 2010].

Xenakis, A., Macintosh, A., 2004, Procedural *Security Analysis of Electronic Voting* [online] Available on http://svn.assembla.com/svn/network_security/Papers/p541-xenakis.pdf [Accessed on June 26, 2010]

Yang, C., et al , 2009, *Implementation of an Electronic Voting System with Contactless IC Cards for Small-Scale Voting*, In Information Assurance and Security, IAS '09, Fifth International Conference on. pp. 122-125.

Ying Lai, J., et al, 2008, *Design and Implementation of an Electronic Voting System with Contactless IC Cards* [online] Available on http://59.127.136.65/publications/200805ICIM_eVoting.pdf [Accessed on June 15, 2010]

Glossary

Abbreviation	Meaning
AIS	American Information Systems
BMD	Ballot Marking Devices
DRE	Direct Record Electronic
E	Electronic
EC	European Commission
EAC	Election Assistance Commission
E-Government	Electronic Government
ES&S	Election System and Software
EML	Election markup language
EVT	Electronic Voting Technology
E-Voting	Electronic Voting
FED	Federal Election Commission
HAVA	Help America Vote Act
MTM	Mobile Trusted Module
NIST	National Institute of Standards and Technology
PCRs	Platform configuration registers
TPM	Trusted Platform Module
TCG	Trusted Computing Group
VSS	Voting System Standards
VVS	Voluntary Voting System
VVSG	Voluntary Voting System Guidelines
VVPAT	Voter Verified Paper Audit Trail

Appendix (1) Project Proposal

PROJECT PROPOSAL

Student Name: ***Mervat Adib Bamiah***

Student No: ***TP020123***

Email Address**:** ***tp020123@ex.apiit.edu.my***

Award Name: ***Master Information Technology Management***

Site Name: ***Staffordshire University, UCTI, APIIT***

Project Title: ***A Trustable Electronic Government Voting Management Framework Using Trusted Platform Module (TPM)***

Proposed Supervisor: ***Mr. Ali Dehghantanha***

Topic Related Modules: ***NST, ITPM, HCI, E-COMMERCE, and EDS***

"*It is enough that the people know there was an election. The people who cast the votes decide nothing*

The people who count the votes decide everything." -- Joseph Stalin

INTRODUCTION

Electronic Voting is a challenging approach for increasing Electronic Participation. However, lack of citizens' trust is the main obstacle that prevents its successful realization**.**

The approach is based on these components:

- The decomposition of Electronic Voting systems into "layers of trust" for reducing the complexity of managing trust issues in smaller manageable layers,
- Identifying and documenting security critical aspects of the emoting system, and a cryptographically secure Electronic Voting protocol.
- Defining and building people trust as positive attitude towards a system that performs its operations transparently.
- A voting system must be usable by people regardless of their age, infirmity, or disability

The main concern in this research is to provide a framework for Electronic Voting Management through using trusted platforms and mobiles. The Trusted Platform Module (TPM) and Mobile Trusted Module (MTM) are promising security technology solutions for the future of secure computing systems by providing **hardware-based** foundation of trust, enabling enterprises and governments to implement, manage, and enforce a number of trusted Crypto-Graphy, storage, integrity management, attestation and other information security capabilities.

Project background

According to (Scholl, 2003) Electronic Government is, "The use of Information Technology to support government operations, engages citizens, and provides government services" which includes both electronic administration and electronic participation by citizens”.

As for Von Lucke and Reinemann definition of Electronic Democracy “The electronic representation of the democratic processes” which contains:

- Electronic Participation “Information acquisition, Formation of an opinion”.
- Electronic Voting “The decision itself”. *(Prosser, A., Krimmer, R., 2004).*

Electronic Voting as a part of Electronic Government is “Using a computer based machine to display an election ballot and record the vote” *(ZDNET, 2009).*

It is an application that encompasses of several different types of voting embracing both electronic means of casting a vote and counting votes.

Electronic Voting Technology can include:

- Punch card .
- Optical scan voting system.
- Voting kiosks (including self-contained touch-screen style voting systems called Direct-recording electronic (DRE).
- Ballot and votes via telephones, private computer network , or the Internet.

Electronic Voting Technology advantages and Disadvantages:

Lesser cost, speed the counting of votes and tabulation of results, improve accessibility, greater accuracy, and lower risk of human and mechanical errors also It provides improved accessibility for disabled voters. Disadvantage of Electronic Voting: machines that they use touch screens for a voter's selection, so there is no paper trail to be used for auditing which leads to no way of detecting a programming error or hack as problems in accuracy and reliability *(ZDNET, 2009).*

Manipulation and fraud:

According to (Computerworld - Washington, 2004) security researchers said that without voter - verifiable paper receipts, the 50 million Americans who will use electronic voting machines are uncertain that their votes will be recorded properly. Also the large and complexity of code base powering the systems allows manipulation of election results. "My biggest concern is that in a very large trusted computing base, the threat of somebody with access to the development environment of the code base, particularly the vendor, basically is in position to make the outcome of the election come out how they would like, and it's virtually undetectable," said Avi Rubin, a professor at the Johns Hopkins University Information Security Institute. "

Potential vendors influencing the elections, especially since some have taken active roles in operating polling stations and, in the case of Diebold Election Systems' CEO Walden O'Dell, stated publicly the intent to deliver election results to President George W. Bush. (*Verton, D., 2004)* Uunauthorized privilege escalation, incorrect use of cryptography, vulnerabilities to network threats, and poor software development processes, voters can cast unlimited votes without being detected by any mechanisms within the voting terminal software. *(STUBBLEFIELD, A., 2004).*

The suggested solution in building users trust and approaching the problems is to use the trusted computing platform, which is an industry standard, as the way to verify the accuracy and reliability of the code installed. According to Trusted Computing Group (TCG) many organizations already have a **security** tool the Trusted Platform Module (TPM), which is a hardware-based security and cryptography chip built into virtually every enterprise devices such as (class desktop, laptop, PC or Mac), to facilitates key managements and escrow for verifying the identity of a PC; can securely sign, encrypt, and decrypt e-mails and digital documents; manages full-drive encryption; provides the second factor in multifactor authentication; and helps assess the security and integrity of the host device . There are more than 100 million computers shipped to date have a TPM installed, as well as numerous government agencies, including the Department of Defense, that explicitly require a TPM for all new computers. *(TCG, 2009)*

Project Problems

- Electronic voting systems have major security problems.
- Security issues in the increased complexity of multiple-channel voting, provided by a multiplicity of agents involved in management of electronic elections.
- Difficulty of achieving Change management and culture change more than technology and applications.

Project Aims and Objectives

- Providing a trustable Electronic Voting Management frame work using TPM.

The objectives of this research project are to:

- Critically analyze the effects of implementing TPM in the current Electronic Voting System.
- Critically analyze the Issues related to the usage of TPM in the Electronic Voting System.
- Justifying the Pros & Cons of using TPM in the Electronic Voting System.
- Proposing a Management Framework for using TPM in the Electronic Voting System.
- Considering practices that should be adopted to reduce risks of using TPM in the Electronic Voting System.
- Extending the usage of procedural security measures to the need for transparency in electronic voting and public confidence and trust towards the newly introduced voting practices.

Research Program Plan

- Evaluating and Selecting information obtained through e-journals, web pages, white papers, books, conference proceedings, research papers and any resource available in the university library (ACM , Athens …etc)
- Reviewing the current Electronic Voting Management Framework.

- Critically discussing the gaps and weaknesses in the current Electronic Voting Management Framework to be targeted by TPM.
- Suggesting a Framework to cover the gaps and weaknesses in the current Electronic Voting system.
- Critically analyzing and deploying of the Electronic Voting Management Framework using TPM.
- Refining

Project Deliverables

- The current Electronic Voting Management Framework
- The gaps and weaknesses in current Electronic Voting Management Framework to be targeted by TPM.
- Reviewing current Electronic Voting Framework and filling the gaps
- Framework & framework presentation
- Thesis

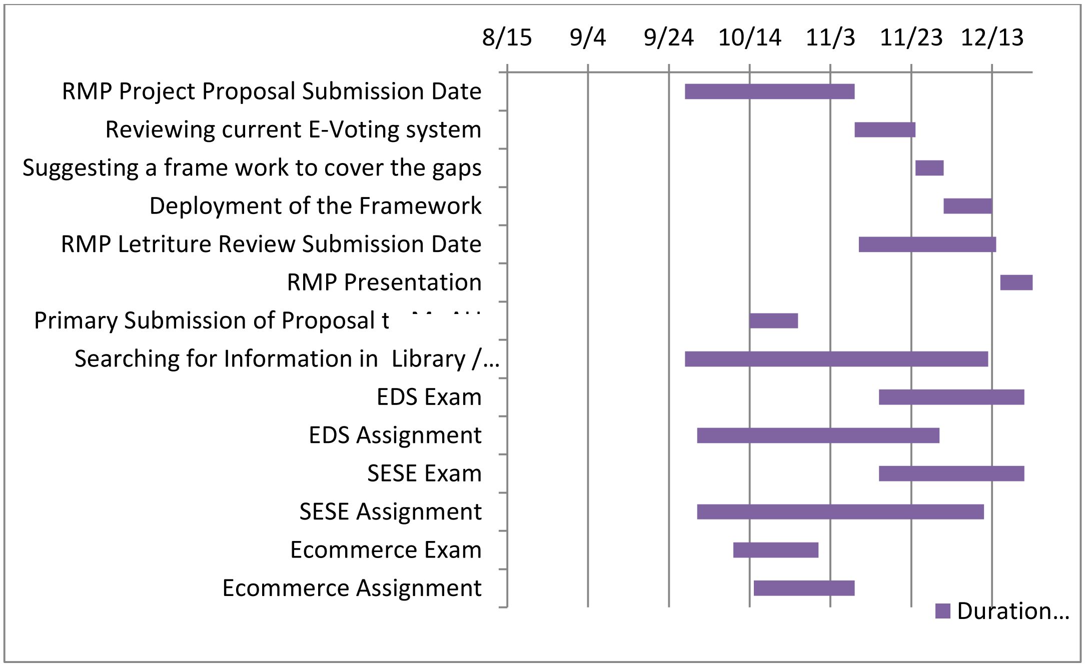


Figure (1) Project Plan

References

Prosser, A., Krimmer, R., 2004, *The Dimensions of Electronic Voting Technology, Law, Politics and Society*, [online] Available on http://subs.emis.de/LNI/Proceedings/Proceedings47/Proceeding.GI.47-3.pdf, Robert.Krimmer}@wu-wien.ac.at [Accessed 28th Oct 2009]

ZDNET & CBS Interactive Inc 2009, *ZDNet Definition for: E-voting*, [online] Available on http://dictionary.zdnet.com/definition/E-voting.html [Accessed 28th Oct 2009]

Verton, D., 2004, *Computer World Government*, *E-voting system security, integrity under fire* [online] Available from http://www.computerworld.com/s/article/92950/E_voting_system_security_integrity_under_fire?taxonomyId=70&pageNumber=2 [Accessed 4th November 2009]

STUBBLEFIELD, A., 2004, Analysis *of an Electronic Voting System*, *IEEE Symposium on Security and Privacy 2004* [online] Available on http://avirubin.com/vote.pdf [Accessed 4th November 2009].

Winmark Corporation, 2009, *E-Government and Security Issues* [online], Available on http://www.wbsonline.com/resources/e-government-and-security-issues/

[Accessed 4th November 2009]

World bank Organization, Information Solution Group, *Designing and implementing e-Government: Key Issues, Best Practices and Lessons Learned* [online] Available on http://siteresources.worldbank.org/INTEDEVELOPMENT/Resources/559323-1114798035525/Workshop_Summary.pdf [Accessed 4th November 2009].

Trusted Computing Group, 2009, Enterprise *Security: Putting the TPM to Work* [online] Available on http://www.trustedcomputinggroup.org/resources/enterprise_security_putting_the_tpm_to_work [Accessed 28th October 2009].

Appendix (2) Literature Review

Project Literature Review

Student Name: ***Mervat Adib Bamiah***

Student No: ***TP020123***

Email Address**:** ***tp020123@ex.apiit.edu.my***

Award Name: ***Master Information Technology Management***

Site Name: ***Staffordshire University, UCTI, APIIT***

Project Title: ***A Trustable Electronic Government Voting Management Framework Using Trusted Platform Module (TPM)***

Proposed Supervisor: ***Mr. Ali Dehghantanha***

Topic Related Modules: ***NST, ITPM, HCI, E-COMMERCE, and EDS***

Table of Contents

Glossary 140

INTRODUCTION 141

History of E-Voting systems 141

Electronic Government 144

Electronic Voting 144

Tasks of E-Voting System 145

Registration 145

Evolution of E-Voting technology standards 145

Benefits of E-Voting System over Traditional Voting 24

Evaluation of Voting Equipment 146

Elements of an E-Voting System 148

Security issues 45

E-Voting Recounting Issue 44

Increasing E-Voting Voter Turnout 56

Literature Review 154

Security Requirements for Cryptographic Voting Protocols 154

Elaborate Checklists for E-Voting Security Requirements 154

Towards a Successful E-Voting System 46

Proven technological excellence for the component of the system 55

Usage of open source technologies and publicly available information 55

Organize pre- and post- application information campaigns 55

E-Voting Suggested Framework 157

E-Voting Future 158

Enfranchising Voters through new E-Voting channels 158

Remote E-Voting (Internet Voting) 158

Conclusion 160

Recommendations 159

References 161

Glossary

Abbreviation	Meaning
AIS	American Information Systems
BMD	Ballot Marking Devices
DRE	Direct Record Electronic
E	Electronic
EC	European Commission
EAC	Election Assistance Commission
E-Government	Electronic Government
EML	Election markup language
EVT	Electronic Voting Technology
E-Voting	Electronic Voting
FED	Federal Election Commission
HAVA	Help America Vote Act
MTM	Mobile Trusted Module
NIST	National Institute of Standards and Technology
TPM	Trusted Platform Module
TCG	Trusted Computing Group
VSS	Voting System Standards
VVS	Voluntary Voting System
VVSG	Voluntary Voting System Guidelines
VVPAT	Voter Verified Paper Audit Trail

INTRODUCTION

The huge adoption and usage of information technology improved government services and the vibrancy of democracy. As for presidential election, governments have trusted technology, adopting E-Voting machines that offer enhanced voter convenience and eliminate the need for subjective recounts. *(Donald P. Moynihan, 2004)*

The voting problem is defined in terms of security requirements. It starts from the trade-off between receipt-freeness and individual verifiability. If a voting system provides any receipt which enables the voter to verify his vote in the final tally, then that receipt can also be used for vote buying or selling *(Cetinkaya, O., 2008).* The voter needs to verify the appropriateness and accuracy of voting process.

This literature review suggests an applicable solution in order to overcome the voting problem by introducing The Trusted Platform Module (TPM) and Mobile Trusted Module (MTM) which are promising security technology solutions for the future of secure computing systems by providing hardware-based foundation of trust, enabling enterprises and governments to implement, manage, and enforce a number of trusted Crypto-Graphy, storage, integrity management, attestation and other information security capabilities.

History of E-Voting systems

In the early 20th century after the implementation of E-Government, as a proposed solution for many problems according to the traditional voting system such as the increasing criticisms of existing voting procedures, increasing numbers of voters and multiple elections falling the same day and second-round runoffs that caused many countries to consider replacing ballot boxes with "voting machines *(Norris, P, 2004).* However, mechanization was limited to putting some buttons and vote counters in a booth before interest waned fatally after the unpromising results of 1970s trials in Europe and North America.

Late 1980s the first electronic systems came online, entering use on a national scale in Belgium and Holland in the early 1990s and Brazil in 1996. In France there were a few trials in Bordeaux and Brest in 1980 but the real test of the all-in-one electronic polling booth with a "built-in ballot box" was the 1999 European Union elections, followed by its use for the 2000 referendum asking their citizens whether or not to reduce the presidential term of office from seven to five years. The success of these two experiences led the Interior Ministry of France to approve three different types of electronic voting decree of 18 March 2004. All three are compatible with the traditional voting station but eliminate the need for a ballot box. Without directly threatening the physical survival of traditional voting devices, the systems nonetheless mark a step towards fundamental subversion of the traditional voting process *(Ledun, M., 2005)*

At the same time the Internet began fostering the first political and administrative applications for technocratic and community-based inspiration in North America and Europe .Most of the first private-sector initiatives were from the U.S.A began to promoting online voting systems for general meetings of corporate stakeholders and of professional associations. In Europe, Germany, Switzerland and the U.K. began studying new voting technologies in the mid-1990s through a series of pilot projects involving television, SMS, postal votes, etc *(Monnoyer-Smith, L.,2003).* However, the European Commission (E.C.) soon took the lead in online voting through its Fifth Framework Program for the User-friendly Information Society.

The issue of remote, online voting different from traditional E-Voting in a polling station because it directly undermines the material basis of the electoral process, but the denaturing of a voting process, led to perceive the new technologies as a threat to having been observed for a long time and sanctioned by custom voting ritual and reduce the technologies to a process of mass rationalization of government administration that transforms the citizen into a consumer, although the availability of the voter in specific time and location is hard to achieve and how close is the relationship between citizens and their elected representatives is another issue. *(Laurence Monnoyer -Smith, 2005)*

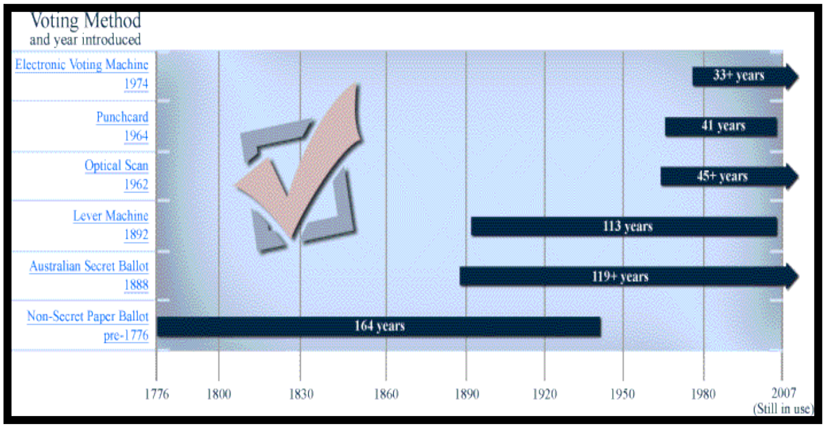


Figure (2.1) Historical Timeline Electronic Voting Machines

This timeline as in figure (2.1) above and the table below shows the history of Electronic voting technology from the first use of uniform paper ballots in 1856 through the Direct Recording Electronic Voting Machines in use today. In the table below the stages of voting system only are mentioned.

Year	Event	Citation
1856	Australia state of Victoria is the first to use Paper Ballots for voting (Australian Secret Ballot system)	(Pros & Cons, 2009)
1888	Massachusetts is the first state in the U.S. to use Paper Ballots for voting (Australian Secret Ballot system)	(Pros & Cons, 2009)
1889	New York the first American state to adopt paper ballots the other countries [1]raise their hands or write on pre printed paper Ballots/votes for state wide elections	(Ekberg, N., Zeglen, R., 2009)
1889	First mechanical lever voting machine (Myers Automatic Booth) prevents over voting, speeds up the vote counting process, and reduces the chance of dishonest vote counting	(Pros & Cons, 2009)
1892	New York began using lever machines	(Ekberg, N., Zeglen, R., 2009)
1962	The first use of optical scan ballots in Kern City, California	(Pros & Cons, 2009)
1964	State of Georgia was the first to use punch cards and computer tally machines BMD used for ADA requirements	(Ekberg, N., Zeglen, R., 2009)
1974	The first use of direct recording electronic voting machine S	(Pros & Cons, 2009)
1977	The first model of precinct-based optical scan systems	(Pros & Cons, 2009)
1982	The AIS model 315 is the first optical scan system to be used throughout the United States.	(Pros & Cons, 2009)
1987	The push-button machine was the first direct recording electronic voting machines to achieve significant commercial success.	(Pros & Cons, 2009)
1990	The FEC developed the first standards for e -voting systems.	(Ekberg, N., Zeglen, R., 2009)
1996	Optical Scanners (Mark sense) were used by 25% of registered voters and DRE used by 8% of registered voters in the United States.	(Ekberg, N., Zeglen, R., 2009)

2002	Federal Government enacted HAVA and formed the EAC to define VSS for design and testing of electronic voting systems.	(Ekberg, N., Zeglen, R., 2009)
2004	Nevada is the first state to insist that all electronic voting machines should be equipped with printers that produce a voter-verified paper audit trail.	(Pros & Cons, 2009)
2005	EAC released updated standards known as the VVS, VVSG and Computerized touch-screen systems DRE with VVPAT	(Ekberg, N., Zeglen, R., 2009)
2007	Increased public scrutiny, introducing open source systems allows the public to participate in the actual development of the system.	(Ekberg, N., Zeglen, R., 2009)
2007	submission of EML to assist and enable the election process, Mobile Voting	(Ekberg, N., Zeglen, R., 2009)
2009	NIST delivered Draft Voluntary Voting System Guidelines Version 1.1	(Security Focus, 2009)[2]

Electronic Government

According to (Scholl, 2003) Electronic Government is, "The use of Information Technology to support government operations, engages citizens, and provides government services" which includes both electronic administration and electronic participation by citizens". As for Von Lucke and Reinemann definition of Electronic Democracy "The electronic representation of the democratic processes" which contains:

- Electronic Participation as information acquisition, Formation of an opinion
- Electronic Voting "The decision itself". *(Prosser, A., Krimmer, R., 2004)*

Electronic Voting

Electronic voting refers to the use of computerized voting equipment to cast ballots in an election securely by implementing the cryptographic voting protocols to make electronic voting secure and applicable. The security requirements for cryptographic voting protocols are privacy, eligibility, uniqueness, fairness, receipt-freeness, accuracy, verifiability, and elaborate checklists presentation *(Cetinkaya, O., 2008).*

Electronic Voting as a part of Electronic Government is “Using a computer based machine to display an election ballot and record the vote*” (ZDNET, 2009).* It is an application that encompasses of several different types of voting embracing both electronic means of casting a vote and counting votes.

Tasks of E-Voting System

The main tasks of e-voting systems are as follows:

Registration of the voters in a list or registry, identification, authentication, and authorization of voters then casting of votes as the electronic ballot is displayed and may be cast anonymously by a citizen after that collecting of votes finally votes are processed and an election result is calculated and presented.

Evolution of E-Voting technology standards

Election and Ballot integrity

- Ballot secrecy
- Voter anonymity and Authentication
- Receipts and coercion resistance
- Anonymous channels
- Secure Bulletin boards and formal security analysis
- Threat models and Electoral systems
- Privacy, Verifiability and Transparency in E-Voting system

Benefits of E-Voting System over Traditional Voting

E-Voting existed as a solution for many traditional voting problems. Benefits of E-voting system are as follows: *(EJEG Electronic Journal of E-Government, 2005)*

- E-voting system can cast and count votes with higher convenience and efficiency.
- E-voting system increases the speed and accuracy of ballot tabulation.
- E-voting system saves materials required for printing and distributing ballots.
- E-voting system offers better accessibility for people with disabilities.

- E-voting system offers a flexible ballot design that can be modified at the last minute.
- E-voting system provides multiple-language support for the ballots.
- E-voting system permits the access to more information regarding voting options.
- E-voting system prevents unintentional mistakes by voters (both in over voting and under voting).

Evaluation of Voting Equipment

In the past, voters went to polling place and toke a blank ballots, then punch a hole or append the seal. If the seal is not clear enough, or the vote is damaged by soiling, it may bring some debate on the result the following are stages of evolving voting mechanism. *(Chaum, D., 2008)*

Paper - based voting: The voter take a blank ballot and use a pen or a marker to indicate his preferred candidate. Hand-counted ballots is a time and labor consuming process, but it is easy to manufacture paper ballots and the ballots can be retained for verifying.

Lever voting machine: is peculiar equipment, each lever is assigned for a corresponding candidate. The voter pulls the lever to poll for his preferred candidate. This voting machine can count up the ballots automatically its interface is not user-friendly enough, that is why training to voters is necessary.

Direct recording electronic voting machine: it integrates with keyboard; touch screen, or buttons for the voter press to poll.

Punch card: The voter uses metallic hole-punch to punch a hole on the blank ballot. It counts votes automatically, but if the voter's perforation is incomplete, the result is determined wrongfully.

Optical voting machine: After each voter fills a circle for selected candidate on the blank ballot, Optical voting machine selects the darkest mark on each ballot for the vote then computes the total result. This machine counts up ballots rapidly. However, if the voter fills over the circle, it will lead to the error result of optical-scan.

Effectiveness of E-Voting Among Different Countries

Recent years, a considerable number of countries has adopted E-voting for their official elections as follows:

Government of the United States holds election collaterally in several ways; each state can choose the suitable way to hold elections independently. Because there are some issues concerning E-Voting, such as uncounted vote casts, or election system crashed during the Election Day. Secretary of State Kevin Shelley established an "Ad Hoc Touch Screen Task Force" to research the debates on DRE in February 2003 .Shelly advanced that DRE should include voter verifiable paper audit trails (VVPAT) to solve electoral debates ***(****Ying Lai, J., 2008)*

Japan: adopted E-Voting for local election in 2002 in Okayama; mayor election of Hiroshima city in February 02, 2003; and mayor election of Kyoto city in February 08, 2004. Considering election of Niimi city for example, electoral centered surveyed the voters' reliability when the election finished. 83% of voters considered that E-voting system is trusted. 56% of them considered that the results of E-voting and paper-based voting are the same therefore E-voting is sufficient for reliable. The reasons why voters can't trust the E-voting system are voters worried about the abuses in E-voting system, and they cannot make sure their ballot are recorded correctly.

Belgium: Election for the Federal Parliament is held in May 18, 2003. Electoral center held short-term training to assist voters to be familiar with E-voting system which improved the counting efficiency in the election process.

Brazil: used E-voting in 1998. When the voter reaches the polling place, he/she shows his/her identity card for authenticating; if he/she is an eligible voter, he/she can get the ballot for E-voting. Brazil's E-voting system transmits votes to electoral center immediately, so that the count of votes can announce rapidly while the voting finished. ***(****Ying Lai, J., 2008)*

Elements of an E-Voting System

E-Voting system can be divided into three main categories; Hardware, Software, and Human Resources that will be described as follows:

Hardware: security has to be implemented on mechanical, electromechanical, and electrical hardware parts

Software: all software components such as operating system, drivers, compilers, programs, databases, rules used in the program, procedures and sequences (order of voting events, voting protocol, encryption techniques) should be secured.

Human factor: this factor comprises usability, rules, strategies (e.g. information flow, security management), politics, and other diverse aspects such as transparency, acceptance, and trust. *(Ondrisek, B., 2009)*

E-Voting Issues

Hardware / Software Reliability

There are concerns that mechanical failures as for an example in touch-screen machines arising from electrical outages and other causes may leave votes uncounted or miscounted, with no means of recovery or Hardware clocks set wrong. As for software deficiencies in some electronic voting systems may affect election outcomes such as poorly designed , developed using inferior software engineering processes, designed without (or with very limited) external audit capabilities, intended for operation without obvious protective measures, Deployed without rigorous, and scientifically-designed testing and Insufficient audit data unable to collect data from some voting machines.

Vulnerability to Hacking

Criminals could hack an electronic voting machine and steal votes using a malicious programming approach. If DRE programming can be manipulated, that same logic dictates that the programming could be surreptitiously altered to change election results after the paper ballot is printed.

Voter Verified Paper Audit Trails

Adding another federal requirement for DRE voting systems to be retrofitted with a VVPAT component issue some problems that could, unintentionally, shatter the system and significantly erode public confidence in the process also needs to take in considerations significant costs, paper jams and malfunctioning printers, voter delays, difficulty for poll workers, and meaningless receipts.

Accuracy in Capturing Voters' Intent

The possibility of an over voting (or making more selections than permissible) or under voting (when a voter makes fewer than the maximum number of permissible selections in a contest) also touch screen machines can misinterpret a voter's intent. For example, a voter might touch the part of the screen identified with his/her preferred candidate Jones, but candidate Smith's box would light up instead."

Security Issues

Security can be external issues due to voters and attackers and internal issues such as system developing and administrating even just inheritance of some objects in the source code are unsuitable can cause the voting system crash. As a suggested solution applying trusted platform is recommended for insuring security and gaining peoples trust. The term "trusted computing" refers to applications that leverage hardware-based at the edge of the network and at the endpoints for higher assurance.

Trusted Platform Module (TPM)

The Trusted Platform Module can be implemented as a stand-alone or integrated component that enables trust in computing platforms.“*The acceptance of the TPM specification by ISO/IEC confirms the position of the Trusted Computing Group as the premier industry group for trusted computing and attests to the growing usage of the specification to secure data, systems and networks*,” according to Scott Rotondo, president, Trusted Computing Group.” *(TCG, 2009)*

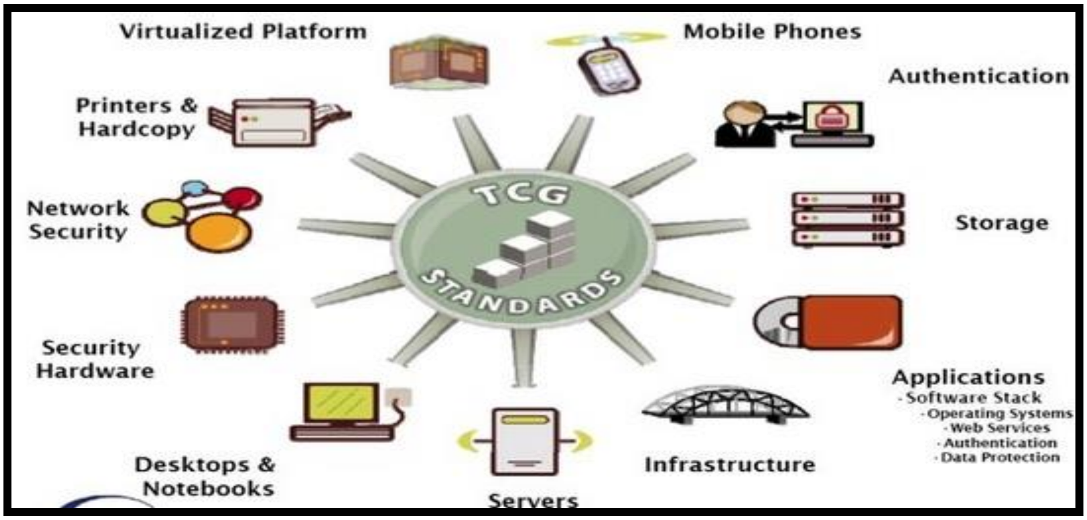


Figure (2.2) Trusted Platform Module, (TCG, 2009)

According to TCG that TPM specification has been ISO standard accepted which reveals that deployment applications based on trusted computing infrastructure exhibit superior capabilities in security governance, risk management and compliance compared to other respondents. TPM is a microcontroller that can be installed on any computing device and can store keys, passwords and digital certificates. It is affixed to the motherboard of a device. The chip also includes a random number generator and the ability to perform certain cryptographic operations, such as the generation of new keys.

TPM ensures that the information stored is more secure from external software attack and physical theft, security processes such as digital signature and key exchange, are protected through the secure TCG subsystem. Access to data and secrets in a platform could be denied if the boot sequence is not as expected. TPM can be integrated into other components in a system. TPM provides a group of crypto capabilities that allow certain crypto functions to be executed within the TPM hardware which can only provide input and output to it. TPM uses RSA built–in engine during digital signing and key wrapping operations.

TPM uses its built-in hash engine to compute hash values of small amount of data. Large amount of data are hashed outside of the TPM, as the TPM hardware may be too slow in performance for such purposes. Random Number Generator that is used to generate keys for various purposes. *(TCG, 2009)*

TPM can use cryptographic means to accurately report its state anytime, which can then be verified to determine the platform's integrity. TPMs include a tamper-resistant microprocessor chip that measures the state of the machine, maintaining a log of all software that has run on the machine since the machine was turned on. TPM use cryptographically to sign the log and bind data to this log, so that a third party can have assurance that the machine only ran trusted software from the time it booted up until the time the measurement was taken. TPM forms the basis of a trusted computing platform by protecting against virtual and physical attacks.

By running on a TPM, each device in an electronic voting system operates in a verified environment, every device can attest to its state as for communicating devices can perform mutual attestation to verify to each other that both devices are in a valid state before communicating. Using TPM approach, a trusted electronic voting system can accurately capture, count, and report the votes. *(TCG, 2009)*

Threats	**Current Solutions**	**Weaknesses**	**TPM Solutions**
Data Theft	Data encryption (EFS, VPN, encrypted email, etc.)	Encryption keys are stored on the hard disk and are susceptible to tampering	Protected storage of keys through hardware
Unauthorized access to platform	Username /Password Biometrics and external tokens for user authentication	Subject to dictionary attacks Biometrics can be spoofed Authentication credentials not bound to platform	Protection of authentication credentials by binding them to platform
Unauthorized Access to network	Windows network logon, IEEE 802.1x	Can be bypassed Certificate can be spoofed Authentication data is stored on the hard disk and is susceptible to tampering	PKI based method for Platform authentication Hardware protection of authentication data[3]

Table (2.2) Security Issues (Bajikar, S. 2002)

Manipulation and Fraud

According to (Computerworld - WASHINGTON, 2004) security researchers said that without voter - verifiable paper receipts, the 50 million Americans who will use electronic voting machines are uncertain that their votes will be recorded properly. Also the large and complexity of code base powering the systems allows manipulation of election results. "My biggest concern is that in a very large trusted computing base, the threat of somebody with access to the development environment of the code base, particularly the vendor, basically is in position to make the outcome of the election come out how they would like, and it's virtually undetectable," said Avi Rubin, a professor at the Johns Hopkins University Information Security Institute. "

Potential vendors influencing the elections, especially since some have taken active roles in operating polling stations and, in the case of Diebold Election Systems' CEO Walden O'Dell, stated publicly the intent to deliver election results to President George W. Bush. (*Verton, Dan, 2004)* Uunauthorized privilege escalation, incorrect use of cryptography, vulnerabilities to network threats, and poor software development processes, voters can cast unlimited votes without being detected by any mechanisms within the voting terminal software. *(STUBBLEFIELD, A., 2004)*

E-Voting Recounting Issue

Electronic voting offers myriad benefits—from multilingual operation to the prevention of over voting—but to be trustworthy, a voting system must satisfy three main goals

- Ensure the election’s integrity,
- Allow results Auditing
- Can be understandable and Trustable for both voters and politicians

Increasing E-Voting Turnout

For increasing number of voter's participation the Author recommends including, Young people, old people, people living abroad and blind / partially- sighted persons

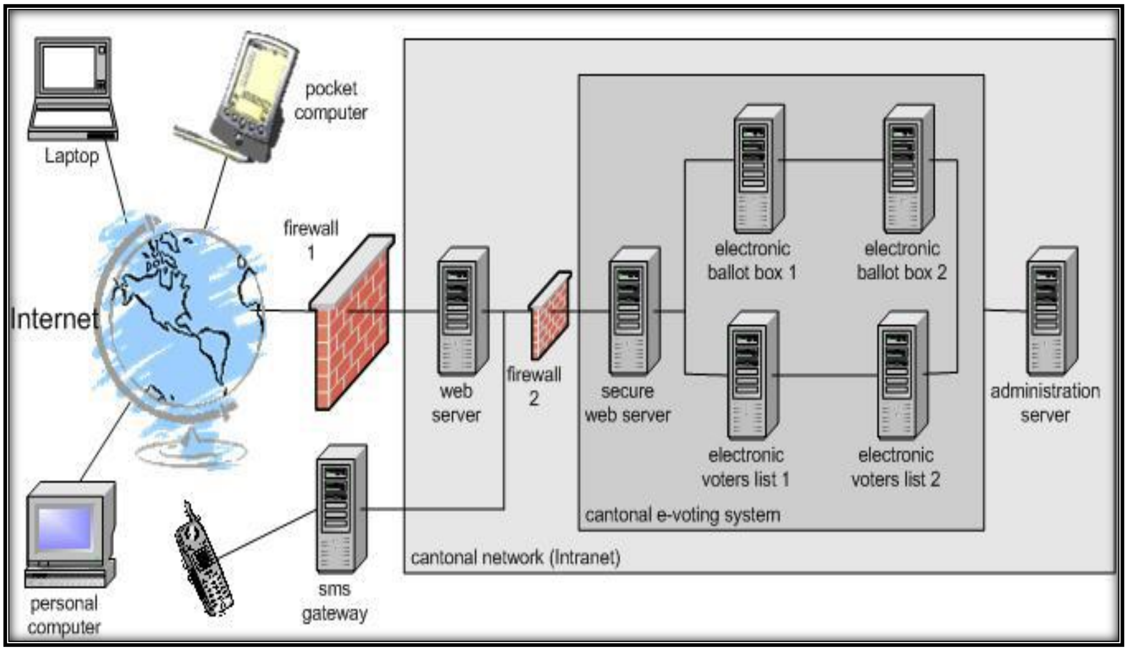


Figure (2.3) Risks / Security (Braun, N., Bundeskanzlei, BK, 2006)

As provided in figure risks such as interception, modification or loss of e-votes in the E-Voting process can be prevented by implementing several security layers encryption of each transaction as follows:

- Voter is prompted to check the "digital finger print" of the server certificate
- System is redundant and protected by firewalls
- Personal access and identification codes is altered for every Election Day
- Frequent refresh of the domain name server during voting period
- Special control devices and protocol filters for protection
- Operators are alarmed and an emergency procedure is launched if any unexpected event happened.
- If the system stopped working the received e-ballots will be saved and the public will be informed to cast votes at polling stations (the voter gets a notice, that his vote has been cast but he/she must not be given a proof of its content else vote buying could take place.

Literature Review

According to *(Cetinkaya and D. Cetinkaya, 2007)* { " There are some studies performed on requirement analysis of E-Voting protocols McGaley and Gibson, define basic requirements for any voting system and they examine them bought by the Irish Government to see whether it can meet those requirements, As for Schryen presents a structural security framework for E-Voting systems. Heindl deals with the legal requirements for E-Voting in Austria. Mitrou et al. addresses the democracy oriented legal and constitutional requirements for any E-Voting system. Cetinkaya [4] provides a comprehensive set of voting requirements. Delaune et al. formalize some of the requirements in applied pi calculus and show the strong relationship between privacy, receipt-freeness and uncoercibility**"**}.

Security Requirements for Cryptographic Voting Protocols

A brief explanation of the security requirements as mentioned in the E-Voting definition as follows:

Elaborate Checklists for E-Voting Security Requirements

Evaluation of the E-Voting systems by explaining the specific cases of the security requirements for each requirement checklist items are given below and they should be satisfied by cryptographic voting protocols *(Cetinkaya and D. Cetinkaya, 2007)*

Voter Privacy

Voter privacy must be preserved during and after the election in order to assure privacy implementation of both **Unlink ability** (No person should be able to deduce any relationship between registration identity, the voter's public key and the voter's casting vote) and **Intractability** (No person should be able to trace the IP address or be able to deduce any relationship between the voter and his vote*)*.

Eligibility

Only eligible voters can cast votes after registration.

Uniqueness

Only one vote per voter should be counted.

Fairness

No partial tally is revealed before the end of the voting period to ensure that all candidates are given a fair decision even for the counting authority should not be able to have any clue about the results.

Uncoercibility

Any coercer (To force someone to act or think in a certain way by use of pressure, threats, or intimidation against his/her wishes), including the authorities, should not be able to extract the value of the vote and should not be able to coerce a voter to cast his vote in a particular way. Any voter must be able to vote freely.

Receipt-freeness

It indicates that the system does not provide a confirmation of the receipt of the vote which may yield its content both during and after the election ends. This is to prevent vote buying or selling.

Accuracy

The published tally should be correctly computed from correctly cast votes

Accuracy can be analyzed in two ways:

- All valid votes should be **counted** correctly, i.e. any cast vote cannot be altered, deleted, invalidated or copied and any falsification on the votes should be detected.

- All counted votes should be **valid and correct**, i.e. eligibility and uniqueness should be satisfied. No participants, voters or authorities can disrupt or influence the election and final tally by adding false votes and nobody should be able to vote in the place of others, even if they are eligible voters but they do not or cannot vote for some reasons or they abandoned the have voting process in any stage. (*Cetinkaya and D. Cetinkaya, 2007)*

Individual Verifiability

Indicates that each eligible voter can verify that his vote is counted correctly by using published data, voter can validate that the ballot and authorities response are correct also Voter can safely re-request data during the voting process if authority response timeouts.

Towards a Successful E-Voting System

The basic issue in E-Voting System is Security and building people Trust to gain the success of E-Voting processes the principal axes of the approach are as follows: *(Manolopoulos, M., 2008)*

Proven technological excellence for the component of the system

The system should use strong technological tools and computer science primitives, preferably scientifically proven and standard-based to ensure the sound operation of the system and its robustness against potential attacks by implementing trustable security technologies such as TPM.

Usage of open source technologies and publicly available information

System development and operation should be based on open source technologies to allow independence from existing vendors and increase transparency.

Involve Infield Voters Assessment

After the end of the voting process, voters should be motivated to assess the system and the whole procedure, Voters feedback should be taken seriously into account for improving the E-Voting system and the organization of the voting procedure.

Organize pre- and post- application information campaigns

Organizing an Information campaign before an e-Voting event improves Stakeholders' understanding of the usage of E-Voting system's capabilities and operation, while information gathered days after the E-Voting event helps them understand each other's views and propose improvements on the operation and usability of the system to reach an E-Voting System that will contribute to its improvements in order to face more demanding e-Voting procedures. In this way, E-Voting will be gradually established and trusted by citizens and the involved stakeholders.

E-Voting Suggested Framework

1. Effective voter registration: E-Voting permission is granted to good faith people and systems.
2. Effective voter authenticity: E-Voting services are only available to those eligible to vote.
3. Effective voter anonymity: Identity of the voter cannot be established with the exception of the ability to warrant under law votes cast.
4. Effective vote confidentiality: E-Voting must guarantee the confidentiality of the vote until it is counted.
5. Effective system identification and authentication: Accountable E-Voting service processes are only accessible to authorized people and systems to access such processes.
6. Effective system access control: Access granted to E-Voting application and assets is the minimum necessary for the identified user to obtain services required.
7. Information integrity: Ensuring that the voter's vote is received and counted as intended.
8. Service availability: Ensuring access to the E-Voting service as and when required.
9. Information availability: Ensuring continued access to E-Voting data assets as and when required.
10. Service protection: Ensuring protection of E-Voting service implementation and associated assets from external interference and penetration.
11. Operator integrity: The employees who are administrating the E-Voting service should be of an unquestionable record of behavior.
12. Open auditing and accounting: The E-Voting service must keep a proper record of significant transactions and the integrity of audit information must be assured.
13. Third party system authentication: Third party systems, used by any E-Voting service, must demonstrate to the voter that they are authorized E-Voting agents.
14. Public verifiability: The E-Voting service must be publicly verifiable. *(Xenakis, A., Macintosh, A ,2004)*

E-Voting Future

Enfranchising Voters through new E-Voting channels

According to *(Scytl, 2009)* the Organization of American States and the Council of Europe**,** have established standards and guidelines on how to implement the internet voting in a secure and reliable manner to improve current E-Voting systems. Scytl collaborated with the Council of Europe in the security and audit standards set in September 2004.

Remote E-Voting (Internet Voting)

Internet voting is regarded by many governments as evolution of electoral processes because of its potential to increase voter turnout rates, facilitate the voting process and enfranchise voters such as overseas voters, military voters and voters with disabilities. Internet voting offers many advantages , including mobility and convenience for voters, greater speed and accuracy in the counting process, prevention of involuntary voting errors, better accessibility, lower costs, support of multiple languages and greater flexibility. Scytl's Internet voting solutions are based on the core security technology, Pnyx.core, ensuring the integrity, privacy and transparency of the election as follows:

Pnyx.Government

Pnyx.Government is an Internet voting platform for the public sector allowing all types of electoral processes (e.g., elections, consultations, surveys, referendums, etc.) to the organization through the Internet and other channels like mobile phones. (Scytl, 2009)

Secure & Cost-Effective Poll-Site E-Voting Technology

It consists of a comprehensive and modular platform that allows governments to introduce E-Voting in their electoral processes in a secure, reliable and cost-effective manner

Pnyx.DRE

Pnyx.DRE is an innovative poll-site E-Voting solution that turns a standard PC into a secure, accessible and reliable DRE E-Voting terminal. It can be used to carry out all types of electoral processes in a secure and convenient manner with the highest usability and accessibility standards. (Scytl, 2009)

Pnyx.VM

Pnyx.VM provides audit ability and redundancy to DREs through a secure and independent verification module, enabling voters to verify their votes before they are cast and recorded. (Scytl, 2009)

Pnyx.VVPAT

It is Voter-Verified Paper Audit Trail solution which cryptographically protects both the printed paper ballots and the corresponding digital votes

Prime III

Prime III It is an electronic secure, open-source, multimodal electronic voting system that delivers the necessary system security, integrity and user satisfaction safeguards in a user friendly interface that accommodates all people regardless of ability.*(United States Election Assistance Commission, 2009)*

Recommendations

To protect the accuracy and impartiality of the E-Voting process, author makes the following recommendations: All voting systems particularly computer-based E-Voting systems must embody careful engineering, strong safeguards, and rigorous testing in both their design and operation. Voting systems should inspection of a physical record to verify voters vote has been accurately cast and to serve as an independent check on the result produced and stored by the system. Making those records permanent (i.e., not only based in device memory) provides a means by which an accurate recount may be conducted. E-Voting system can include Biometric voter verification for ensuring the reliability, security, and verifiability of public elections.

E-Voting system must ensure the reliability, security, and verifiability of public elections is fundamental to a stable democracy Convenience and speed of vote counting are no substitute for accuracy of results and trust in the process by the electorate. It must have Validation and Verification processes to assure the security and reliability of the E-Voting protocols and systems. E-Voting system must be accessible to people who speak different languages, have a wide range of handicaps, or may be serving overseas.

Conclusion

Traditional voting systems should be computerized to reduce the vote counting time, to insure that vote is being correctly accounted, to reduce fraud, to remove errors in filling out ballots, and improve system usability for people with special needs.

This approach raises several security issues, given that democratic principles depend on the electoral process's integrity. Beyond the traditional security properties (integrity, confidentiality, and availability), other properties need to be ensured. Some e-voting system requirements seem contradictory, like ensuring voter authenticity and vote anonymity, providing a vote-counting proof while preventing vote trade, allowing voting via the Internet but avoiding voter coercion, guaranteeing the uniqueness of the vote in decentralized voting, allowing vote automation while providing vote materialization, and ensuring audit ability in a software or hardware environment that could malfunction by implementing TPM as a security solution voters trust are gained which improves the voting process. A widely available, inexpensive and easily used component on most devices. TPM is used to check PCs at start-up for any changes to the software used to run the computer and helps detect any suspicious code before the PC is booted and connected to the network. TPM stores keys, certificates and passwords securely and enables authentication and attestation, critical to trusted computing for E-Voting process.

References

Anup Ghosh, 2008, Guest Editor Introduction, [online] Available on http://www.computer.org/portal/web/computingnow/archive/july2008
[Accessed on 12th December 2009]

Bajikar, S. 2002, Mobile Platforms Group Intel Corporation, *Trusted Platform Module (TPM) based Security on Notebook PCs - White Paper* [online] Available on http://www.intel.com/design/mobile/platform/downloads/Trusted_Platform_Module_White_Paper.pdf [Accessed 14th December 2009]

Braun, N., Bundeskanzlei, BK, 2006, Electronic Voting 2006 Conference Bregenz, *Swiss E-Voting Pilot Projects | Evaluation, Situation Analysis and How to Proceed* [online] Available on http://www.evoting.cc/static/evoting/files/Swiss_Experiences.pdf
[Accessed on 12th December 2009]

Cetinkaya, Orhan., 2008 , *Analysis of Security Requirements for Cryptographic Voting Protocols (Extended Abstract),* ARES '08: Proceedings of the 2008 Third International Conference on Availability, Reliability and Security - Volume 00, IEEE Computer Society [online] Available on http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4529515&isnumber=4529303
[Accessed on 3th December 2009]

Donald P. Moynihan, 2004, Building Secure Elections: E-Voting, Security, and Systems Theory [online], Available on
http://catedras.fsoc.uba.ar/rusailh/Unidad%204/Moynihan%202004%20Building%20secure%20elections%20y%20e%20voting.pdf [Accessed on 4th December 2009]

EJEG Electronic Journal of E- Government, 2005, Paper1 Issue 1, [online] Available on http://www.ejeg.com/volume-1/volume1-issue-1/issue1-art5.htm
[Accessed 11th December 2009]

Ekberg, N., Zeglen, R., 2009, *Security Challenges of Electronic Voting Systems* NYSTEC, [online] Available on
http://www.cscic.state.ny.us/security/conferences/security/2009/documents/Challenges-of-Electronic-Voting-Systems.pdf [Accessed on 7th December 2009]

LORI STEELE, 2009, *The Future Of E-Voting Online Election Vendor Discusses The Spread Of Internet Voting Technology Across The World And It's Future In The U.S.* National journal [online] Available on http://www.nationaljournal.com/njonline/no_20090109_6718.php
[Accessed on 4th December 2009]

Laurence Monnoyer-Smith, 2005, *how e-voting technology challenges traditional concepts of citizenship: an analysis of French voting rituals* [online] Available on
http://www.evoting.cc/static/evoting/files/monnoyersmith_challenge_citizenship_61-68.pdf
[Accessed on 4th December 2009]

Manolopoulos ,M., Nakou , P., Panagiotaki , A., Sofotassios , D, .Stamatiou , Y., Spirakis P., 2008 ,ACM International Conference Proceeding Series; Vol. 351, Proceedings of the 2nd International Conference on Theory and Practice of Electronic Governance *A Step-Wise Refinement Approach for Enhancing e-Voting Acceptance* [online] Available on http://portal.acm.org/citation.cfm?id=1509096.1509153 [Accessed 13th December 2009]

Nathanael Paul and Andrew S. Tanenbaum, 2009, Trustworthy Voting: From Machine to System, IEEE Computer Society, [online], Available on http://www.computer.org/portal/cms_docs_computer/computer/homepage/May09/r5pra.pdf [Accessed 25th November 2009]

Ondrisek, B., 2009, Proceedings of the 42nd Hawaii International Conference on System Sciences - 2009, *E-Voting System Security Optimization* [online] Available on http://electrobabe.files.wordpress.com/2009/01/ondrisek_e-voting-system-security-optimization_05-02-02.pdf [Accessed on 13th December 2009]

Price, A, 2009, *TRUSTED COMPUTING GROUP TRUSTED PLATFORM MODULE SPECIFICATION GETS ISO STANDARDIZATION*, [online] , Available http://www.trustedcomputinggroup.org/files/resource_files/E1999F71-1D09-3519-AD5DA10D3647ED32/TPM%20ISO%20aug%203%2009%20finalpdf.pdf [Accessed on 14th December 2009]

Prosser, A. & Krimmer, R., 2004, *The Dimensions of Electronic Voting Technology, Law, Politics and Society*, [online] Available on http://subs.emis.de/LNI/Proceedings/Proceedings47/Proceeding.GI.47-3.pdf, [Accessed 12th December 2009]

ProCon.org, 2009, Voting Machines, *Historical Timeline Electronic Voting Machines and Related Voting Technology*, [online] Available on http://votingmachines.procon.org/viewresource.asp?resourceID=273#1975 [Accessed on 12th December 2009]

Security Focus, 2009, *U.S. issues revised e-voting standards*, [online], Available on http://www.securityfocus.com/brief/968 [Accessed on 13th December 2009]

STUBBLEFIELD, ADAM, 2004, Analysis *of an Electronic Voting System***,** *IEEE Symposium on Security and Privacy 2004* [online], Available on http://avirubin.com/vote.pdf [Accessed 4th November 2009].

Storage Newsletter, 2009, *TCG Starts Trusted Platform Module Certification*, [online] Available on http://www.storagenewsletter.com/news/security/tcg-starts-trusted-platform-module-certification [Accessed 13th December 2009]

Trusted Computing Group, 2009 [online] Available on http://www.trustedcomputinggroup.org/ [Accessed 14th December 2009]

United States Election Assistance Commission, 2009, *Current and Future Trends in Election Technology* [online] Available on http://www2.sbe.virginia.gov/GRDocs/Training/2009%20Annual%20Training/070109%20The%20Future%20of%20Voting%20Equipment%20Brian%20Hancock.ppt
[Accessed on 14th December 2009]

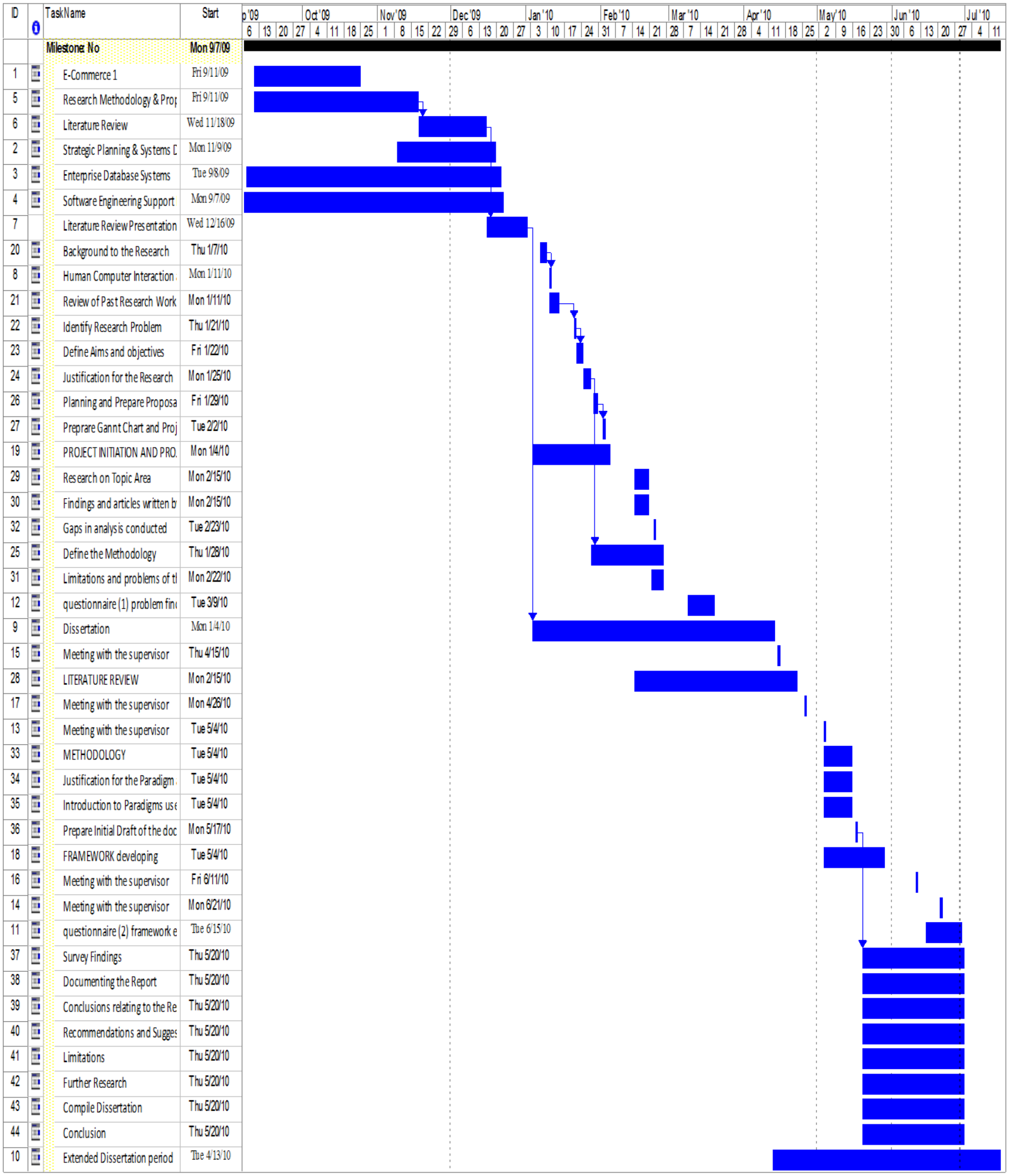
Verton, Dan 2004, *Computer World Government*, *E-voting system security, integrity under fire* [online] Available on http://www.computerworld.com/s/article/92950/E_voting_system_security_integrity_under_fire?taxonomyId=70&pageNumber=2 [Accessed 4th December 2009]

Washington, DC: U.S. Government Printing Office U.S. Office of Management and Budge t (OMB). 2001. *The President's Management Agenda*. Washington, DC: U.S. Government Printing Office [online] Available on http://catedras.fsoc.uba.ar/rusailh/Unidad%204/Moynihan%202004%20Building%20secure%20elections%20y%20e%20voting.pdf [Accessed on 4th December 2009]

Xenakis, A., Macintosh, A, 2004, Procedural *Security Analysis of Electronic Voting* [online] Available on http://svn.assembla.com/svn/network_security/Papers/p541-xenakis.pdf
[Accessed on 12th December 2009]

Ying Lai, J. et al., *Design and Implementation of an Electronic Voting System with Contactless IC Cards* [online] Available on http://59.127.136.65/publications/200805ICIM_eVoting.pdf
[Accessed 13th December 2009]

Appendix (3) Gantt chart



ID	Task Name	Start
	Milestone: No	Mon 9/7/09
1	E-Commerce 1	Fri 9/11/09
5	Research Methodology & Prop	Fri 9/11/09
6	Literature Review	Wed 11/18/09
2	Strategic Planning & Systems D	Mon 11/9/09
3	Enterprise Database Systems	Tue 9/8/09
4	Software Engineering Support	Mon 9/7/09
7	Literature Review Presentation	Wed 12/16/09
20	Background to the Research	Thu 1/7/10
8	Human Computer Interaction	Mon 1/11/10
21	Review of Past Research Work	Mon 1/11/10
22	Identify Research Problem	Thu 1/21/10
23	Define Aims and objectives	Fri 1/22/10
24	Justification for the Research	Mon 1/25/10
26	Planning and Prepare Proposa	Fri 1/29/10
27	Preprare Gannt Chart and Proj	Tue 2/2/10
19	PROJECT INITIATION AND PRO.	Mon 1/4/10
29	Research on Topic Area	Mon 2/15/10
30	Findings and articles written b	Mon 2/15/10
32	Gaps in analysis conducted	Tue 2/23/10
25	Define the Methodology	Thu 1/28/10
31	Limitations and problems of tl	Mon 2/22/10
12	questionnaire (1) problem fin	Tue 3/9/10
9	Dissertation	Mon 1/4/10
15	Meeting with the supervisor	Thu 4/15/10
28	LITERATURE REVIEW	Mon 2/15/10
17	Meeting with the supervisor	Mon 4/26/10
13	Meeting with the supervisor	Tue 5/4/10
33	METHODOLOGY	Tue 5/4/10
34	Justification for the Paradigm	Tue 5/4/10
35	Introduction to Paradigms use	Tue 5/4/10
36	Prepare Initial Draft of the doc	Mon 5/17/10
18	FRAMEWORK developing	Tue 5/4/10
16	Meeting with the supervisor	Fri 6/11/10
14	Meeting with the supervisor	Mon 6/21/10
11	questionnaire (2) framework e	Tue 6/15/10
37	Survey Findings	Thu 5/20/10
38	Documenting the Report	Thu 5/20/10
39	Conclusions relating to the Re	Thu 5/20/10
40	Recommendations and Sugges	Thu 5/20/10
41	Limitations	Thu 5/20/10
42	Further Research	Thu 5/20/10
43	Compile Dissertation	Thu 5/20/10
44	Conclusion	Thu 5/20/10
10	Extended Dissertation period	Tue 4/13/10