ADDRESSING VERIFIABILITY PROBLEM OF ELECTRONIC VOTING SYSTEM

OLADAYO SUNDAY OLALEKAN

MASTERS OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

AL-MADINAH INTERNATIONAL UNIVERSITY

MALAYSIA

APRIL 2014/ 1435H

ADDRESSING VERIFIABILITY PROBLEM OF ELECTRONIC VOTING SYSTEM

By

OLADAYO SUNDAY OLALEKAN

(MIT131AT387)

THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTERS OF SCIENCE

In the

DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

FACULTY OF COMPUTER AND INFORMATION TECHNOLOGY

AL-MADINAH INTERNATIONAL UNIVERSITY

MALAYSIA

APRIL 2014

صفحة التحكيم

CERTIFICATION OF DISSERTATION WORK PAGE

أقر بحث الطالب _____ بعنوان _____ من قِبل الآتية أسماؤهم:

The thesis of student named: ***Oladayo Sunday Olalekan*** *Under title* ***Addressing the verifiability problem of electronic voting system****. has been approved by the following:*

Academic Supervisor **المشرف على الرسالة**

Asst. Prof. Dr. Najeeb Abbas Al-Sammarra	***Name/*** **الاسم**
……..	***Signature/*** **التوقيع**

Supervisor of correction **المشرف على التصحيح**

……...	***Name/*** **الاسم**
……...	***Signature/*** **التوقيع**

Head of Department **رئيس القسم**

Asst. Prof. Dr. Najeeb Abbas Al-Sammarrai	***Name/*** **الاسم**
……	***Signature/*** **التوقيع**

Dean, of the Faculty **عميد الكلية**

……...	***Name/*** **الاسم**
……..	***Signature/*** **التوقيع**

Academic Managements & Graduation Dept **قسم الإدارة العلمية والتخرج**

Deanship of Postgraduate Studies **عمادة الدراسات العليا**

DECLARATION

I hereby declare that, this dissertation is the result of my own investigation, except where otherwise stated.

Name: Oladayo Sunday Olalekan

Signature ……..

Date: ……..

PERMISSION TO USE

In presenting this thesis in fulfillment of the requirements for a postgraduate degree from Al-Madinah International University, I agree that the University Library make it freely available for inspection. I further agree that permission for copying of this dissertation in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor or, in his absence by the Dean of Faculty of Computer and Information Technology or the dean of Postgraduate Studies. It is understood that any copying, publication, or use of this dissertation or parts for financial gain shall be given to me and to Al-Madinah International University for any scholarly use which may be made of any material from my dissertation.

Request for permission to copy, make other use of materials in this thesis, in whole, or in part should be addressed to:

Dean of Faculty of Computer and Information Technology or the dean of Postgraduate Studies,

40100, 11th floor –Plaza Masalam

Section 9, Shah Alam

Malaysia

ABSTRACT

Internet voting could represent an effective way to improve accessibility to voting platform during election and increases turnout amongst the young people during the exercise. While the internet is sufficiently safe for conducting bank transactions, this is not yet the case for politically binding elections.

Designing a robust system algorithm to solve electronic (internet) voting system verifiability problem is a challenging task in Computer or Information and Communication Technology world.

The integrity of election process is fundamental to the integrity of democracy itself. The election system must be sufficiently robust to curb varieties of fraudulent behaviors and must be sufficiently transparent and comprehensible that voters and candidates can cast and accept the result of election without any violent eruption afterward.

An effective way to gaining voters' confidence in the credibility of election is to ensure that they can verify that their votes were counted as cast especially citizens in Diasporas and others who will cast their votes at the comfort of their remote locations by connecting to the internet.

This work is based on designing a voter verifiability system which uses graphical interface to capture and display updated number of electorates' cast votes. The system will help voters to verifier that their votes are counted as cast. The display will be followed by instant short message service broadcast to all registered voters.

The verifiability system will fulfil all modern voting system requirements which includes guide against security threats, transparency and secrecy. The ability of electorate to verify that his vote was counted during election and that he was not short changed makes him believe in the credibility of the election.

ACKNOWLEDGEMENTS

All the adoration and thanks to Almighty God, the master of universe for giving me life, good health, energy and wisdom to carry out my research work against all physical odds. He is always there to grant me success in all my endeavours. Countless are His bounties on me.

I would, also, like to express my deepest gratitude and appreciation to my main supervisor;

Assistant Professor Najeeb A. Al-Sammarraie, for his invaluable encouragement and guidance. His support and comments have provided me with the adequate direction and courage that made it possible for me to undertake this work.

I am equally grateful to other erudite scholars, Assistant Prof Dr. Abdulsamad Yahyah, Associate Prof Dr. Doukoure Massire, Associate Prof Dr. Mubarak Mohammed and others whose names could not be mentioned on this page of the book for all their kind gesture towards the success of this research work.

Last but not the least, my sincere thanks to my family; my late sweet mother who always gave me courage and strong reason not to admit defeat (may her gentle soul rest in perfect peace), my dearest wife (Moyosoluwa) for her support, Mrs Alice Ooi (my Malaysian adopted mother), and friends who have always shown their faithful support during my study. I appreciate their unwavering patience that has never stopped during the long period of my study.

Finally, I will like to appreciate Mr David Alabi for guide and advice on how to live away from home as a good ambassador.

I am so grateful to you all.

DEDICATION

I dedicate the research work to the Almighty God who has been everything to me and to my beloved late mother who lost her life while sourcing for daily bread in vehicle accident, May her gentle soul rest in perfect peace.

TABLE OF CONTENTS	
CONTENTS	Page

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

E	Electronic
DREVS	Data Record Electronic Voting System
I-V	Internet Voting
GUI	Graphical User Interface
SMS	Short Message Service
ID	Identity
AIDC	Automatic Identification and Data Capture
PHP	php Hypertext preprocessor
SQL	Structure Query Language
HTML	Hyper Text Markup Language
INT	Integer
VARCHAR	Variable Character
DB	Database
SDP	Social Democratic Party
PDP	People Democratic Party
APC	All Progressive Congress
CIS	Computer Information system
IS	Information System
CAI	Common Authentication Infrastructure
DOS	Denial-of-service
DDOS	Distributed denial-of-service
DRE	Direct-recording electronic
E2E	End-to-end
GSM	Global System for Mobile Communication
HMAC	Hash-based Message Authentication Code
HTML	Hypertext Markup Language
HTTPS	Hypertext Transfer Protocol Secure
WWW	World Wide Web
OCR	Optical Character Recognition

PIN	Personal Identification Number
PKI	Public Key Infrastructure
SAML	Security Assertation Markup Language
SHA	Secret Hashing Algorithm
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
ISP	Internet Service Provider
VOI	Vote over Internet

CHAPTER ONE

INTRODUCTION

1.1 Background

Electronic voting (e-voting) is one of the possibilities to vote in addition to other voting methods. I-voting in this context means voting via Internet, not voting by using a special voting device.

In 2012 a separate Electronic Voting Committee was established in Estonia who is now responsible for conducting Internet voting while the National Election Committee retains a supervisory role.

Internet voting was first introduced in the local elections of 2005, when more than Nine thousand voters cast their ballot via the Internet (this corresponded to about two percent of all participating voters). Today, I-voting with binding results has been carried out six times in Estonia: in the local elections in October 2005, the parliamentary elections in March 2007, the European Parliament elections in June 2009, the local elections in October 2009, the parliamentary elections in March 2011 and the local elections in October 2013.

As of 2013, the source code of the I-voting software has been made public on the internet at this universal resource locator [1].

One of the traditional ways to vote is outside the polling district of the voter's residence. This means that during the voting, the voter puts his or her vote into double envelope and the envelope is delivered to the voter's polling division of residence. The general concept of I-voting has been derived from the above-mentioned voting outside the polling district of residence. What is similar in these two voting methods is the way of checking that the vote has been cast only once and guaranteeing the anonymity of vote.

In order to understand the I-voting system better, the envelope voting method used in Estonia is described shortly below:

- A voter presents an ID document to be identified.
- The voter then receives the ballot and two envelopes.
- The voter fills in ballot paper and puts it into the envelope, which has no information about the voter.
- Then he encloses the envelope into outer envelope on which the voter's information is written.
- The envelope is delivered to the voter's polling division of residence. After the eligibility of the voter is determined, the outer envelope is opened and the inner (anonymous) envelope is put into the ballot box.

The system guarantees that the voter's choice shall remain secret and recording the vote in the list of voters in the polling district of residence prevents voting more than once.

I-voting is carried out according to the same scheme. The downloaded I-voting application encrypts the vote. The encrypted vote can be regarded as a vote contained in the inner, anonymous envelope. After that the voter gives a digital signature to confirm his or her choice. By digital signing, the voter's personal data or outer envelope are added to the encrypted vote.

I-voting is possible only during seven days of advance polls - from 10th day until 4th day prior to Election Day. This is necessary in order to ensure there is time to eliminate double votes by the end of the Election Day.

To ensure that the voter is expressing their true will, they are allowed to change their electronic vote by voting again electronically during advance polls or by voting at the polling station during advance polls.

For example, if a voter cancels his/her electronic vote by going to the polling station to vote, it is guaranteed that only one vote is counted per voter. To that end, all polling stations are informed of the I-voters on their list of voters after the end of advance polls and before the Election Day. If it is found at the polling district that the voter has voted both electronically and with a paper ballot, the information is sent to the Electronic Voting Committee and the voter's I-vote is cancelled.

Before the ascertaining of voting results in the evening of the Election Day, the encrypted votes and the digital signatures (i.e. data identifying the voter) are separated. Then anonymous I-votes are opened and counted. The system opens the votes only if they are not connected to personal data.

The field of information system has experienced an explosive growth in the last few decades. It is the rapidly developing branch of Electronic and Computer Engineering. Information system (IS) has many applications in different fields of electronic and computer Engineering. Internet or electronic voting system is one of the numerous applications of the information system. Voters' data capture, data selection and encryption in electronic voting are all made possible with the advent of information technology.

Information system is the study of complementary networks of hardware and software that people and organizations use to collect, filter, process, create and distribute data.

The study bridges business and computer science using theoretical foundations of information and computation to study various business models and related algorithmic process within a computer science discipline. [2].

Silver et al provided two views on information system that includes software, hardware, data, people and procedure. [2].

The advent of computer information system / information system (CIS/IS) has completely changed the phase of business operation. It has made life so easy and reduced operational cost.

This has led to the introduction of electronic mail, electronic commerce, electronic

governance, electronic library, electronic voting and so on (e-mail, e-commerce, e-governance, e-library, and e-voting respectively).

1.2 Motivation

The very fast growth and adoption of electronic voting system has opened door for researchers to bridge loop holes in the system.

Election allows citizens to choose their representatives and express their preferences for how they will be governed for every period of time stipulated by constitution.

Naturally, the integrity of election process is fundamental to the integrity of democracy itself. The election system must be sufficiently robust to withstand varieties of fraudulent behaviors and must be sufficiently transparent and comprehensible that voters and candidates can cast and accept the result of election without any violent eruption afterward.

History made it known that manual system of voting which is still in practice in most parts of the world gives room for manipulation in order to influence the outcome of election.

There have been several studies on using computer technologies to improve election. These studies raise alarm on the challenges associated with electronic voting which include software engineering, insider threat, network vulnerabilities, secrecy, verifiability and the auditing of electronic voting (also known as e-voting) which encompassing several different types of voting, embracing both electronic means of casting a vote and electronic means of counting votes.

Assuring Accuracy, Integrity and Security in National Elections; Electronic or computer (Information and communications technologies) are being used increasingly with significant benefits to the election registration and voting process. However, implementation of these technologies has vulnerabilities and risks, with potential for harming the integrity of the process.[3].

The U.S. Congress is ultimately responsible for setting the rules governing the conduct of Federal elections (i.e., for President, Vice-President, and its own membership) with a near certitude of extension of its applicable decisions to state and local government elections.

In Current Vote-Casting and Counting. Over 55% of American voters now vote with computer-readable and computer-tallied ballots, or cast their votes directly into vote-tallying computers without ballots by using touch-screens or push-buttons. Computer-readable ballots, using either holes or marks as choice-indicators, have been in use since the 1960s. Such ballots may be fed into precinct-located computers, or collected, transported, and fed into centrally located computers for counting and summarization. Non-ballot, direct recording voting systems, which must be precinct-located, has been in significant use only in the past five years. The two essential technical processes, regardless of system type, are vote-casting and vote-tallying. The vote-casting process may be carried out in two steps: first, by the voter filling out a computer-readable ballot and second by the reading of the ballot; or in one step: by the voter directly entering choices into a computer. Vote-casting, from a technical viewpoint, is a machine-sensing of a voter's choice and a conversion of that choice to a machine-processible signal. Vote-tallying is caused to occur by machine logic that is designed into software and hardware.

In Future Vote-Casting and Counting, there may be more use of on-line voting, in which the voter, remotely stationed at a terminal or terminal-like device, is connected by communications to a central computer facility. The central facility would need to have, on-line, the complete registration database for those voters expected to vote by that method. Voting by phone, which fits this model, has been tried in a few communities. Whether voting by phone becomes more widespread remains to be seen; general acceptance will depend on characteristics such as user-friendliness, ability to attract additional voter participation (over current methods), cost-effectiveness, and security. Voting at a personal computer (PC) with a communications connection to a central computer is a similar possibility; a blank ballot would be communicated to the PC from the central computer, the voter would vote on-screen, and the filled-out ballot would be

transmitted back to the central location. The use of fax machines to transmit absentee ballots is a step in the direction of on-line voting. A bill that would enable use of faxed ballots in Federal elections has been introduced in Congress as an amendment to the Uniformed and Overseas Citizens Absentee Voting Act. With a traditional fax system, the ballot would be printed out at the receiving end, but a computer system with a communications interface could be arranged to receive a fax directly without it being printed. However, the faxed ballot would need to be seen by a human (who may also see the sender's name to verify registration) in order to be voted, whether printed or not. The next step towards on-line voting is e-mail, which is a computer-to-computer interchange, but also intended for human interpretation. The final step is electronic data interchange or EDI, which is a computer-to-computer interchange, but in which the ballot is strictly formatted using standard rules. Then, the ballot can be processed by a computer program at the receiving end without human intervention, thus preserving confidentiality at that point.

In Voter Registration and Sign-In. Computerized databases are now widely used to maintain lists of registered voters, but maintenance of accurate lists is not easy, due partly to the high mobility of the American public. The U.S. Postal Service is widely used to help in verifying addresses. Accurate updating of the voter registration database as well as precinct boundary definition can be made easier by automated reference to a computerized map of jurisdiction geography, including listings of all residence identifications and multi-family dwelling designations. Ability of the voter registration database to automatically acquire driver's license and death record information could contribute to assurance of an accurate list. A computer system storing the voter registration database, if it had on-line access capability, could make possible access to the database from terminals at precinct locations on election day, to help in the sign-in (registration verification) process.

Special forms of information technology may be used for personal identification for voter sign-in on Election day, e.g., computer-based signature matching, but for on-line voting systems allowing voting from phones or remote terminals, voter identification

Could require the use of more advanced techniques, such as cryptographic-based digital signatures.

In automated ballot generation. Generation of ballot or screen layouts for vote-counting equipment is an important computer application. In a consolidated election in one of the larger counties, in which Federal, state, and local government offices as well as referenda and other questions may be simultaneously contested, the number of different ballot styles required, due to the presence of incongruent districts, may be quite large. The necessary number of styles may be multiplied by two, three, or more, if ballot rotation (alternating the top position among opponents) is required by law. The use of a computer for ballot generation may reduce the likelihood of an error in the provision of ballot styles to particular precincts. The coordination of the vote-tallying software with the ballot-generation software is a necessity; an error would result in mis-assigned votes.

Vote-Casting. Proper accounting for all computer-readable ballots is an internal control issue, and inaccurate computer reading of the voters' choices is an engineering issue, involving both hardware and software. Among ballot types, the pre-scored punch card (of the "votomatic" type) continues to be selected for use in jurisdictions including about 40% of U.S. voters, yet its capability to very accurately record voter's choices, as well as its capability for reproducing those choices in a recount, is in serious doubt. The problem is the pre-scoring which may, through incorrect punching or rough handling, cause extra Chad to fall out, or cause hanging Chad to be forced back into the ballot card, thereby misstating the voter's choices to the computer. The National Institute of Standards and Technology (NIST) recommended the elimination of pre-scored ballot cards in 1988, but this recommendation carried no mandatory requirement, and very little elimination of pre-scored ballot cards has occurred. NIST's recommendation was not a Federal Information Processing Standard (FIPS), but even if it were, such standards may not be applicable to Federal elections at this time. Whether or not minimum performance requirements, such as accuracy requirements for ballot reading, should be mandatory is a policy issue that needs investigation.

Electronic voting technology speeds up the voting processes which include registration, casting of votes and counting of votes. Using electronic voting technology, voters need not to travel through long distance to get a polling booth and queue up for some time before been called to cast their votes. With electronic voting system, multiple users can vote simultaneously using their computers, GSM phone and pads at their remote comfort zone.

This voting system addresses the age long tradition of election rigging, stolen of ballot boxes and violence among rival parties which always results in to loss of lives and properties. This is always the experience in Nigeria after election. The electoral knowledge Network emphasized that the introduction of information and communications technologies (ICT) into the electoral process is generating both interest and concern among voters, as well as practitioners across the globe. Today, most electoral management bodies (EMBs) around the world use new technologies with the aim of improving the electoral process. These technologies range from the use of basic office automation tools such as word processing and spreadsheets to more sophisticated data processing tools, such as data base management systems, optical scanning and geographic information systems. [4].

Some of these tools have been available for some time and their strengths and weaknesses are well known. Every year, however, new technologies and tools that are not as well known are introduced to the market. As this is being written, for instance, there are several voting systems in use that automate the recording and/or counting of votes cast. Other systems verify voter eligibility and voter authentication. Some countries are also experimenting with Internet voting as a way to facilitate voting and to increase voter participation in elections. All of these efforts aim to ensure the credibility of the democratic process and the reliability of elections results.

While these technologies open up new frontiers and offer new possibilities for the electoral process, especially for voting operations, there may be unforeseen risks involved, such as an increase in vote selling or difficulty in auditing election results. Careful consideration also needs to be given to the risks of inappropriate or untimely introduction of technology, especially if it has the potential to compromise transparency,

local ownership or sustainability of the electoral process.

Among all of the new technologies being introduced, public attention is focused mainly on those that support electronic voting (E-voting). However, the aim of the Elections and Technology topic area is to introduce technologies that have an impact on a variety of activities related to the administration of elections.

In many countries, technology is present in activities related to the electoral process, and in some cases it is essential to the conduct of elections. 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 application of technology to elections can increase administrative efficiency, reduce long-term costs and enhance political transparency.

Technologies used for elections can include familiar and older ones like printing presses, ball point pens, manual typewriters, electronic calculators and radios, or newer technologies like computers, optical scanners, digital mapping and the Internet. The logistics of modern large-scale elections can be a considerable challenge for countries without access to technology.

The complexity level of technology used for the administration of elections around the world varies enormously. The rate of technological change is so high that election management bodies (EMBs) must regularly re-evaluate their use of technology to determine whether they should adopt new or updated technology to improve their performance.

1.2.1 History of electronic voting system

In this section, theory related to existing voting systems and technologies used are presented. This includes technologies for paper-based voting systems where electronic means are used to count the paper ballots, and technologies for electronically casting votes.

Some of the technologies mentioned are older technologies used in less voting systems these days, while some are still in phases of development and testing.

Electronic voting technology can include punched cards, optical scan voting systems and specialized voting kiosks (including self-contained direct-recording electronic voting systems, or DRE) and paper based electronic voting system. It can also involve transmission of ballots and votes via telephones, private computer networks, or the Internet.

1.2.1.1 Punch card system

The use of punch cards for data handling is a technology that has been used since the 19th century. The punch card sorting and tabulation equipment was invented by a statistician named Herman Hollerith. It was first built to process the large amount of information from the 1890 US census, but later developed for commercial and scientific purposes, and also for voting. [5]

The machinery of a punch card system consists of several components to carry out the processes. A punching device as showed in Figure 1.1 punches the information and data on the cards. When having several decks of punched cards a card collator machine can sort and merge cards from different stacks according to certain factors, for instance address. To sort/tabulate the cards with specific loads a sorting/tabulation machine can be used. An example of a tabulation machine is showed in figure 1.2.

The punch cards are stiff cards or paper strips that are punched according to a certain value or designation. There exist a lot of different types of punch cards, of different sizes, with a different amount of punching locations, for different purposes. Punch cards were used as input for data processing in electromechanical devices like tabulation machines and unit record equipments, which was used before the invention of today's electronic computers.

These machines had a function of sensing punched holes with either electrical or optical sensors, and could have high-speed mechanical feeders that made it possible to process up to 2000 cards per minute. [5].

To generate a summary (report) of a deck of punch cards, they could be fed into the tabulation machine and selected fields from each card were added to the value of one or several counters in the machine.

Early computers were using punch cards for program entry and storage.

When using punched cards, the computer could register the presence of a punched hole with "1" and the absence of a hole with "0" and by this save the information in the binary number system. As late as up to 1970, the punch card was the most popular storage medium used, but is now an almost obsolete technology. Figure 1.3 shows an example of a punch card from a Fortran program. The punch card is no longer used for programming purposes, but has been used in voting systems in some states in the US recently. Advantage of punch card system used for the 1890 census, except for the efficiency, was the ability for verification. The card with its printed image was kept by a board and enabled all the cards to be read back for recounting or for verification by others. Verification and paper-audit trail are also issues that arise in the discussion about electronic voting scenarios.

1.2.1.2 Punch cards for voting

Electronic voting systems based on punch cards have been used since 1964 for voting purposes [4]. The punch cards were used to record the vote and they were run through a tabulation machine to count the votes. When using punch cards as ballots for voting purposes the perforations represents the polling choice made by the voter. The voters punch holes in the cards (with a supplied punch device) opposite their candidate or ballot issue choice and place it in a ballot box. To generate a result, the punch cards can be fed into a tabulation machines at the precinct, or all punch cards can be gathered and transported to a central location for tabulation.

There are two common types of punch cards used for voting purposes; the

"Votomatic" card and the "datavote" card. The "votomatic" card is a direct descendant of the original punch cards and only has numbers indicating the holes to be punched. The ballot issue choices or list of candidates are printed on a separate booklet, and you punch the card according to which number that corresponds to your choice of candidate. On the "datavote" card, the names of the candidates are printed on the ballot next to the punch

hole. The use of punch cards systems for voting purposes has both advantages and concerns. When using punch cards and a sorting machine there is easy to detect misplaced cards, to prevent errors in the counting process. Another advantage is that there exists an audit trail of punch cards making it possible to perform a recount if necessary. One of the concerns associated with the use of punch cards is related to the material of the card. When using punch cards for tabulation, errors related to the holes on the card can occur. When punch cards were used for elections in the US the voters cast their vote by using a pin to punch through the card by hand. This leftover paper that was punched out is referred to as the "Chad". If the holes are not aligned or fully punched, called the "hanging Chad", the ballot can be counted incorrectly when tabulated. Many jurisdictions switched from punch card systems to more advanced systems like marksense or DRE systems, when these could be deployed. In the
County of Los Angeles, the largest election jurisdiction in the US with 3.8 million registered voters; they continued to rely on their punch card voting system in the late 1990s and 2000. For the 1996 US Presidential election, a variation of a punch card system was used by 37.3% of registered voters in the United States (US Federal Election Commission). In the 2000 US presidential election, the votomatic punched card systems got a considerable bad reputation. In three of Florida's counties, after counting and recounting, it was claimed the punch card system's uneven use had even affected the outcome of the election [6]. With this, the US presidential election of 2000 brought the punch card systems into infamy and the US was criticised of using such an old-fashion technology.

Figure 1.1 A punching device to punch holes in a punch card.

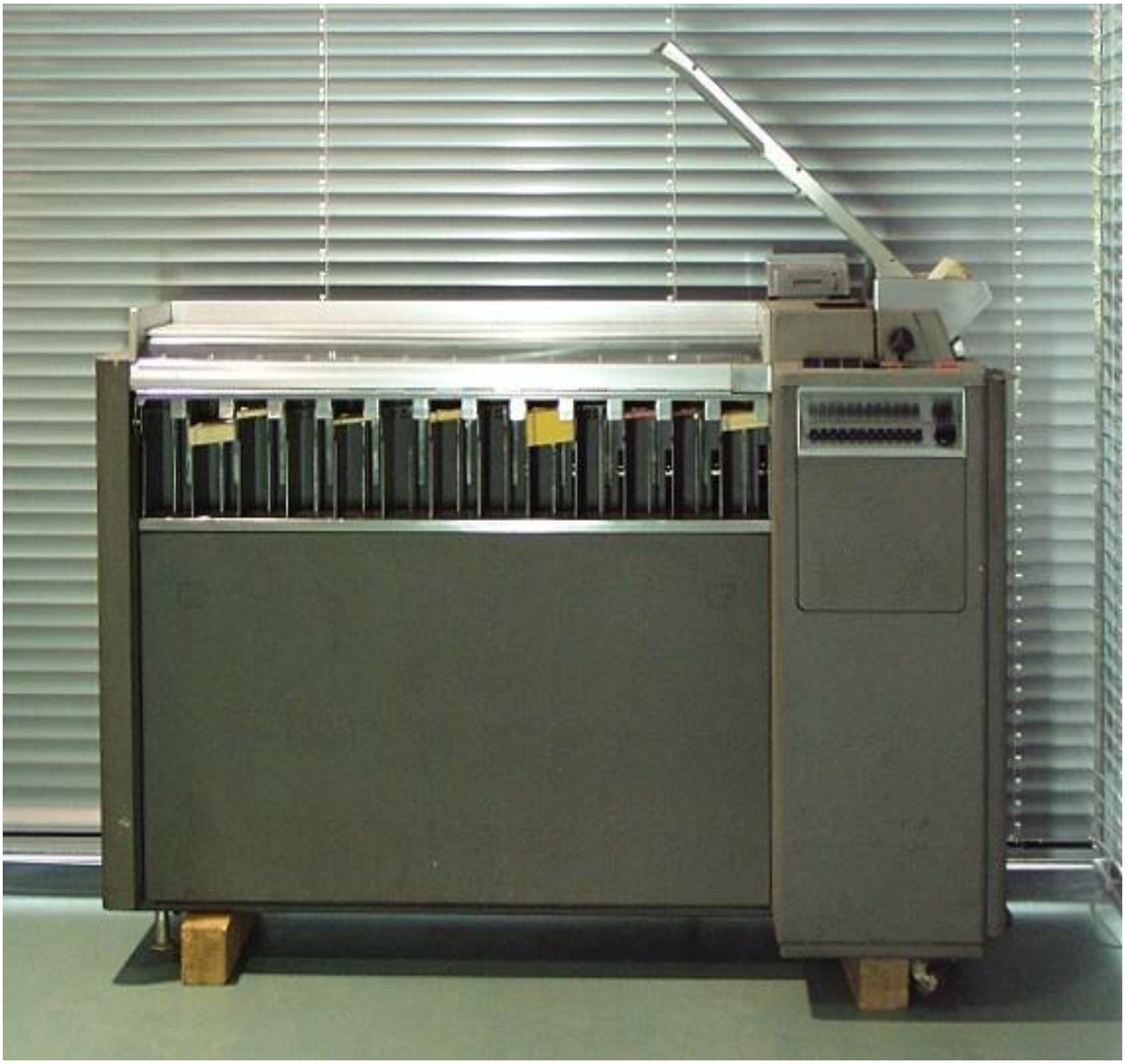


Figure 1.2: A sorting machine for punch cards.

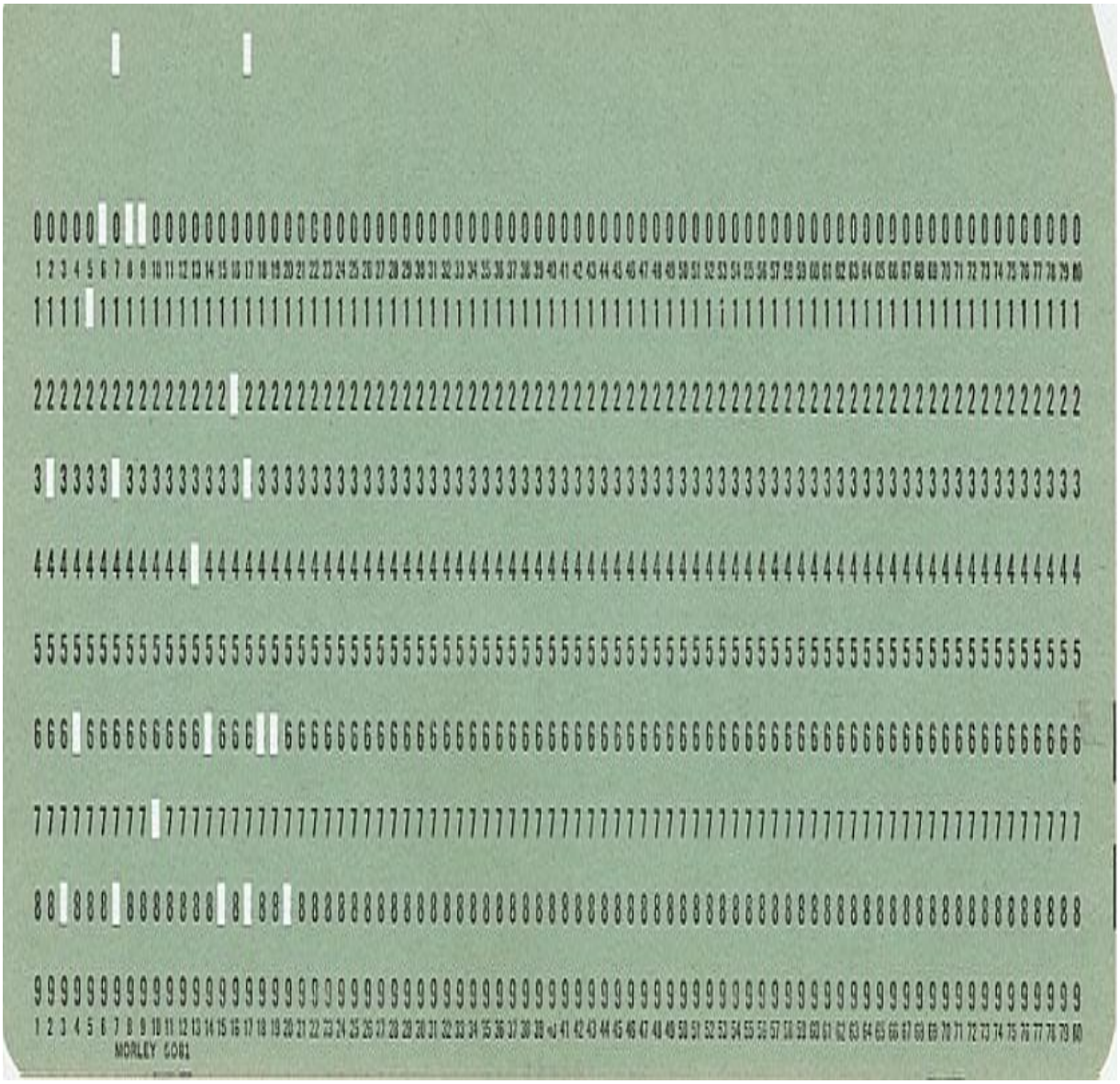


Figure 1.3: A punch card with a FORTRAN programming statement.

1.2.1.3 Paper-based electronic voting systems

In today's progressive and ever changing world, there are all kinds of new voting technologies and electronic voting equipment. This doesn't mean, however, that paper based voting is entirely a thing of the past. E-voting, as it is commonly called, actually defines any type of voting where electronic processes are used in any way, shape or form, such as to cast the votes or to count them. The use of e-votes allows for faster processing time and is expected to pave the way to voting online completely in the future.

For now, however, paper based e-voting is probably the most commonly used type of voting technology. Through this system, electronic votes are placed using a touch screen. This is simply a screen, similar to a computer screen that responds to the user's touch. So, for example, a person would touch the name of the candidate he wished to vote for in order to cast the vote. The "paper-based" part comes in at the end of the voting process when the touch screen, which is hooked up to a printer, prints out the ballot. The voter then checks over the ballot to make sure it is correct and then takes it to the election officer. Later, the votes will be counted using an optical scan voting system. Though, many people feel the paper-based system is slowly becoming outdated and hope to move voting completely online, there are many good things about this system. First of all, since the ballot is printed out after each vote, there is always "proof" of which vote was cast, making it impossible to cheat during counting. Furthermore, all ballots are numbered, making it obvious when one or several ballots are missing. There are, of course, some kinks that still need to be ironed out with the system. Sometimes, the counting machine may falsely read the ballots accidentally, often due to stray marks made on them or being loaded improperly. For this reason, votes are still recounted by hand.

Figure 1.4 Paper based electronic voting booth.

Figure 1.5 Paper based Electronic voting visual display unit.

Paper-based electronic voting systems are voting systems where the electronic means of tabulation is used to count paper ballots. The votes are cast, or marked, on paper ballots by hand or using a marking device, and then an electronic tabulation device is used for counting. This can speed up the process of counting, and not only give less manual work but also less error regarded to human failure. To use the electronic mean of counting ballots, different types of marked paper ballots can be used to cast the vote, depending on what kind of electronic device that is used for tabulation.

The paper ballot system employs uniform official ballots of various stock weights on which the names of all candidates and issues are printed. Voters record their choices, in private, by marking the boxes next to the candidate or issue choice they select and drop the voted ballot in a sealed ballot box.

This paper ballot system was first adopted in the Australian state of Victoria in 1856 and in the remaining Australian states over the next several years. The paper ballot system thereafter became known as the "Australian ballot." New York became the first American State to adopt the paper ballot for statewide elections in 1889.

As of 1996, paper ballots were still used by 1.7% of the registered voters in the United States. They are used as the primary voting system in small communities and rural areas, and quite often for absentee balloting in other jurisdictions.

1.2.1.4 Optical scan systems

Optical scan is another technology that can be used for the counting of paper ballots, and was first applied to voting in the 1980s.

An optical scan voting system is an electronic voting system and uses an optical scanner to read marked ballot papers and tally the results.

An optical scan system used for voting is made up of the following four components:

1. Computer-readable ballots
2. Marking devices
3. Privacy booths

4. Computerized tabulation device

The votes can be cast using a marksense system and using a computer or direct-recording electronic voting system.

1.2.1.5 History of optical scan system

While mark sense technology dates back to the 1930s and optical mark recognition dates to the 1950s, these technologies were first explored in the context of standardized tests such as college entrance exams. The first suggestion to use mark sense technology to count ballots came in 1953, but practical optical scanners did not emerge until the 1960s. The Norden Electronic Vote Tallying System was the first to be deployed, but it required the use of special ink to mark the ballot. The Votronic, from 1965, was the first optical mark vote tabulator able to sense marks made with a graphite pencil. [7]

Types of optical scan systems

1. **Marksense systems**

Marksense systems are using a paper ballot where the candidates and choices are printed next to an empty marking space (could be an empty square, rectangle, circle or oval). The voters cast their vote and record their choices by filling in the space and place the ballot in a sealed ballot box or feed the ballot into a computer tabulating device at the precinct.

The optical-mark-recognition equipment is a device for reading printed or handwritten symbols or bar codes from paper and translates the information to bits. The device reads and counts the vote using "dark mark logic" where the computer selects and count the coloured or dark spot.

The technology used in this system is optical mark recognition scanners where voters mark their choice in a voting response location, usually filling a rectangle, circle or oval, or by completing an arrow. Various mark-sense voting systems have used a variety of different approaches to determining what marks are counted as votes. Early systems, such as the Votronic, introduced in 1965, had a single photo-sensor per column of marks

on the ballot. Most such tabulators used analog comparators that counted all marks darker than a fixed threshold as being votes. The use of digital imaging technology to view the ballot does not necessarily imply more sophisticated mark recognition. For example, the Avante Vote-Tracker simply counts the number of dark and light pixels in each marking area to determine if the mark counts as a vote [8].

More sophisticated mark recognition algorithms are sensitive to the shape of the mark as well as the total overall darkness, as illustrated by the ES&S Model 100, introduced in the mid 1990s. [9].

Figure 1.6: An example of an optical scan ballot.

The ballot can be immediately tabulated at polling stations allowing for voters to be notified by the voting system of voting errors such as an over vote and can prevent residual votes. One such method can display a digital image of the ballot being submitted and allows the voter to review how their ballots are being read [10].

This is known as a precinct count voting system. Alternately the ballots can be collected in the polling station and tabulated later at a central facility, known as central count voting system.

2. **Electronic ballot marker**

An electronic ballot marker (**EBM**) or ballot marking device (**BMD**) is an electronic device that can aid a disabled voter in marking a paper ballot. This device can allow for audio interfaces and still provide paper ballots.

3. **Digital pen voting systems**

Digital pen voting systems use ballots on digital paper which is recognized by a small camera in the pen while it is marked by the voter.

The ballots are collected in a ballot box and the digital pen is returned to an election official for tabulation.

This technology was expected to be used in the 2008 Hamburg state elections, but eventually was decided against due to controversy surrounding the accuracy of voting tallies.

The technology was first used by the town of Menstrie, Clackmannanshire Scotland in their 2006 local community council elections.

Security and concerns

Optical scan voting systems are a form of document ballot voting system, meaning that there is a tangible record of the voter's intent (a paper ballot). Like traditional paper ballots these are subject to electoral fraud and ballot stuffing.

One form of wholesale fraud possible with optical scan voting systems is during the recording of votes. Douglas W. Jones of the University of Iowa states that if a potential attacker were to gain access to the voting system configuration files, they would be able to "credit one candidate with votes intended for another." He found these files are exposed in the computer system used to prepare the election, making them vulnerable to anyone setting up the election. The files are then transferred to the voting system using removable media, and "anyone with access to these media could potentially attack the system." [7].

Another form of wholesale fraud is during tabulation. Possible attacks have been demonstrated by Harri Hursti and the University of Connecticut. [11].

If an attacker is able to obtain a blank ballot (by theft, counterfeit, or a legitimate absentee ballot) the attacker can then mark the ballot for their chosen candidates and convince (through intimidation or bribery) a voter to take the pre-marked ballot to a polling station, exchange it for the blank ballot issued and return the blank ballot to the attacker. This is known as chain voting [7].

Some suggest many of these well-known vulnerabilities can be effectively mitigated. Ballot stuffing may be resolved with incorporation of randomly generated ballot identifier for each paper ballot and capturing digital ballot images of scanned ballots as electronic audit [12].

Tabulation fraud and wholesale tampering can also be prevented by adding a cryptographic verification mechanism. This approach is mathematically based, and thus invariant to software attacks or breaches in chain-of-custody of the paper ballots. One such system is Scantegrity.

Benefits of optical scan voting machines

An advantage of these systems is that the voters don't have to learn to use a voting machine. Physically able voters can simply use pen and paper to mark their intent. Some disabled voters could use a machine to print a voted ballot, which can then be fed into the optical scanner along with all the other ballots, thus preserving the secrecy of their ballot.

Optical scan voting systems can allow for manual recounting of ballots. Statistically relevant recounting can serve as a tool to detect or deter malfunction or fraud. Once an error in the counting process is suspected a full recount can determine the proper results.

An advantage compared to DRE voting machines is that even if the optical scanner fails, voters can still fill out their paper ballot, and leave it to be scanned when the machine is fixed or replaced with a spare.

1.2.1.6 Direct-recording electronic voting systems

A more recent invention used for elections is called direct-recording electronic (DRE) voting systems. This is an electronic implementation of the old mechanical lever systems, where the voters cast ballots by pulling down levers that correspond to each

candidate or issue choice and each lever had a mechanical counter that recorded the number of votes for that position.

The DRE machine was first introduced in the 1970s and is still used in elections [13]. Figure 1.7 shows a picture of an example DRE machine at a polling station.

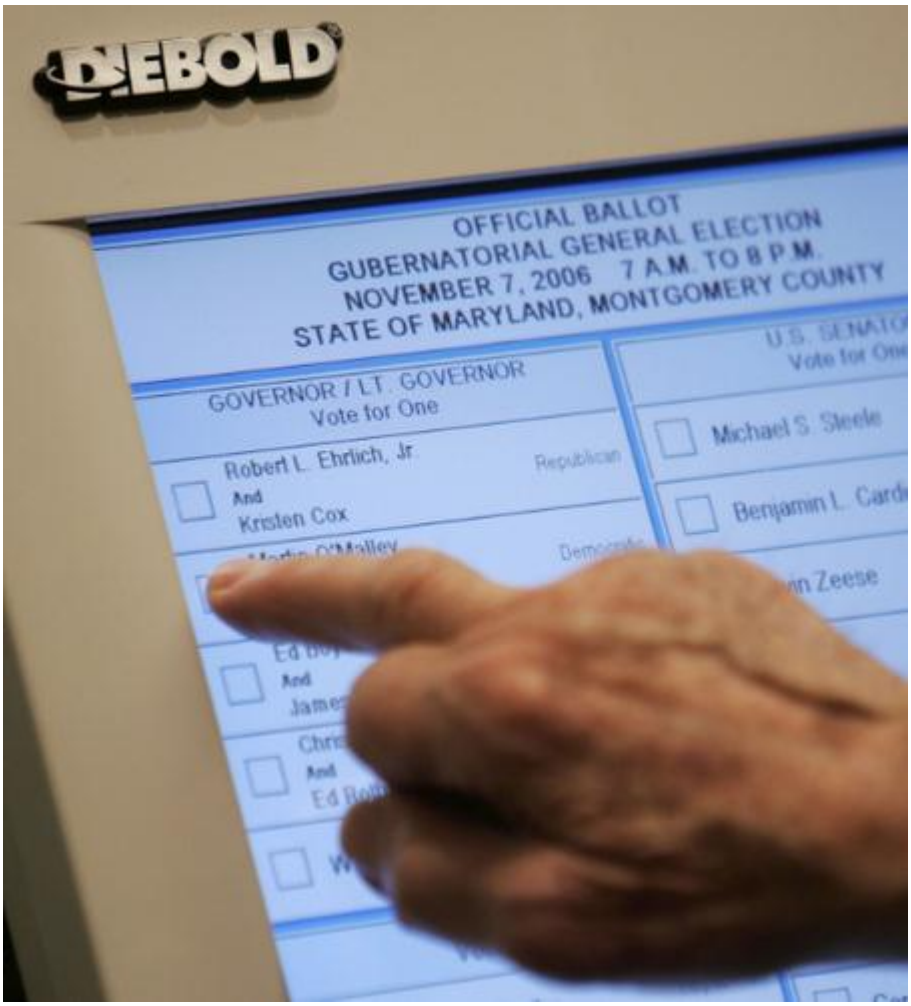


Figure 1.7: A display on a DRE machine showing the electronic ballot, where the voter can cast his vote using the touch screen.

The DRE voting system is a computer on the precinct with a screen to display the ballot and an input device in the form of push buttons or a touch screen.

The machine processes data with computer software and records voting data and ballot images in memory components. The DRE machines can also be used for just the casting

of the vote, and then print a ballot for tallying if other electronic tabulation techniques like optical scanning is used.

The ballot information is prior to the election programmed into electronic memory storage and uploaded to the machine. The screen displays the electronic ballot and the voter registers his choice of vote directly into the system, as shown in figure 1.7. The vote is saved on an electronic storage medium together with the other votes cast on the machine. The tally can be performed at the precinct and the result transmitted, or all the votes can be saved on an external storage medium and transported to a centralized location for tallying.

In a DRE system the ballot styles can be programmed for each precinct regarding the layout, the contests, candidates, pictures of candidates, bilingual options etc. Special options can be configured to support disabilities, for instance larger text or an audio option for visually impaired voters.

For more security features on a DRE machine, smart card technology can also be used [13]. The DRE machines can include a card cartridge system, for activation before access, and can have integrated circuit chips to process and store data - used to open poll and authorize voter access to ballots. When the voter inserts his card, the correct ballot is displayed on screen.

One of the advantages of the use of a DRE voting machine is that the vote is stored directly into the machines memory and saved for electronic tallying, and the DRE system can later also print a record of ballots cast to produce a paper audit trail if necessary (Voter Verified Paper Audit Trail (VVPAT)).

Another advantage is that the voter can print a "receipt" after casting the vote to verify to him that the correct vote was registered. One concern, as mentioned before, when not printing an audit trail, is that it is easier to lose an electronic ballot than a physical paper ballot if an error occurs.

In 1996, 7.7% of the registered voters in the United States used some type of

DRE voting system, and in 2004 the number had grown to almost 30% (US Federal Election Commission).

Regarding the earlier Florida problems with using punch card system, in 2004 a number

of Florida counties changed to DRE units . Again they were criticized, this time of not providing any paper copy accountability of the DRE machines' reliability, and for the 2008 election they went back to using paper ballots read by optical scan machines

1.2.1.7 Public network DRE voting systems

As explained, a DRE voting system is an election system that uses DRE machines to display electronic ballots, and the voter cast his vote directly into the storage memory using for instance a touch screen. A public network DRE voting system can use a DRE machine (computer) at the polling station for the casting of the vote, but after the vote is cast the system can transmit the vote date from the polling place to another location over a public network. By this the public network DRE voting system can utilize either precinct count or a central count method. The vote data may be transmitted as individual ballots as they are cast or as one batch when the polls close. The vote data may also be transmitted periodically as batches of ballots throughout the Election Day to support an updated result at all times. At the central location vote data from several precincts are added up.

Public network DRE voting system not only includes casting the vote from a computer at the polling station, it also includes remote voting as Internet voting and telephone voting.

In general, two main types of e-Voting can be identified:

1. E-voting which is physically supervised by representatives of governmental or independent electoral authorities (e.g. electronic voting machines located at polling stations);

1.2.1.8 Polling place or supervised e-voting

These terms refer to systems where a voter casts their e-vote inside a polling station or a location supervised by electoral officials. Such systems include the DRE voting machines that record the vote electronically without the use of the Internet or other network.

The interface of a DRE machine can be a selection of buttons, a touch screen or a scanner that scans the ballot paper. Some DRE systems also employ a card swipe or cartridge system that must be activated before a vote can be made. Votes are then stored on a memory card, compact disc or other memory device.

Figure 1.8: DRE Voting Machine

2. Remote e-Voting where voting is performed within the voter's sole influence, and is not physically supervised by representatives of governmental authorities (e.g. voting from one's personal computer and mobile phone (also called i-voting)).

Voting over the Internet can be done from remote locations using a computer connected to the Internet. The term Internet voting could also imply the use of traditional polling locations with voting booths consisting of voting systems connected to the Internet. But when referring to Internet voting in this thesis we mean votes cast from a remote location, for instance through the web browser of your home computer, your GSM phone and pad via the Internet. These Internet voting systems are also called cryptographic voting systems.

Internet voting is a type of absentee voting which means the voter can use any personal computer, pads, GSM phone with Internet connection to cast the vote, and it is sent to be stored in the election system.

This is regular Internet users with personal computers installed with standard operating systems other application software.

To vote over the Internet, the voter needs a digital signature to log into the system.

For instance, he needs to identify himself with a unique national Identification number, PIN code or a smart card and then the particular ballot for an election he can participate in is showed.

The voter submits his choice and the encrypted ballot is transmitted over the Internet to a remote server (an electronic ballot box) of the election system.

An overview of am example remote e-voting architecture is showed in figure 1.9

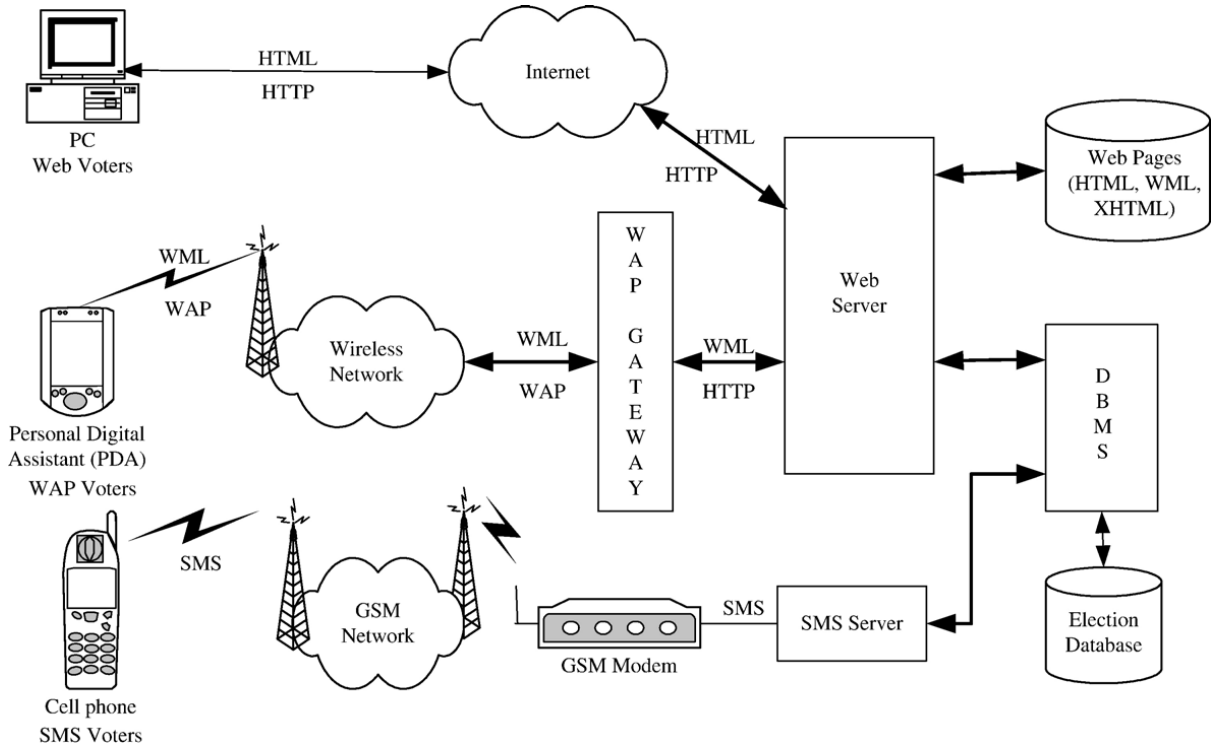


Figure 1.9: Sample remote e-voting system topology

A telephone voting scheme can be based on the voter calling to cast a vote or voting with SMS. An example of a telephone voting scheme could be a voter calling the number of a vote collector, where an automatic answering message informs about the voting procedure. The voter authenticates keying in a PIN code, and then makes his choice by keying in a code corresponding to for instance the candidate he is voting for. After the voter having made his choices the system can recite the voter's options, so the voter can choose to change or confirm his choices. SMS is another mean of casting votes over the GSM network. This is a non-interactive method compared to the "calling

method", where voting is performed in one text message. A "SMS vote", in this type of vote, voter will have to send information which includes the voter's code, a district code and the code to the candidate voting for.

After transmitting a valid vote, the system sent back a SMS confirming the vote was recorded. The receipt did not say anything about which candidate the voter voted for.

Cell phones could also be used as a supplementary channel, in addition to the Internet, for instance to receive codes for authentication or for verification.

The area of remote voting is growing in popularity and the last decade several countries have developed and are testing the use of Internet voting.

Internet voting systems for Government elections has been developed in the UK, Estonia and Switzerland and for party primary elections in the US and France [14].

In Switzerland Internet voting is already an established part of local referendums and voters get their passwords to access the online electronic ballot through the postal service.

In Estonia most voters can use Internet voting, if they want to, both in local and parliamentary elections. They had a pilot project of Internet voting for the municipal elections in 2005, and now almost everyone on the electoral roll has access to the e-voting system.

1.3 **Problem Statements:**

This research work intends to help address the verifiability challenges associated with electronic/ internet voting system with focus on how to address the following questions:

1. What is the impact of verifiability method as related to trust in Internet voting system?
2. How secure is the internet voting system?
3. How would the voters' freedom be not compromised?

These questions will be addressed with more emphasize place on verifiability method of internet voting system.

1.4. Research Objective

The objective of this work is to address the verifiability problem of e-voting or internet voting system which involves:

- To design a system that will capture electorate's vote, instantly updates number of votes cast for each contestant and send verification message to electorate.
- To design a system that will boost electorates' confidence in the electoral process by showing that the vote is count as cast.

1.5. Significance of the study

Significance of this work is to increase trust and popularity of internet or electronic voting system (i-voting/e-voting system) by addressing the verifiability problem associated with the system.

1.6. Scope of the Research

Internet voting system acceptability is mar with many challenges that question its transparency and integrity. Some of the major bottlenecks to the internet voting platform include but not limited to security, secrecy, freedom and verifiability problem. This research work will focus on the verifiability problem of internet voting. The scope of the research job is to design an algorithm with a graphical user interface (GUI) that presents all the political parties identities and option to cast vote for preferred candidate represented by party symbol. The system captures voter's input (vote), do instant database update to display number of votes that electorates cast for each contestant as soon a voter casts his or her vote and send a verification short message service (sms) to all registered voters. This form of verification will show that electorate's vote really

counts.

The system will display the message showing the voter's unique identification number and the increase in the number of votes cast for his or her preferred candidate.

Normally secrecy of the vote is conceived as an easy way to dissuade intimidation, bribery, and other similar coercion of the voter, the system will adhere to this standard and protect electorate freedom.

1.7 Thesis Outline / Organization

This thesis contains five chapters organized as follow:

Chapter one gives background information about electronic voting system, the history, different platform or types, motive behind it, application and problem associated with electronic voting system.

Chapter two explore different related research works carried out on verifiability problem of electronic voting system so as to bridge the gap by addressing all grey areas that are left unaddressed or provide better alternative method of addressing the problem.

Chapter three is the product of critical study of electronic voting system and bottlenecks to its general acceptability or popularity among nations of the world. It attempts to solve the verifiability problem of electronic voting system through a graphical interface that displays updated result as a means of vote cast verification. The essence of this is to prove beyond reasonable doubt that the electorate votes count. This chapter explains methods involved at arriving at this solution

Chapter four explains result of the research work and provides discussion platform.

Chapter five gives summary of the research, derived conclusion and spells out recommendations for possible future work.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

Remote Internet voting system is now developing into being categorized as cryptographic voting systems, not only to provide the sufficient secrecy but also to provide possibilities of verification. The purpose of cryptographically verifiable voting systems is to prevent incorrect recording and tallying, by making the processes verifiable for everyone.

The latest development in the area of voting systems verifiability is end-to-end (E2E) verifiable systems, also called open-audit voting systems. The last few years have witnessed the emergence of end-to-end voting systems, which enable voter-verification of election outcome (Program and presentations at nist e2e workshop) [15].

The purpose of E2E systems is primarily to improve election integrity through E2E verifiability.

The cryptographic voting protocols offer the promise of verifiable voting without needing to trust the integrity of any software in the voting system. E2E systems are voting systems with strict integrity properties and strong tamper resistance.

End to End systems use existing cryptographic methods to generate receipt and proofs, giving the voter a possibility of verifying their votes. The voters by this mean of receipt codes and proofs also verify their votes have not been modified by corrupt actors and are accurately recorded in the election system.

Those who cast the votes decide nothing; those who count the votes decide everything.[18].

By the use of different cryptographic methods this verification is possible without revealing for the system or outsiders which candidates were voted for

The first use of Internet voting for a binding political election was found to be in the U.S. in 2000, with more countries subsequently beginning to try and use Internet voting. Each year since 2006, four to six countries have used this voting method. A total of 11 countries have now used remote Internet voting for binding political elections.

The group of Internet voting system users consists of four core countries which have been using Internet voting over the course of several elections/referenda: Canada, Estonia, France and Switzerland. Estonia is the only country to offer Internet voting to the entire electorate. The remaining seven countries have either just adopted it, are currently piloting Internet voting, have piloted it and not pursued its use, or discontinued its use.

Examples of Internet voting in other countries around the world vary widely in scope and functionality. The early cases of Internet voting were less technically advanced than those being developed more recently. Many of the changes seen in Internet voting systems have been aimed at improving the quality of an election delivered by the Internet voting system and meeting emerging standards for electronic voting.

It is fair to say that Internet voting is not a commonly used means of voting, with only 11 countries having so far used it in any form, and only seven of these 11 countries currently having any intention of using it in the future. However, this low level of usage globally needs to be put into the context of Internet voting being a relatively new voting technology, and one that has been developing significantly over the previous 10 years. Internet voting seems to fit, for many countries, a niche corner of the electoral system. It is largely targeted at those who cannot attend their polling station in-person on Election Day.

In fact, many more countries have expressed or shown an interest in the use of Internet voting, especially when they have large numbers of expatriate voters. However, the implementation of Internet voting, according to emerging standards, is a very technical exercise. It can also pose some difficult political questions if the aim is to facilitate the inclusion of large numbers of expatriate citizens in the political process.

The technicalities of implementing Internet voting systems are largely a result of attempts to reconcile the use of Internet voting with emerging and existing standards with which elections and electronic elections are required to comply. These standards include the need for secure online voter authentication, protection of the secrecy of the vote, appropriate transparency mechanisms, testing and certification regimes. The need for secure online voter authentication mechanisms may be one of the biggest hurdles in implementing Internet voting. It presents a challenge for many established democracies,

which often do not have an ID card system with secure online authentication mechanisms.

Verifiability is quite a tricky thing, but there is already an analog method (mail ballot) already in place. Most mail ballots have two envelopes which contains the ballot. The outer envelope contains enough information to identify the voter. A ballot worker will take this information, verify the ballot, and then place the inner envelope into the ballot pool. So long as this is managed correctly, it would work.

The analog to this in the digital world would be to encrypt your data first with a public key that only the election office can decrypt (to ensure your data can't be guessed via a collision), and secondly with a signature that you have voted, something that presumably would be mailed to you. Your vote is passed to a computer server, which verifies you are eligible, and haven't voted, which then passes the encrypted vote portion on to a second system, which records your votes. Still, there is some inherit danger in someone frauding this system.

There are some systems which allow for calculations on encrypted data, but for the most part, these are not yet ready for prime time. Still, these would allow for an even more secure system, one in which all votes could be public, but no one would know who voted for who.

To some extent anonymity can be achieved by traditional voting on paper ballots. (Of course, there is no longer guarantee that the ballots do not contain hidden features invisible for the voter.) Electronic ballots are much harder to handle: if the ballots are identical, then there will be many ways to attack the system by casting additional votes.

If the ballots are unique, then they might be used for uncovering voters' preferences and for vote selling. If they contain random values, then these values may be used to leak secrets.

Another practical issue for Internet voting is voter authentication, but it always assumed that the voters can authenticate themselves with digital signatures.

Verifiability of the election results is one of the major issues for electronic voting: while for the paper ballots there are some procedures against election frauds (they work as long as the commissions are honest), electronic voting is virtual and the voter may

distrust the security mechanism of mixing and counting the votes. Therefore, one of the important features would be to provide the voter a (printed) trace that enables her to check that her vote has been counted and included in the final result. This concept of voting receipts is a central feature in many schemes.

However, it is also a major problem for system design. At the same time two requirements should be satisfied:

- ✓ A receipt must convince a voter that her ballot was properly counted,
- ✓ A receipt must not reveal voter's choice.

According to International experience with e-voting [19], trust in the electoral process is essential for successful democracy. Where this trust is lacking the integrity of the overall electoral process may be called into question, undermining the legitimacy of elected institutions and the authority of elected government.

The rational choice needed for voters to trust Internet voting seems to require a level of technical expertise that the average voter cannot be expected to have. In order to compensate for the inherent complexity of Internet voting, extra measures need to be taken to ensure that voters have a sound basis on which to give their trust to Internet voting systems. Institutions and experts can play an important role in this process, with voters trusting the procedural role played by independent institutions and experts in ensuring the overall integrity of the system.

A number of mechanisms can be used to enable the development and maintenance of trust in Internet voting systems.

One of the fundamental ways in which trust can be enabled is to ensure that information is made available about the Internet voting system. The system must also be trustworthy, and measures to ensure the integrity of the system are important.

A vital aspect of integrity is ensured through testing, certification and audit mechanisms. Due to the inherent lack of transparency with Internet voting, it is important to separate the responsibilities for different stages of the Internet voting process. Such a separation of duties means it is more difficult to manipulate the system. Allowing the casting of repeated Internet votes also helps generate trust amongst voters. Making the Internet

voting system verifiable, so that the results can be independently verified against the votes cast, is an increasingly important trust mechanism, although this needs to be done in a way that does not violate the secrecy of the ballot. Internet voting systems should be subjected to various evaluation mechanisms which include Safety and secrecy of voting, Robustness of Internet voting system, Authorization and authentication of voters, Eligibility, Availability, reliability and operability of voting, Testing and certification, Auditability, User-friendly usability, Transparency of voting, Enfranchisement and uniformity of voting, Verifiability, repeatability and controllability of vote counting, Unprovability of voting, Possibility for re-vote and Supremacy of conventional voting.

Many of the concerns raised by Internet voting are very similar for postal voting. Both channels are based on voting from unsupervised environments and such environments cannot provide the same guarantees of secrecy and freedom as are commonly implemented within polling stations. Briberies, intimidation and other similar coercions are more likely to happen and also the principle of secrecy might be endangered both by Internet and by postal means.

Once remote voting is accepted as a legitimate channel to cast a ballot, it is worth noting that postal voting may also be implemented in different ways with different impacts on electoral principles. For instance, in Spain postal voting is allowed, but voters can only cast their ballots through recommended mail. That is to say, they have to show up at a postal office, identify themselves (only recently) and insert their ballot in a special envelope. Although this protocol does not provide the same guarantees as a traditional polling station, it intends to implement some degree of protection for postal voting.

However, other countries allow postal voting in a more flexible way. In Switzerland, for instance, voters can cast their ballot by inserting the polling card that they have previously received in a normal postal box located in any street. Ordinary mail, with no supplementary mechanisms of control, is used even for electoral material.

Verifiability is one of the key issues that any Internet voting project has to address. As with other remote voting channels (e.g. postal voting), it does not normally provide a voter with any proof that his or her vote was cast or received as intended. In fact, receipts that can be used to prove the content of a vote are prohibited by some

international electoral standards as they facilitate the coercion of voters and vote buying practices. [20].

However, voting receipts are still a technically feasible solution and would improve the system's trustworthiness, provided they manage to overcome the problems concerning the secrecy of the vote and the freedom of the voter. While some countries (e.g. the Netherlands) decided to include voting receipts despite their negative effects over such principles, other projects, like the Norwegian one, intend to use voting proofs in a way that does not violate the principles of voter freedom or secrecy.

Voter Verified Paper Audit Trail (VVPAT) and voter verified paper ballot (VVBP) are equivalent and refer to a kind of "vote receipt" printed by an electronic voting machine that shows the voter's vote as it is being entered into the electoral system.[21]. Voters will be asked to perform an action that confirms that their choices have been recorded correctly on the paper, hence making it a verified (rather than just "verifiable") ballot in a legal sense. The Voter Verified Paper Audit Trail / voter verified paper ballot is kept by the election official, as the record of votes cast, for audit and recount purposes. Verification of a small percentage of VVPAT should to be activated when elections are close.

Thus VVPAT cannot be used to verify electronic electoral results unless they are all counted. If VVPAT is printed and counted for each casted vote then we simply run a paper election which ballots are printed by machines instead of being hand written by voters. If each voter could (and would) verify the vote recorded on his behalf is really the one he cast, and then we would verify the correctness of the election's result. I think such a result's verification is impossible to realize since all the voters should verify their own vote simultaneously at the same time in which a (proven error-and-fraud-free) tally is executed to produce the final result. If the counting would not occur in the same moment while all the votes are being verified, it will be difficult to prove that all votes are properly tallied up. It will be a difficult task to program any computer to show voter his true vote and then not taking it in account during the count.

Furthermore, we can't build any system allowing people to verify how their votes have been recorded because:

- Votes would be no more anonymous since voters could be tracked .We would miss the anonymity requirement due to the possibility to link a vote with its voter. It is not enough to say that the "key" to make such link might be only available to the voter himself. In paper ballots such key doesn't exist at all.
- There is no way to know if a claim of error would be honest.
  We know voters can't be given any "receipt" stating how they voted, and thus there is no way for them to prove. If this is the case, the vote stored in their behalf is not the one they really cast.
  Even if an algorithm that allows the verification of the recorded votes without breaking their anonymity exists, it should be used with great care. In fact it would in any case show the voter how their vote has been recorded and thus it would be much like as they were given a receipt of the cast vote

These are in fact the procedures adopted to date by all the liberal democracies; a written vote in secret on an anonymous ballot-paper that is first mixed with hundreds of others and then counted in public together with the others. In this way the ballot-papers are tangible, legible to the naked eye, anonymous and durable in time. They are also verifiable later. The counting procedures, if public control is effectively carried out, guarantee that all the ballot-papers of a polling station are correctly interpreted. In this way, the voters are certain that their own vote has been correctly counted even though the anonymity of the ballot-papers does not allow the identification of individual votes. The results of the count at every polling station are numbers visible to the naked eye and, being public, also the counting procedures are verifiable by everyone; even the sum at the various levels (local authority, province, region/state and nation) can be verified.

The public and repeatable procedures and votes that are tangible objects, like the ballot-papers, constitute the only system that can guarantee anonymity and assure the correct counting of the votes.

Internet voting has gone from private and military trials to mainstream politics in two European states.

2.2 Internet voting a success in two European Countries

The internet as a means of casting votes lead to distortions in the political sphere? How neutral is this new technology?" Fears that e-voting would affect the outcome of elections was a key reason that trials within the US Army were shut down in the early 2000s. A similar debate was happening across the Atlantic in Switzerland: "The left said the internet was just for rich people; rich people have access to the technology and are voting on the right, therefore it could be our death knell. The right said that the internet was a new thing for young people, and the young people are more on the left, so it's not good for us."

But whereas citizens in the US are still not able to vote online, the practice has been rolled out across Swiss cantons and was enshrined in Geneva's constitution in 2009. The other European success story – Estonia – is remarkable owing to its political past. [22] "Estonia was leapfrogging, going from a Soviet republic in 1989 to one of the most advanced democratic systems, in terms of the way they handle votes, in only 16 years," said the professor, who led a Council of Europe-funded team researching e-voting in the country.

In both Estonia and Switzerland e-voting was introduced in part to tackle the problem of a decline in turnout as "one of the major problems of democracy". Although the two countries differ greatly in their political history and structure, both states had a modern electoral administration, high levels of internet penetration and political will, which made them fertile ground for e-voting.

Furthermore, "both cases were clever – they involved social scientists from the beginning, something other early movers [which failed to implement e-voting following trials] didn't do. Their international work was very important; both the Swiss and the Estonians were very active in setting international standards".

Voters can now use a card – or also a mobile phone ID in Estonia – to cast their ballot over a set period of time. Estonia rolled out e-voting in 2005 and by 2009 nearly a quarter of all votes cast were online, while the canton of Geneva in Switzerland says e-

voting is now stable at around 20 per cent, a decade after the first binding e-votes were cast.

In Estonia, it was found that around 16 per cent of e-voters said they probably would not have voted had internet voting been unavailable. “In 2009 this turnout loss [overall] would have been 2.6 per cent, so it’s a small effect on turnout. It’s very clear a convenience factor is important,” he said.

Another vital sign of a successful e-voting system is trust, Netherlands had to abandon the practice after its electronic voting machines were hacked, calling into question the reliability of the new technology.

Trust was found to be imperative not only in the technology but also the wider voting system: “You cannot see internet voting in separation from the entire system and functioning of the voting administration. If the voting administration is not properly functioning, there’s a high risk of internet voting not functioning either.”

2.3 Internet Voting and Individual Verifiability

The return codes used in the Norwegian Internet voting system were simply text messages sent to the voter immediately after he or she had cast a ballot. The message included a code representing the party list that the voter had cast a vote for and indicated the number of personal votes that had been cast. An SMS message was sent each time an Internet vote was cast. Before the election, each voter received a polling card containing a list of codes for each party list on the ballot for the municipal and county elections. The combination of codes assigned to the party lists on the ballot was unique for each voter.

Therefore, when the voter received the SMS message with the relevant code, he or she could refer to the polling card to determine whether the code represented the cast ballot. If the code did not match, representing a clear technical flaw in the system, the overall

Electoral process could continue because the voter would still be able to cast another I-ballot, which would hopefully be recorded correctly; the option to vote by paper ballot would have also been an option. Such codes clearly improve the verifiability of the

voting system as they provide proof that the system received the vote as cast and that it was cast as intended. However, it is only a partial verifiability because return codes do not prove that the vote is stored as cast or that it is included in the count as it is stored. However, the mechanisms mentioned above intend to complete this sequence of verifiability encompassing all the electoral stages. With the challenges that these return codes generate in mind, the following sections will analyze how the return codes address the protection of the secrecy of the vote and to what extent they comply with the standards that preclude the use of voting receipts for remote voting projects.

In electronic voting, verification and validation processes should be performed to assure the security and reliability of the e-voting protocols and systems. Since an e-voting system usually depends on an e-voting protocol, the verification and validation of the e-voting system typically covers verification and validation of the e-voting system and its underlying e-voting protocol.

In practice, verification and validation activities should occur both during, as well as at the end of the development life cycle to ensure that all requirements have been fulfilled and the system works properly. The quality of the requirements can be improved and costs and risks can be controlled by performing verification and validation early in the development process.

Verifiability and verification in e-voting is started to be discussed recently. Unfortunately the definitions for verifiability are inadequate and unclear. Moreover, verifiability is categorized as individual verifiability and universal verifiability, where they are generally misused in the literature. Besides, validation has not been discussed properly yet and there is no obvious consensus about the definitions [23].

Delaune formalizes some of the e-voting requirements and then verifies whether the requirements hold on particular e-voting protocols. [24]. Specifically they use the formalism of the applied pi calculus which is a formal language similar to the pi calculus but with useful extensions for modeling cryptographic protocols and has been used to analyse a variety of security protocols in other domains.

Delaune et al [24]; brings the formal verification on some of the e-voting requirements; however, they do not mention anything about the validation issues. Formal verification is the act of proving or disproving the correctness of intended algorithms underlying a

system with respect to a certain formal specification or property, using formal methods of mathematics. This research seems important for future studies since it meets formal verification with e-voting.

2.4 Individual and universal verification methods

One of the major concerns of remote voting in general is the lack of means for the voter to verify the correct reception and count of his or her vote. The introduction of remote electronic voting can provide to the voters some means to individually verify the voting process, providing more confidence and detecting possible attacks. The verification process can be split in two methods:

1. **Cast as intended verification.**

The cast as intended verification is base on ensuring that the vote received by the voting server contains the voting options originally selected by the voter. For instance, it can be used to detect if the voter computer has any malware that is changing his or her voting options before encryption. One way to perform this verification consists on calculating special codes (commonly called Return Codes) using the encrypted vote received at the voting server, and returning them to the voter. The voter will in turn use a special voting card issued for the election to verify that the received return codes are those assigned to the voting options she has chosen. Since the return codes are calculated using a secret key only known by the voting server, an attacker cannot deliver forged return codes to the voter without being detected.

2. **The counted as cast verification**

The counted as cast is base on ensuring that the vote cast by the voter is included in the final tally. This verification detects manipulation or deletion of cast votes. One method to ensure that the vote has reached the counting phase is to deliver to the voter a receipt with a random identifier. If this random identifier can only be retrieved from the encrypted and tallied votes, a voter can then verify that her vote has been included in the tally. It is of paramount importance that these random identifiers cannot be correlated with clear text votes. Otherwise, the voting receipt could be used for vote buying or

coercion practices. This measure must be complemented with the universal verification of the decryption process. Universal verification should allow auditors and observers to verify in an irrefutable way that the decrypted votes represent the contents of the encrypted ones.

In other words, that the decryption process did not manipulate the results. This can be achieved using advance cryptographic techniques.

2.5 Verification and validation (v&v) in e-voting

Many e-voting protocols have been proposed from both theoretical and practical perspectives in the literature. However, no complete solution has been found because of the importance of security requirements in voting systems such as privacy, accuracy, fairness and robustness.

E-voting protocols have an anonymity requirement, which means the unlinkability between the voter and his cast vote. Anonymity is the primary requirement of the e-voting protocols in order to satisfy voter privacy. [23]

Fraud and system violations can be done without being detected in anonymous environments. This characteristic of e-voting forces the researchers to find a way to persuade the voter that his vote is really counted and the voting is done properly. This requirement is named as verifiability and used many years in the literature.

In software engineering, verification is the process of verifying that the system complies with design specifications and formally specified properties, such as consistency and redundancy; and validation is the process of validating that the system satisfies the intended use and fulfils the user requirements (IEEE 1996). In other words, verification is building the system right and validation is building the right system.

In an ideal world, a verified system would be naturally validated, but this is far from what is currently possible in practice. Even if it is possible to specify formally all of the user requirements, and then to verify that a system conforms to this specification, there would still be no guarantee that the requirements were correct.

Verification can be viewed as a part of validation, it is unlikely that a system that is not “built right” to be the “right system”. However, verification is unlikely to be the whole

of validation, due to the difficulty of specifying user requirements. Therefore, it seems that validation should be more than verification.

In e-voting, verification is the process of verifying that the e-voting system complies with design specifications and formally specified system requirements, such as robustness and fairness; and validation is the process of validating that the e-voting system satisfies its intended use and fulfils the user requirements, such as accuracy and eligibility. Verification also includes the review of interim work steps and interim outputs during the e-voting process

2.6 Trust in internet voting

Auditability is defined as the capacity of a system to "provide evidence to auditors that the system functioned in the way it was supposed to. In addition, the voting system and its supporting election procedures must provide assurances that the evidence provided by the system is trustworthy.

The word "trustworthy" is at the heart of the auditability problem. While server technology can be tested for integrity and proper operation, the fundamental issue is whether the humans who are responsible for constructing and operating the online voting system can be trusted to do so honestly and competently.

Indeed, exercising such judgment is precisely what an elected official is elected to do. Our Constitution establishes a system of representative government. Thus, at least in some measure, that document assumes that citizens will trust their representatives to execute their duties with honesty and competence. Frequent and regular elections, plus the powers of impeachment, are ways for the citizenry to remove officials who violate that public trust. But without some measure of trust, representative government would not be possible.

To put a human face on this political theorizing, in 2011, West Virginia Secretary of State, Natalie Tennant, was invited to participate on a panel, which, as we mentioned above, turned out to be very one-sided. She was the only defender of Internet voting, while there were several high profile anti-Internet voting activists on the other side. The issues of trust and official responsibility soon came up. When a panelist demanded to

know how her office vetted the companies that provided her state's Internet voting service, she replied that the vendors had to agree to several conditions.

One of these was that third party experts be allowed to inspect the equipment and operating codes the vendors used. She said the companies not only agreed to these conditions, but offered to do the whole job for free, as a demonstration project. Given that situation, the Secretary decided not to exercise the right to bring in a third party inspector. She said she trusted the companies.

Another panelist insisted that the vendors could be corrupt and she wouldn't know it. She replied that election officials have to exercise their professional judgment as to when such trust is reasonable. When pressed by the moderator about possible insider wrongdoing as well as software rigging, Ms. Tennant stated that she trusted the workers in her department because it was like a small community in which everyone knew each other. She trusted the system because it used military grade encryption, had an intrusion detection function, and other security checks. She also pointed out that it was a serious felony to tamper with elections, and this law is a part of the security system [25]

In a large and complex political system like the US, if election officials could not be trusted to carry out their responsibilities well, public elections would risk descending into anarchy, and the entire political order fall into ruin. Imagine the chaos if mobs of "election integrity" enthusiasts demanded to observe and perhaps photograph or film all voters, the voted ballots, and the officials as they sorted through high piles of paper trying to tally the vote. At least since the discovery of agriculture, the division of labour has made modern civilization possible. Having some trust in the other fellow to do his part has made the division of labour possible; for, if everyone felt that he or she could not depend on anyone else, nothing would get done, and humanity would have to live, like primates, as foragers. As Secretary Tennant understood, the formula for Internet voting success, then, is to combine the ancient, and constitutional, principle of reasonable trust in other people with 21st Century technology. From that, the further advancement of democracy will follow.

2.7 The Helios Voting System

The Helios voting system [http://blog.heliosvoting.org] is a web-based open audit system developed by Harvard University and Ben Adida [26]. The voting system opens for new possibilities of verifying and auditing ballots cast over the Internet. Using Helios, anyone can create an election, invite voters to cast a secret ballot, compute a tally and then generate a validity proof of the entire process [27].

The Helios system is built on existing web programming techniques and cryptographic voting protocols using the Google App Engine to run the voting application [28].

2.8 A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)

This is a review and critique of computer and communication security issues in the SERVE voting system (Secure Electronic Registration and Voting Experiment), an Internet-based voting system being built for the U.S. Department of Defense's FVAP (Federal Voting Assistance Program). While the system is called an experiment, it is going to be used to count real votes in the upcoming general elections. Members of SPRG (the Security Peer Review Group), a panel of experts in computerized election security that was assembled by FVAP to help evaluate SERVE. The task was to identify potential vulnerabilities the system might have to various kinds of cyber-attack, to evaluate the degrees of risk they represent to the integrity of an election, and to make recommendations about how to mitigate or eliminate those risks[29].

The SERVE system was planned for deployment in the 2004 primary and general elections, and to allow the eligible voters first to register to vote in their home districts, and then to vote, entirely electronically via the Internet, from anywhere in the world. Besides being restricted to overseas voters and military personnel, SERVE was limited to people who voted in one of 50 counties in the seven states (Arkansas, Florida, Hawaii, North Carolina, South Carolina, Utah, and Washington) that are participating. The program is expected to handle up to 100,000 votes over the course of the year, including both the primaries and the general election. (By comparison, approximately 100 million votes were cast in the 2000 general election.) The eventual goal of SERVE was to

support the entire population of eligible overseas citizens plus military and dependents. This population is estimated to number about 6 million, so the 2004 SERVE deployment must be judged as a prototype for a very large possible future system.This exercise led to these discoveries about internet voting system

a. DRE (direct recording electronic) voting systems have been widely criticized elsewhere for various deficiencies and security vulnerabilities: that their software is totally closed and proprietary; that the software undergoes insufficient scrutiny during qualification and certification; that they are especially vulnerable to various forms of insider (programmer) attacks; and that DREs have no voter-verified audit trails (paper or otherwise) that could largely circumvent these problems and improve voter confidence. All of these criticisms, which were endorsed, apply directly to SERVE as well.
b. Because SERVE is an Internet- and PC-based system, it has numerous other fundamental security problems that leave it vulnerable to a variety of well-known cyber attacks (insider attacks, denial of service attacks, spoofing, automated vote buying, viral attacks on voter PCs, etc.), any one of which could be catastrophic.
c. Such attacks could occur on a large scale, and could be launched by anyone from a disaffected lone individual to a well-financed enemy agency outside the reach of U.S. law. These attacks could result in large-scale, selective voter disenfranchisement, privacy violation, vote buying and selling, and vote switching even to the extent of reversing the outcome of many elections at once, including the presidential election. With care in the design, some of the attacks could succeed and yet go completely undetected. Even if detected and neutralized, such attacks could have a devastating effect on public confidence in elections.
d. It is impossible to estimate the probability of a successful cyber-attack (or multiple successful attacks) on any one election. But we show that the attacks we are most concerned about are quite easy to perpetrate. In some cases there are kits readily available on the Internet that could be modified or used directly for attacking an election.

And we must consider the obvious fact that a U.S. general election offers one of the most tempting targets for cyber-attack in the history of the Internet, whether the attacker's motive is overtly political or simply self-aggrandizement.

e. The vulnerabilities that were described cannot be fixed by design changes or bug fixes to SERVE. These vulnerabilities are fundamental in the architecture of the Internet and of the PC hardware and software that is ubiquitous today. They cannot all be eliminated for the foreseeable future without some unforeseen radical breakthrough. It is quite possible that they will not be eliminated without a wholesale redesign and replacement of much of the hardware and software security systems that are part of, or connected to, today's Internet.

f. We have examined numerous variations on SERVE in an attempt to recommend an alternative Internet-based voting system that might deliver somewhat less voter convenience in exchange for fewer or milder security vulnerabilities. However, all such variations suffer from the same kinds of fundamental vulnerabilities that SERVE does; regrettably, we cannot recommend any of them. We do suggest kiosk architecture as a starting point for designing an alternative voting system with similar aims to SERVE, but which does not rely on the Internet or on unsecured PC software.

g. The SERVE system might appear to work flawlessly in 2004, with no successful attacks detected. It is as unfortunate as it is inevitable that a seemingly successful voting experiment in a U.S. presidential election involving seven states would be viewed by most people as strong evidence that SERVE is a reliable, robust, and secure voting system. Such an outcome would encourage expansion of the program by FVAP in future elections or the marketing of the same voting system by vendors to jurisdictions all over the United States, and other countries as well. However, the fact that no successful attack is detected does not mean that none occurred. Many attacks, especially if cleverly hidden, would be extremely difficult to detect, even in cases when they change the outcome of a major election. Furthermore, the lack of a successful attack in 2004 does not mean that successful attacks would be less likely to happen in the future; quite the contrary, future attacks would be more likely, both because there is more time to prepare the attack, and because expanded use of

SERVE or similar systems would make the prize more valuable. In other words, a "successful" trial of SERVE in 2004 is the top of a slippery slope toward even more vulnerable systems in the future. (The existence of SERVE has already been cited as justification for Internet voting in the Michigan Democratic caucuses.)

h. Like the proponents of SERVE, we believe that there should be better support for voting for our military overseas. Still, we regret that we are forced to conclude that the best course is not to field the SERVE system at all. Because the danger of successful, large-scale attacks is so great, we reluctantly recommend shutting down the development of SERVE immediately and not attempting anything like it in the future until both the Internet and the world's home computer infrastructure have been fundamentally redesigned, or some other unforeseen security breakthroughs appear. We want to make clear that in recommending that SERVE be shut down; we mean no criticism of the FVAP, or of Accenture, or any of its personnel or subcontractors. They have been completely aware all along of the security problems we describe here, and we have been impressed with the engineering sophistication and skill they have devoted to attempts to ameliorate or eliminate them. We do not believe that a differently constituted project could do any better job than the current team. The real barrier to success is not a lack of vision, skill, resources, or dedication; it is the fact that, given the current Internet and PC security technology, and the goal of a secure, all-electronic remote voting system, the FVAP has taken on an essentially impossible task. There really is no good way to build such a voting system without a radical change in overall architecture of the Internet and the PC, or some unforeseen security breakthrough. The SERVE project is thus too far ahead of its time, and should wait until there is a much improved security infrastructure to build upon.

2.9 Computer Technologists Statement on Internet Voting

Election results must be verifiably accurate – that is, auditable with a permanent, voter-verified record that is independent of hardware or software. Several serious, potentially insurmountable, technical challenges must be met if elections conducted by transmitting votes over the internet are to be verifiable [30]. There are also many less technical questions about internet voting, including whether voters have equal access to internet technology and whether ballot secrecy can be adequately preserved.

Internet voting should only be adopted after these technical challenges have been overcome, and after extensive and fully informed public discussion of the technical and non-technical issues has established that the people of the U.S. are comfortable embracing this radically new form of voting.

A partial list of technical challenges includes:

• The voting system as a whole must be verifiably accurate in spite of the fact that client systems can never be guaranteed to be free of malicious logic. Malicious software, firmware, or hardware could change, fabricate, or delete votes, deceive the user in myriad ways including modifying the ballot presentation, leak information about votes to enable voter coercion, prevent or discourage voting, or perform online electioneering. Existing methods to "lock-down" systems have often been flawed; even if perfect, there is no guaranteed method for preventing or detecting attacks by insiders such as the designers of the system.

• There must be a satisfactory way to prevent large-scale or selective disruption of vote transmission over the internet. Threats include "denial of service" attacks from networks of compromised computers (called "botnets"), causing messages to be mis-routed, and many other kinds of attacks, some of which are still being discovered. Such attacks could disrupt an entire election or selectively disenfranchise a segment of the voting population.

• There must be strong mechanisms to prevent undetected changes to votes, not only by outsiders but also by insiders such as equipment manufacturers, technicians, system administrators, and election officials who have legitimate access to election software and/or data.

• There must be reliable, unforgeable, unchangeable voter-verified records of votes that are at least as effective for auditing as paper ballots, without compromising ballot secrecy. Achieving such auditability with a secret ballot transmitted over the internet but without paper is an unsolved problem.

• The entire system must be reliable and verifiable even though internet-based attacks can be mounted by anyone, anywhere in the world. Potential attackers could include individual hackers, political parties, international criminal organizations, hostile foreign

governments, or even terrorists. The current internet architecture makes such attacks difficult or impossible to trace back to their sources.

Given this list of problems, there is ample reason to be skeptical of internet voting proposals. Therefore, the principles of operation of any internet voting scheme should be publicly disclosed in sufficient detail so that anyone with the necessary qualifications and skills can verify that election results from that system can reasonably be trusted. Before these conditions are met, "pilot studies" of internet voting in government elections should be avoided, because the apparent "success" of such a study absolutely cannot show the absence of problems that, by their nature, may go undetected. Furthermore, potential attackers may choose only to attack full-scale elections, not pilot projects.

The internet has the potential to transform democracy in many ways, but permitting it to be used for public elections without assurance that the results are verifiably accurate is an extraordinary and unnecessary risk to democracy

2.10 Return Codes and Vote Secrecy

Regardless of whether return codes are used or not, Internet voting always entails serious concerns about the secrecy of the vote and the freedom of the voter.

This voting channel is normally used in uncontrolled environments, that is to say, a situation in which there are no means to guarantee that the voter is free from external influence in casting his or her ballot. There is no voting booth to ensure secrecy or official supervision to ensure that the voter is alone when voting, and therefore the vote might be submitted under pressure from external forces, which would breach both to the voter's freedom to vote as well as the secrecy of the vote. Return codes only serve to strengthen these concerns. These SMS messages would simplify the task of coercers and vote-buyers because they need only ask the voter to provide the appropriate proof generated by the Internet voting system itself. Unless the voter manages to send a faked SMS message, which is difficult to do because they are sent by the server itself, the coercer would not be compelled to directly supervise the voting session to know how the voter cast his or her ballot.

Taking these risks into account, most Internet voting projects do not include individual verification means. They assume that the advantages linked to remote voting channels (e.g. easier access to the voting process for some groups) justify not being able to replicate some guarantees that exist in supervised voting environments (e.g. direct supervision). From this point of view, Internet voting can be seen as similar to postal voting. Postal voting is allowed in many Western democracies; despite being unable to guarantee the freedom of the voter and the secrecy of the postal votes cast, it is seen as a legitimate voting channel.

Postal voting does not provide any means by which the voter can individually verify that his or her vote has been received or counted as cast. While Estonia and some Swiss cantons (e.g. Geneva) use such an approach, the Netherlands and Norway sought to implement Internet voting with mechanisms for individual verification.

2.11 Electronic Voting and Privacy

Despite the many obvious benefits of implementing electronic voting in twenty-first century American society, the topic is riddled with pitfalls that must be carefully dealt with if such an election system is to be successful. Given the lack of historical precedent for electronic voting systems, case law is lacking. The courts, faced with Internet voting cases in the future, will be forced to examine more non-traditional sources of precedent, and to look at the unique issues which affect the validity of any computer-based election. In particular, issues of voting privacy, security, and integrity are of overwhelming importance. These issues go to the core of the nature of voting, and the problems that must be addressed in any electoral system.

One of the most fundamental rights of voters in the United States is the right to secretly cast a ballot. In a very real sense, this concept of election secrecy ensures that an election will be sound and that citizens can make choices without fear of reprisal from the government or special interest groups. The most terrifying image of what a non-confidential election could represent is a non-Democratic country whose ballots are

placed into two boxes, based on a vote for the president. One box is for the incumbent, and the other is surrounded by military officers with assault rifles, and the obvious implication that a vote other than for the incumbent could be hazardous to the voter's health. Therefore, the need to ensure a confidential vote is apparent.

Recently, implementation of Internet-based elections has been prolific on college campuses. While one must admit that the sanctity of a student government election is less critical than that of national offices, the security measures imposed are certainly indicative of valid methods for operating an election. At the University of Maryland, for example, student government officials instituted an Internet-based election in 1998 [31]. University of Maryland student elections involve students entering their social security numbers and personal identification codes, then submitting their birth dates, and finally casting a vote.

One might assume that such a system would be secure, but it is important to realize that submitting one's identity for purposes of assuring voting eligibility can easily serve to identify what vote an individual has made. Even though it is assumed that such comparisons will not be made, it is important for a voter to know that they are technically possible. In addition, the vote-recording process is invisible to the voter; thus there is no reliable way of ensuring that propriety is kept.

The U.S. Court of Appeals for the Sixth Circuit recently heard NELSON v. MILLER, 1999 FED App. 0112P (6th Cir.), in which a blind man sued the State of Michigan on behalf of all persons who are unable to independently mark ballots given to them. Michigan, like many states, provides ballots to disabled voters and permits them to have third-party assistance in casting their ballots. Nelson argued, however, that Michigan's policy did not allow for his right to "secrecy of the ballot." The Court dismissed the case based on the fact that Michigan's policies did not violate the Americans with Disabilities Act of 1990.

However, the NELSON case is still germane to a discussion of electronic balloting. Clearly, electronic voting could have eliminated the case of action in NELSON v. MILLER, since adaptive technologies exist for computers that the Plaintiffs could have

individually acquired. Nonetheless, a computer-based voting system could have easily been construed, as discussed earlier, to violate any individual state's secrecy in election laws. By virtue of the fact that all voters, in effect, require the assistance of a third party – usually a private elections company, or even the computer staff of the local government – in actually casting a vote and not simply in its tabulation, electronic voting could be challenged. For the purposes of a challenge, all voters might be considered "disabled," in the context of the NELSON case, since they do not have the ability to actually cast their own ballots. Despite the dismissal of NELSON, future challenges would certainly not be unreasonable.

The security of an election is also critical. Even if an individual were able to physically cast his own ballot, the process requires additional precautions. In traditional elections, a person typically arrives at a polling place, confirms his name and address, and signs an affidavit in front of an election judge. That person is subsequently permitted to complete an anonymous ballot. Given that a person's address and similar information are easily obtainable by a third-party, identification of voters using current methods is inherently insecure.

A digital alternative could easily accommodate the same security measures, and could easily incorporate more reliable identification mechanisms. The inherent difficulty of computerized processing as compared with conventional voting is that, where physical mechanisms are in place to ensure anonymity, electronic precautions are taken with electronic voting. By their very nature, electronic operations on data are invisible to the user, and experts in the field confirm that the technology simply does not exist to authenticate transactions while ensuring the anonymity of the voter [32]. Therefore, even if a voting program stated that it kept identification information separate from voting information, an individual voter would have no way to confirm this.

In physical voting places, election judges are able to ensure the physical security of the vote and the voter. However, an electronic vote could take place in a person's home or office, at a library, in a shopping mall, or any multitude of locations, all without election judges. In these situations, it is impossible to determine whether a third party may be

observing or interfering with a vote, whether a vote is being electronically intercepted and altered, or even whether a voter is voting in the midst of an election campaign operation.

Notwithstanding physical security issues, the media have recently drawn attention to the so-called "cracking" of governmental and corporate Internet sites. While an idealist might hope that election sites would be immune from such interference, it is only realistic to understand that it is only a matter of time once Internet-based voting is implemented before such an event takes place. Although any well-designed Internet voting system would implement high-level security and encryption measures, even the leaders in Internet technology and security have not been untouched by this phenomenon. According to a recent article in Wired News, a leading Internet news service, major financial institution, NASDAQ had its Web site altered by attackers. Peter Shipley, a computer security expert reported in the article that the motive for such attacks has typically been publicity. However, it is not difficult to see how a political action group with sufficient funds could use the same tactics to perpetrate election fraud. Cracking into high-profile computer systems is trivial, and "how-to" guides even exist to teach a novice how to accomplish basic electronic vandalism.

Possibly even more dangerous has been a rash of "denial of service" attacks on Internet computers. With such tactics, a malicious attacker does not even need to have illegal access to a computer hosting an election to alter it, and attacks are even more difficult to detect and track. Instead, he and other legitimate voters for a particular candidate or issue could vote early, and then pummel the site with random traffic, so that the network and computer resources are taken up and no additional voters gain access. So far, the so-called denial of service "DoS" attacks have touched even the biggest leaders in electronic commerce: Wired News confirms that Internet giants CNN, eTrade, Buy.com and Yahoo! have been affected. Archives of defaced Web sites even exist in order to garner attention for the vandals. In DoS and traditional data-altering attacks, electronic voting is at an increased risk as compared to traditional voting, because a loss of the electronic data or a loss of access on the part of voters would be much more difficult to recover from.

There are clearly significant pitfalls in any implementation of electronic voting. In addition to malicious attacks on the computer infrastructure, we must deal with the legal issues surrounding this topic. To what extent can voting privacy and anonymity be ensured, and what measures must be taken to ensure the physical and electronic security of the election? In order for an electronic vote to become the norm in our government, these issues must be addressed and developed into policies, which will ensure that the newly formed electoral process can be beyond reproach.

2.12 Security Threats of a Modern E-Voting System

Just like other information systems, an electronic voting system is also vulnerable to computer attacks. Although Internet voting may improve several election factors, there are concerns that the benefits are overshadowed by the issues of many potential security threats. The security flaws are often concerning the voter's home computers and that these are the weakest link because people do not keep their personal computers secure [33]. Voters daily experienced some kind of virus infection to their personal computer Malicious Payload is a security threat to the voter's personal computer. The malicious payload is software or configuration designed to harm computers and this could be a Virus, worm, Trojan horse, or a remote control program which maybe the biggest threat in a voting scenario. If a malicious program is installed on a voter's computer it could secretly change the vote. The owner of the computer might be unaware of even having a malicious program installed because these programs can be difficult to detect (run in stealth mode). Malicious programs like these have advanced in sophistication and automation the past years in a way that they can do more damage, is more likely to succeed and disguise themselves better. Even though an Internet voting system has strict protocols for encryption and authentication, the malicious code can do its damage before these other security features are applied to the data.

Spoof sites are malicious web sites that are created to look like legitimate web site, and in a voting scenario we understand that this could be really bad, as the site could be used to launch phishing attacks to collect voters' credentials like a PIN or a password needed to cast a vote. The web site can look exactly like a government voting site, but redirect the voter's browser to a malicious web server. There are several ways that an attacker

could spoof a legitimate voting site. One way could be to send email messages to users telling the users to click on a link which would then bring up a fake voting site were the adversary could collect the user's credentials, steal the vote, and then use this to vote differently. An attacker could also set up a connection to the legitimate server and then feed the user with fake web page acting like a man in the middle, transferring and controlling all the traffics between the user and the web server. By transferring all the information between user and server, the user's vote can be altered before further sent to the server.

Another threat to Internet voting is Denial-of-service (DOS) attacks. DOS attacks are carried out by automatically sending a good of messages to website, a server, over a channel or similar, to make it crash or decrease quality because it cannot handle all the generated traffics by using a distributed DOS Attack (DDOS), attackers can cause routers to crash or election servers to get flooded, or it is possible to attack a large set of hosts for instance targeted demographically to cease the function of the election. This can be a significant threat to the Internet voting if for instance the voting occurs on a single day.

It is important to have extra bandwidth to handle the traffic. The voting can occur over several days in advance of the election.

As mentioned, not only the users host machines can be attacked by malicious intentions, also the election server could be the object of attacks. The server could not only be attacked by various malicious programs and software intruders like a DOS attack, but it can also be affected by physical intruders and physically factors like power outage.

2.13 Motivations of an E-Voting System

The motivations behind electronic voting are many. An improved system for counting ballots would speed up the process of counting, quicker display of partial or final result, and could reduce the errors associated with manual counting. People make errors, while computers don't, if configured correctly.

The use of electronic means to cast a vote has many advantages. Using an electronic voting machine for election would reduce the use of paper ballots, as the machine displays the ballot electronically. It would also make it easier to prepare special ballots

for other languages or visually impaired voters programmed into the system, instead of printing out several options.

The newest development in the area of e-voting is using the Internet for remote voting. By making it possible for voter to vote from his home computer, one of the goals is to improve the accessibility for disabled voters, as they don't have to actually go to the polling station. The overall participation would probably also increase because of the easiness of voting from home, and it would be more appealing to the youth doing the voting electronically.

The use of Internet for voting gives advantages both when it comes to speeding up the calculation of election results and regarding disabled voters. Remote voting also makes it possible to vote from your home computer, making it easier for disabled voters, and the electronic ballots can be adapted for people with a visual handicap (as with DRE-systems). This can increase the total participation in elections, not only for disabled voters but also for absentees. For instance people who travelled, in the military, students at college boarding would be able to vote.

Using computers for voting has many advantages, but a system for electronic voting requires means to preserve every aspects of a traditional voting scenario when it comes to security aspects like authentication, secrecy and anonymity. The system has to prevent attacks, errors and any electronic fraud.

2.14 Requirements of a Modern E-Voting Solution

A traditional voting scenario includes phases of preparing the election, setting up the lists of candidates and print ballots, identification/authentication of voters coming to the polling station to vote, checking the voter to the electoral roll, install the voting booth to let the voter cast his vote secretly and anonymous and be able to verify it (receipt), the secure transportation of all the votes (the sealed ballot boxes) to a secure location for counting, and of course for all this we need trustees (people we trust doing this, election officials).

Then there is the process of tallying where they have to make sure the counting and the results are correct, and keep an audit-trail for a possible recounting.

The requirement and challenge is to maintain some and improve some of these features in the electronic voting scenario. An electronic voting system with voting over the Internet should fulfill certain requirements and have features similar to a traditional voting system. The desirable properties of such voting systems are security, by auditability and ballot secrecy, as well as usability and accessibility. The step of trustees mentioned in a traditional voting scenario can be improved by involving complete mechanisms of verification, where the voter do not have to trust election officials or even system components (as described with end to end verifiable voting systems). An election model summary includes:

- Election Set up
- Ballot Casting and Recording (with audit possibilities)
- Ballot Tallying (with audit possibilities)
- Election Audit(s)

The criteria for a successful election system according to national workshop on Internet voting are stated below:

- Eligibility: Only eligible voters are allowed authentication to vote
- The eligible voter can only vote once (have one valid vote)
- Accuracy: Votes are recorded correctly
- Integrity: Votes cannot be altered or deleted
- Verifiability: The system has the ability to verify that votes are correctly counted
- Reliability: The system should work without compromising votes, even if system failures occurs
- Secrecy: Votes should be secret
- Flexibility: The system should be usable by different type of voters (support multilingual ballots, accommodate handicaps by audio or visual features)
- Convenience: The voting process should be convenient
- Certifiable: The system should be tested by election officials
- Transparency: Voters should be able to understand the system generally
- Cost: The system should not be too expensive

[34.]

A real-world Internet voting system has significant functional constraints.

Not only, as mentioned above should the voting process be convenient, it is a functional constraint that the voter should not have to interact with the voting system more than once to submit a ballot.

Another functional constraint, not mentioned above is regarding performance.

It is not enough for the system to have the requirements of accurately recording ballots; ensuring the integrity and secrecy of the ballots and so on, it also has to keep up in performance. Most ballots will probably be submitted during peak hours, but they still have to be processed quickly. And also, once the ballot box closes, the system has to provide and make the result available as soon as possible.

In a voting system, an issue of great significance is trust. An important part of creating a voting system is that it has to gain trust among the voters.

If the property of trust is not satisfied, there is no point of creating such a system. The success of a voting system relies on the public trusting the system.

According to a presentation at a NIST workshop, to trust a voting system is the same as assuming that [35]:

I. Procedures are followed as intended, count is correct.
II. A secure chain of custody is provided
III. Error free Software
IV. Secure Hardware
V. Secure Cryptographic Algorithms
VI. Trusted specialized user interfaces

With the introduction of end to end verifiable voting systems, especially cryptographic

End to end verifiable systems, the statement "I trust the voting system "is not sufficient. The possibility of verifying or audit any process of the voting system is a significant requirement to emphasize.

The Goals of a secure verifiable voting system is more like the following:

a. Cast-as-Intended
b. Counted-as-Cast
c. Verifiability
d. One voter, One vote

e. Coercion Resistance

f. Privacy

The end-to-end verifiable voting systems not only have to include earlier mentioned requirements of voting systems, it also has to include several processes of verification means. The voter should be able to verify that his vote is cast as intended, by auditing the process of encryption, that the vote is counted as cast, by verifying his vote is recorded in the system and by verifying election tally. Since the developments are heading against remote voting systems the coercion issue is a problem widely discussed, but as in earlier voting systems it has to be taken into consideration. We need receipt free verifiable elections.

A requirement that is not specifically included in the earlier mentioned requirements is the requirement of usability. A requirement of flexibility, regarding languages settings is included, and it is said that the voting process has to be convenient. It is important to emphasize the requirement of usability. In a presentation on the end to end NIST workshop a presentation specifies two desirable properties of a voting system [36]:

1. Security (Including auditability and ballot secrecy)
2. Usability and accessibility

The usability of a system lays the properties of the systems learnability and efficiency. Other important factor is the user satisfaction when interacting with system and if any errors occur in any steps or processes.

When having auditability as a requirement of a voting system, this introduces usability requirements. It is the voter that will be the one auditing his vote to ensure the correct functionalities of system components, and the system has to be usable for this even though the voter does not have any computer knowledge beyond normal. The learnability should be good by guiding the voter through steps of auditing. There is a tension between usability and auditability. The voter would probably need to perform some extra tasks to enable auditability, and at least these steps should be convenient and efficient.

Usability versus auditability issue regarding the voter were only mentioned, but there are three types of users the system should provide good usability for [36].

In addition to the voters, the system should provide a user-friendly setting for the poll workers or administrators of the elections. It is also desirable that public auditors audit the system and the elections, and to request this, a user-friendly environment has to be provided.

2.15 Internet Voting in Estonia

The user authentication for the Estonian voting system was builds on the country's national identity card. The national identity card used in Estonia is a smart card equipped with a computer-readable microchip, and by this not only function as a paper document but also as an electronic identity [37].

The electronic ID cards enable secure online authentication and is used to get access to the online ballot in an election. All a voter needs is his identity card, a computer, a card reader and PIN codes associated with his identity card to be able to vote from a computer anywhere in the world. The voter inserts the card into their computer, with a suitable adapter, and it allows them to authenticate to a government web site over an SSL-encrypted channel. PIN1 is used to authenticate the voting person, while after the voter has made his choice a second pin PIN2 is used to confirm the choice and sign. Electronic votes over the Internet can only be cast during the days of advance voting and on Election Day the voters, that has not voted electronic, have to go to polling stations and fill in a regular paper ballot.

To protect privacy and a free expression (against coercion), a voter can replace his vote as many times as he wants, with only the last vote actually being tallied [37].

The ability to cast multiple votes during a period will provide some resistance against bribery and coercion attacks.

A resistance against network attacks like a man-in-the middle attack can be provided by the use of Secure Sockets Layer (SSL) [37].

Secrecy of the Estonian voting system is based on a "double envelope" scheme, where the voter's choice is encrypted by the voting application and then signed digitally. Works like the voter seals his choice into an inner blank envelope and then puts the inner envelope into another envelope which he writes his name and address on. All the signed and encrypted votes are collected at the central site to check and make sure only one

vote per voter is counted. After this control, the digital signatures with personal data (the signed envelope) are removed and the anonymous encrypted votes (the last ciphertexts of each voter) are mixed together in a simulated ballot box. After mixing, these ciphertexts are sent to a tallying component for decryption and counting.

The scheme uses public key cryptography and the National Electoral Committee holding the private key, opens the encrypted votes collegially on the Election Day.

The Estonian voting system shows no protection against compromised client platforms.

The Estonian system does not really have countermeasures against any corrupt components. If the voter's computer is compromised the ballot information is visible to the attacker, and the attacker has the possibility of changing the votes. If the ballot box that collects or mixes the electronic votes is compromised, ballots can be deleted or room could be given for fraudulent ballots to be inserted.

In worst case, if the tallying device is corrupt it can decide the entire election result.

2.16 The Voting Over the Internet (VOI) Pilot Project in the US

Another example of an Internet voting system was a pilot program called Voting over the Internet (VOI) that was carried out in 2000 by the Federal Voting Assistance Program (FVAP) [38].

Their project was a test to see if votes could be cast in a reliable and secure manner using the Internet, and only included 84 volunteers in 21 states and 11 countries. How e-voting works: Voting over the internet.[39].

To make sure, and assure the volunteers, that their votes would be counted in the case of a failed experiment, each volunteer was also allowed to cast a traditional paper-based absentee ballot. The system was not designed to tabulate votes, only imitate established absentee ballot and cast these electronically over the Internet.

To carry out the pilot, each of the volunteers received a CD with a browser plug-in so they could display and transmit ballots to the FVAP servers. The Department of Defence (DoD) controlled a digital certification program to authenticate the voter identity, which they deactivated once a voter transmitted a ballot to prevent multiple casting of votes. The entire ballot, except the destination, were encrypted and then transmitted over the Internet to the FVAP server. The FVAP server was protected by keeping it in a secure

location with very limited access and uninterrupted power supply. In addition, two intrusion detection systems (IDS) were installed to monitor and detect any malicious activity.

At the local election sites the election officials used terminals to access a local election official (LEO) server that was connected to the FVAP server. The FVAP server transmitted the encrypted ballots addressed to that specific LEO site over the Internet, and once the ballots arrived, a computer at the LEO site could decrypt the ballots and print paper copies.

The VOI project was cancelled in 2004 due to concerns about security issues, and was never implemented.

The issues were regarding the voter anonymity being compromised or hackers intercepting and manipulating the ballots sent over Internet, and the Department of Defense would not approve of implementation.

Counting votes

The counting of electronic ballots is divided into three phases:

I. The cleansing phase
II. The mixing phase
III. The counting phase

The counting of paper ballots first involves a scanning process with manual verification, and then the vote is recorded electronically and to be counted the same way as an originally electronic ballot.

2.17 Recording and verifying electronic ballots

The electronic ballot box and other data collected by the Vote collection server is transferred securely using a storage device to a new system in a secure location for counting. This system is not connected to the Internet. The system components in these counting systems are only connected to each other, and cannot be reached from the outside.

The electronic ballot box, which is digitally signed to ensure its authentication and integrity, contains the digitally signed encrypted votes and cryptographic proofs generated by the voters.

In the cleansing phase the digitally signed ballot box is received from the Vote Collection Server, and the content is validated through some pre-established rules of the election. The digital certificates are validated based on the X509 standard. The cleansing process is executed in an air-gapped environment and it can import a digitally signed copy of the electoral roll.

The cleansing phase produces a digitally signed, cleansed ballot box (with only valid votes) for each municipality or county as defined in the election configuration.

Also the digital receipts from all the electronic votes in the digital ballot box are kept to allow voters to verify that their votes have reached the counting process.

After the cleansing phase, the digital ballot box is transmitted for the mixing service following some air-gapped approach.

In the mixing phase, the digital signature of the ballot box is first verified to check the authenticity and integrity. To check that all of the votes still belong to valid voters, that no rogue votes has been added or modified, then the digital signatures of the votes are also verified.

After these verifications, the digital signatures from the votes are removed so the votes now are anonymous. The votes are then processed by a re encrypting universal verifiable Mix-net which breaks any correlation between the votes and their voting order. The result or output of this mixing process is that all the votes are re-encrypted and shuffled, and in addition a set of cryptographic proofs of correct mixing behavior is produced.

After when the integrity of the mixing process has been validated, the thresh-old of all the parts of the secret key can be combined and votes can be decrypted by the Electoral Board. Then the list of all decrypted votes is digitally signed by the Electoral Board and forward for the counting process.

2.18 Recording and verifying paper ballots

The paper ballots are scanned in batches using optical scan technology. The scanning workstation consists of a document scanner connected to a computer installed with Read

soft Scan Software, and controlled by an operator. Optical character recognition (OCR) is performed real time to extract data from the images. The scan results in images in TIFF-format of the paper ballots and values extracted from the scanned images, which is transferred to another workstation for manual verification, called the verify workstation [40]

The verify workstation is installed with Read soft Verify Software, and is also controlled by an operator. The software installed can display uncertain results from the OCR, and the operator can make a judgment and then make decisions based on directions given by the Election Committee.

The resulting image files of the scan are transferred for electronic storage while the validated data are transferred to a Quality Assurance workstation for further validation.

In the Quality Assurance workstation, two separate scans are compared for validation to ensure correct results. The operator of the quality assurance workstation controls the results and can choose to discard the results if the two scans differ, or accept the results if the two scans produce an equal result. After the result is accepted the data are transferred to files in the same format as electronic votes. The data is now in EMLformat, identical to the data format from the electronic voting console and are exported, encrypted and transferred to a central collection server for counting.

2.19 Counting the votes

In the counting phase, votes are counted per candidate or party in order to create the results of the e-votes. This output is digitally signed by the Electoral Board and recorded in a removable device for being transferred to the settlement system. The system provides publishing of the voting receipts obtained from the e-counting process on a website. Voters can then individually verify whether their voting receipts are included on the published list.

2.20 Decryption and tallying

Because the Government should not have been able to trace a vote back to a voter, but at the same time they have to mark off against the electoral roll that the actual voter has cast a vote. The e-voting system is using a cryptographic double envelope scheme. The

process of a mix net can both prove the vote cannot be traced back to the voter and that no vote has been lost or changed in the process [41].

The systems also uses threshold decryption, meaning that the decryption key does not exist until the votes have been randomized (outer envelope removed) and cannot be traced back to voters. The decryption key is divided into several parts, shared by different parties of the election with different interests). When it is time to decrypt votes these parties in possession of the key shares, have to come to the secure location to combine the parts and create a usable decryption key. This key can then be used to decrypt (open the inner envelopes) and the votes can be counted.

After the decryption, the person identifiable ballots and decryption key is deleted, so no one afterwards can decrypt the person identifiable ballots and read the content of these signed ballots from voters.

The decryption service of the election system is a standard system consisting of a mix net followed by a verifiable decryption. No further details are published.

This decryption service decrypts all the ciphertexts and publishes the resulting ballots in a random order.

Auditors supervise the processes of encryption and decryption (as explained in the next section).

2.21 Auditing

As noted, auditing is an important mean to ensure every step of the election is working according to planned. Not only should the user verify his vote was correctly recorded by the system, he would also want to know that his vote was counted in the tallying process. All the processes of the system has to be audited, and in the Norwegian system auditors supervise that the recording and tallying of ballots are correct.

After the polls have closed the auditor receives:

1. The entire content of ballot box
2. A list of hashes of encrypted ballots (Generated or seen by the receipt generator)

Then the auditor can compute its own list of encrypted ballots that should be counted by the system.

The auditor verifies:

1. The content of the ballot box (signatures and proofs)
2. That no ballot has been inserted or lost, compared to the receipt generator list
3. That the list he has computed is the same as the list of ciphertexts inputs to the mixnet
4. The proofs offered by the mixnet and the decryption service

After verifying these points above, the auditor publishes hashes of every ballot. The voter can then also verify that his ballot was included in the counting process.

2.22 Authentication

The creator of a Governmental election system has to ensure that the election system has the necessary access controls needed to meet security requirements.

To get access to cast a vote from the election web site, the voter has to authenticate himself using an electronic ID to prove he is eligible to vote in the actual election.

As in the case of Norwegian electronic vote, a new electronic ID was developed based on a common identity provider (a PKI called Common Authentication Infrastructure (CAI)).

The authentication scheme is planned to include a national ID card (smartcard) together with a card reader, to let Norwegian citizen identify on the Internet. As with "MinID" this scheme also federates authentication, and CAI authenticates using the SAML 2.0 protocol. The system requires two-factor authentication, with a password to be used together with the electronic ID. According to, these passwords will be stored as "the hash-value of at least two secure one-way hashing algorithms" and a unique salt will be used when hashing each password [41].

Both voters and election administrators, as well as auditors has to authenticate to the system. These users will have different roles in the system, authorized to perform different tasks in the system.

If electronic ID was not developed and ready for the test project in 2011, authentication would have been done using "minID". By basing authentication on login using "minID", the voting system can then be sure that voter has voted.

To vote in the election the voter himself has to make sure he has "minID".

The system stores details about the voter authentication process and any certificate that was used. This and any stored additional information is digitally signed by the system, to guarantee its integrity and authenticity.

2.23 Threats, attacks and countermeasures

This section presents some of the threats of an Internet voting system and the countermeasures the any electronic voting system should hold. The voting system has to have countermeasures against several possible attacks.

"In practice, the two most significant security problems are compromised computers and coercion". No cryptography can protect a voter from coercion when voting from home or some public location, but the system should include features to hinder coercion. A "solution" to the coercion problem is the possibility of submitting multiple ballots. The system allows the voter multiple re-voting only counting the final ballot. It is also possible to vote at the polling station, and a paper ballot would overwrite any electronic vote no matter what timestamp (submitted before or after a submitted e-vote).

The previous matter is a measure against coercion from external "attackers", but coercion can also be done by election insiders or officials. A voter authenticates before casting a ballot, and the election official having access to the authentication system could detect any electronic e-voting by a voter.

The election official cannot see the content of the casted ballot, but it could see or detect the coerced voter casting a new ballot. A coercing election official having access to the counted ballots could also verify that the coerced voter (his victim) did not revote. If forcing the voter to submit a ballot with the desired effect the coercer can observe the counted ballots and check if the ballot(s) are present among these.

Compromised home come computers are the other significant threat. As mentioned earlier, a notable fraction of home computers are compromised, and there is need for a protocol to provide the voter with a possibility of detecting ballot tampering without relying on the computers. This is complicated since the voter cannot perform any cryptographic computations without a computer, and this is where the method of using a receipt generator and pre-generated receipt codes is involved. The voter receives pre-computed receipt codes on his voting card with his voting card and after casting a ballot,

the receipt codes generated by the receipt generator and the ballot box is sent to the voter not via the system and the computer, but through an independent channel (postal service). If a voter's computer is corrupt, the attacker can be able to see the voter's ballot, and the attacker can also modify the ballot. And therefore this security mechanism allows the voter to notice tampering with high probability.

The infrastructure is divided into a small number of separate players, based on technical measures, it can be assumed that an inside attacker can compromise at most one infrastructure player.

There is one attack model the cryptographic voting protocol implemented for "E-vote 2011" cannot protect against. Assume the following scenario:

If the voter's computer and for instance the receipt generator responsible for sending the receipt code to the voter are corrupt problems arise. The computer can send the voter's real ballot to the infrastructure, but the corrupt receipt generator can then delay the receipt code to the voter. In the meantime the compromised computer can submit a forged ballot to the infrastructure, leading to the computation of a new receipt code. The receipt generator can then discard this new receipt and the first computed receipt code is sent to the voter. The voter believes his ballot was correctly received, but is really replaced by a forged ballot.

The cryptographic voting protocol cannot protect a voter if both one particular infrastructure player and his computer are corrupt.

The e-voting protocol deployed for the Norwegian system will have a static corruption model, stating that an attacker may corrupt:

1. Any single infrastructure player and any subset of voter's computers
2. The receipt generator

In the election scheme the receipt generator will be so protected that it is very unlikely a possibility of it getting compromised.

In the description of attacks in the following section a simplified attack model is used. In this model an attacker may corrupt one of the following:

1. Any subset of voters and computers
2. Any Passively infrastructure player

(Meaning eavesdropping of compromising privacy, but no active operations.)

2.24 Attacker controlling Parts of the Infrastructure

In this section, based on the description of the voting protocol, explanation will be given on how the full protocol will defend against potential active attacks from the infrastructure players. Here the voter and the voter's computer are also included because they have roles of attack or verification purposes in the protocol.

Some of the active attacks the analysis mention could be:

I. Ballot stuffing by corrupt voter
II. Ballot stuffing by a corrupt ballot box
III. Corrupt ballot box falsely claiming that a given ballot belongs or corresponds to another voter than the correct one
IV. Corrupt ballot box using a corrupt voter to submit the ballots of honest voters as it owns, and then learns the ballot content from the receipt codes.

The countermeasure against active attacks from infrastructure players is based on all actors having to prove that they have executed the protocol as instructed. For instance, the voter's computer has to prove it has knowledge of the ciphertexts content and the ballot box has to prove the accuracy or correctness of its computations. As additional security measures to provide the integrity of a ballot and the sources, the use of digital signatures from a PKI hash functions are included.

If the receipt generator is corrupted it can leak the number of options on a submitted ballot, because the number of receipt codes is equal to the number of options chosen. But this is not discussed any further because the receipt generator will be well protected and a make compromise of this component quite unlikely.

To prevent a corrupt ballot box from inserting forged ballots, the mean of digital signatures is used. The voter, in cooperation with his computer, signs the submitted ballot with a digital signature from a PKI. The corrupt ballot box could create a fake digital signature, but does not the possibility of creating a digital signature correctly corresponding to this voter and his computer. The digital signature can also immediately prevent a corrupt ballot box of falsely claiming a given ballot to correspond to a different voter than it actually does.

The feature of digital signatures also prevents a corrupt voter from executing ballot stuffing. Using signed ballots, it is trivial to ensure that a voter can only register with one vote. "Any attempt to add rogue votes (digitally signed by untrusted digital certificates or voters not belonging to the Electoral Roll) is detected and prevented".

An eligible voter can of course cast as many votes as he like, but the digital signatures ensures that only one ballot is counted per voter.

If a corrupt ballot box using a corrupt voter as a fellow actor submits ballots generated by honest voters as its own, the ballot box can theoretically learn the ballot contents from the receipt codes generated. The countermeasure to prevent the chance of this is based on the computer submitting the vote(s) having to prove that it knows the content of every submitted ballot or ciphertexts.

Not only the computer, but also the ballot box has to prove self to prevent this attack. "The ballot box has to show the receipt generator the signed ballot and also prove that is computed correctly". By doing this the corrupt ballot box and voter cannot take advantage of the receipt generator' decryption capability to learn the content of honest voter's ballots.

The verification of the computation is done by the receipt generator based on the ballot box creating a proof of correct computation. To do this, the receipt generator needs see the entire ballot and know the voter's digital signature and the computer's proofs of knowledge (created as mentioned earlier).

First the ballot box receives the voter's encrypted ballot from the voter's computer, together with a proof and the voter's signature.

"To simplify the security proof, the ballot box also randomizes the ciphertexts.

This is done using El-Gamal encryption with a random public key as a commitment scheme (keeping the value hidden, bind until revealed).

Proofs of correct computation are created by the property that El-Gamal commitments are homomorphism, computationally hiding and unconditionally binding. A binding property means that when decrypted, we can know that the outcome is the same committed to originally.

After the ballot box has computed a proof of its computation of everything computed up to now is sent to the receipt generator. The receipt generator has access to the entire ballot information and verifies the voter's digital signature and every proof.

After verification, the receipt generator creates a hash of the ballot and returns this signature to the ballot box which is instructed to forward the signature to the voter's computer.

The voter's computer will not inform the voter that the ballot has been accepted before receiving this signature. If the ballot box for some reason discards a voter's ballot, the voter (together with an auditor) can prove his ballot was discarded. When receiving the signature the voter's computer "forward" this and a hash of the encrypted ballot to the voter.

There are also security issues that would certainly be detected, but that is hard to do anything about. A corrupt infrastructure player would usually cause suspicious integrity failures and thereby stop the election. The Norwegian election system's countermeasures to detect such attacks are based on verification of the processes and components with digital signatures.

If an attacker controls any of the infrastructure players, he can make the corrupt infrastructure player halt and thereby stop the entire election.

The system's solution against attacks that brings down the election system might be the use of an N-structure architecture, or the possibility of advance voting over a period of time so a system breakdown or corruption can be checked and does not ruin the entire election. The scenario of an attacker controlling network or parts of it is discussed in the section below.

2.25 Attacker Controls Network

An external attacker or organization can be able to compromise a number of voters and a large number of computers, and thereby launch network attacks (like a DOS attack described in this thesis). An attacker controlling a large amount of computers can perform a DDOS attack to bring down the election server or other system components, by generating a such a load of traffic that the components cannot handle the legitimate

traffic of ballots or other requests, or the components respond so slowly they are rendered unavailable.

A DOS attack can prevent the election web site or systems components from functioning efficiently or functioning at all, both temporarily and indefinitely.

If an attacker controls the network between a voter's (or several voters') computer(s) and the election infrastructure he can also delay or block the submission of ballots.

To decrease the efficiency of a DOS attack, the Norwegian election system allows the voter to vote in a 3 month advanced period, making it harder to launch a DOS attack. In addition, to reduce the damage of such an attack, the system is considering having an N-version architecture, in any parts of the system it is possible (Christian Bull, security E-vote "2011"). By doing this there would be N versions (N being larger than 2) of a system component working in parallel, making it harder for an attacker to affect the system performance.

The use of an N version architecture, where the difference could be made by different contractors would also provide a better and more accurate election result. If one of the versions presents a result that differs from the majority, it can be assumed this version has an error and the result can be excluded.

2.26 Summary

Those who cast the votes decide nothing while those who count the vote decide everything.

Simultaneous vote verification is not possible and this makes electronic voting verification not error and fraud free.

Voting receipt as a method of verification of electronic vote is not supported by international electoral law standard and system’s trustworthiness and secrecy is hard to overcome.

SMS was sent as soon as a voter casts his or her vote during Norwegian Internet voting as a method of verification. The SMS contains the party code of which the voter did cast the vote and number of people that did cast vote for the party candidate.

This is not a perfect verification method as the voter did not get to know number of votes his or her preferred party candidate had before casting his or her vote.

There has not been perfect and transparent method of internet voting verifiability method so far.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

Internet voting could represent an effective way to improve the accessibility of voting, and contribute to an increase in electoral turnout amongst the young people. But while the internet is sufficiently safe for conducting bank transactions, this is not yet the case for politically binding elections. However, with research into the areas of concern progressing quickly, that will not be the case indefinitely.

Internet voting has the potential to provide efficient elections with higher voter participation, better accuracy and lower costs as compared to the current manual methods. People who have used internet banking and internet shopping know the convenience provided by the internet instead of standing in queues. One of the major areas of concern in internet voting is for the voters to be able to verify that their votes are counted as voted for the candidate of their choice.

This chapter provides a detailed description of the research method of achieving the objectives discussed in chapter one. The system consists of four distinct component parts:

1. Data Capturing Interface (for voter's registration).
2. Vote Capturing.
3. Vote Processing
4. Output and verification system.

The voter registration process may seem simple to most voters. They give their names, addresses, birth date, and in some cases party affiliations to election officials with the expectation that they will be able to vote on Election Day. In reality, election officials must oversee a complex system managing this process. They must ensure that the voters' information is accurately recorded and maintained, that the system is transparent while voter information is kept private and secure from unauthorized access, and that poll workers can access this information on Election Day to determine whether or not

any given voter is eligible. A well-managed voter registration system is vital for ensuring public confidence in elections. State and local governments have managed voter registration using different approaches among different jurisdictions.

The system's data capturing component handles the electoral registration stage; it captures information that are unique to individual electorate like; First name, Middle name, Last name, date of birth, Sex, State of Origin, Religion, Phone Number, e-mail address, National Identity Number, passport photo and finger Print (Biometric data).

While technology will help election officials manage this complex system, it also creates new risks that must be addressed.

3.2 Data Capturing Component of the System

Data capturing system could be automatic or manual type. Automatic identification and data capture (AIDC) refers to the method of automatic identifying objects, collecting data about them, and entering that data directly in to computer system without human involvement. Automatic identification data capture technologies include bar codes, Radio Frequency Identification (RFID), biometrics, magnetic stripes, Optical Character Recognition (OCR), smart cards and voice recognition. AIDC is also commonly referred to as Automatic Identification, "Auto-ID" and "Automatic Data Capture"

Data capture component of the system obtains external data such as text and images for analysis. To capture these data as shown in figure 3.1, transducer was employed which converts the actual image into a digital file. The file is then stored and at later time it can be analyzed by a computer or compared with other files in the database to verify identity or to provide authorization to enter a secured system for vote casting. At this voters' registration stage, individual's data is captured on the data capturing system. This system allows voters bio-data to be captured and stored in the central database system. Biometric security system is employed at this stage to prevent multiple registrations and discourage election fraud.

The biometric security system captures or acquires human unique characteristics such as finger image, palm image, facial image, iris print or voice print which involves audio data while other characteristics involve video data. The type of human characteristics

that is captured by this system is finger image. Once these data are captured and submitted in to the data base, it triggers an algorithm in which the server automatically generates a unique identification number for each registered user which will be used with the unique national identity number as access or authentication keys to the voting platform.

Transducer Block Diagram

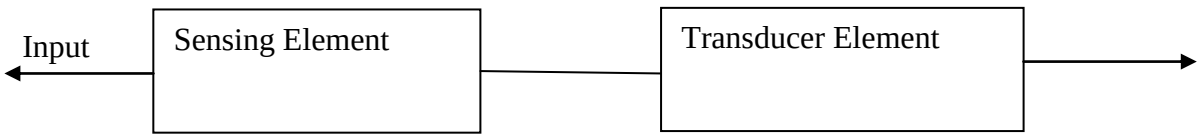


Figure 3.1. Data capturing system Transducer block diagram.

The sensing element of the transistor senses the physical quantity (image) or its rate of change and responds to it. The output of the sensing element is passed on to the transduction element. This element is responsible for converting the non digital signal to its proportional digital signal.

3.2.1 Biometric Data

Biometrics refers to the quantifiable data or metrics related to human characteristics and traits.

Biometric identification or biometric authentication is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance.

This data capturing system has biometric identifier which is distinctive and has measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological and behavioral characteristics.

Physiological characteristics are related to the shape of the body. Some examples include fingerprint, face recognition, DNA, palm print, hand geometry, iris

recognition, retina and odour. Behavioural characteristics are related to the pattern of behaviour of a person, which includes typing rhythm, gait, and voice. Some researchers have coined the term behaviour metrics to describe the latter class of biometrics.

Figure 3.2 describes how a physiological characteristic is presented as a means of identifier by the electorate at a point of registration. The data capturing system captures the biometric characteristic presented by the electorate, processes it with the help of transducer and store it at the time of registration. When is time for electorate to cast the vote, he present his biometric character for access authentication, the system compares it with the stored character at registration; if it matches, then the system validate the voter and allow access to the digital ballot page.

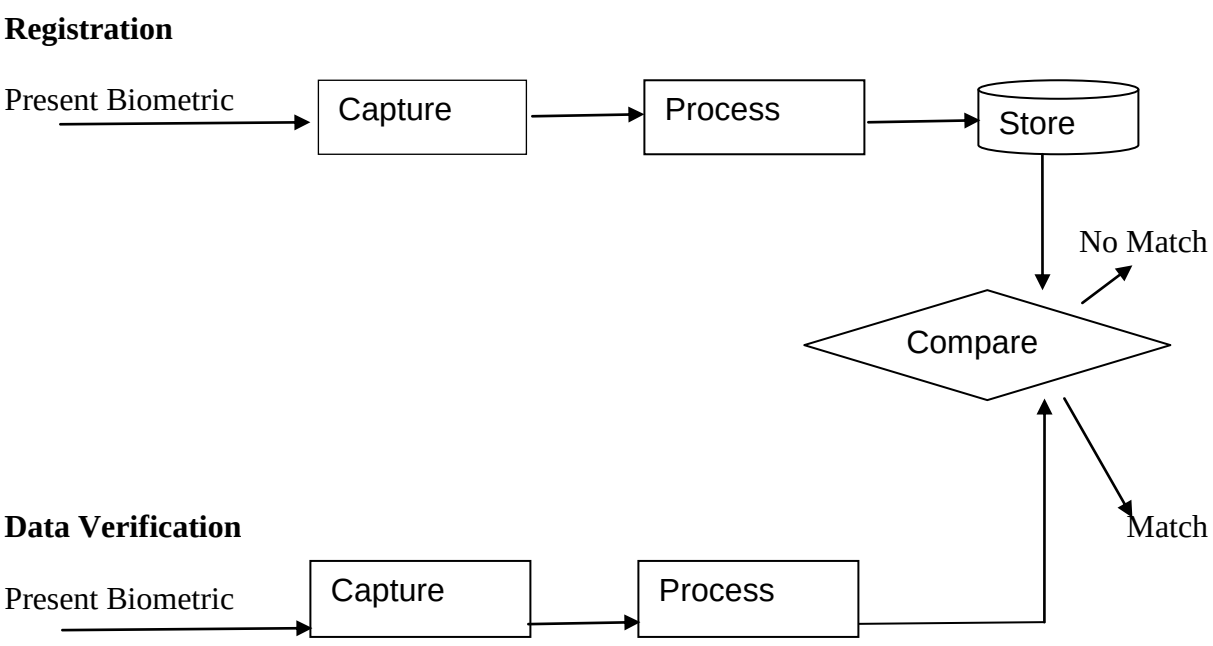
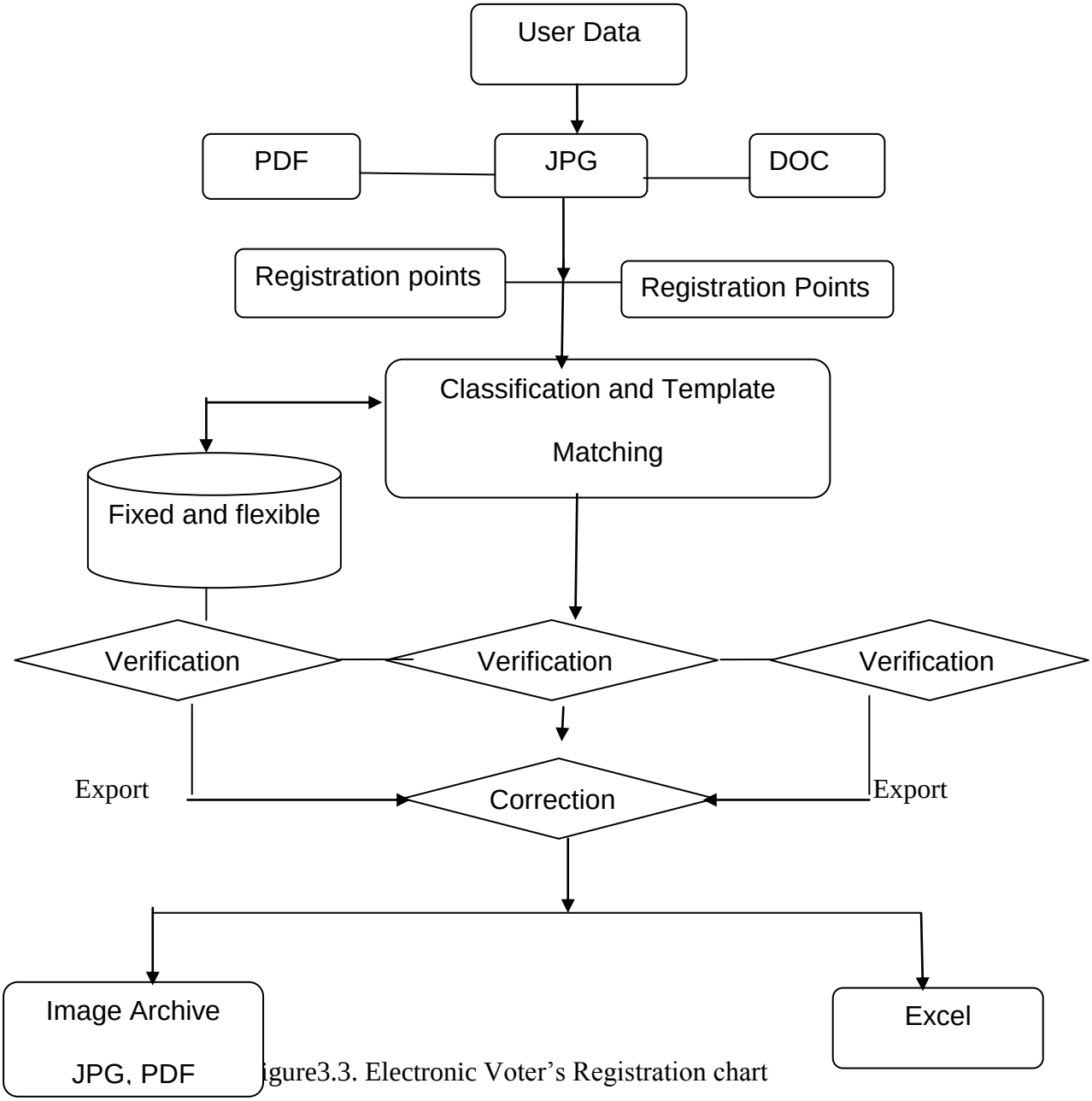


Figure 3.2. Biometric data capturing chart

3.2.2. Electronic data Capturing form

Electronic data capturing form is a soft document that contains relevant data boxes or text field for candidates to enter their personal data which after submission it goes to the database for future reference. For internet voting data capture form, data to be captured from voters includes First name, Middle name, Last name, Sex, Date of birth, State of origin, Nationality, Religion, electronic mail address, Phone number, Passport Photograph, National identification number and marital Status.



igure3.3. Electronic Voter's Registration chart

3.3 Voter's Unique Identification Number/ Registration Number

Electronic voter's registration is done by filling electronic form. Once the online form is filled by eligible candidate (the candidate that meets up with the age requirement) and submit-button is clicked, the system automatically generates a unique random number. This unique random number is one of the primary keys for accessing electronic ballot windows where voter will cast the vote.

The system is designed in a way that once a particular registration number is used with respect to the corresponding national identity number to access a voting platform and vote is cast, such a number will be recorded in the system while additional attempt by same voter for multiple votes will be denied. This is done to checkmate electoral fraud, boosts the trust of electorates in the system and makes it more acceptable.

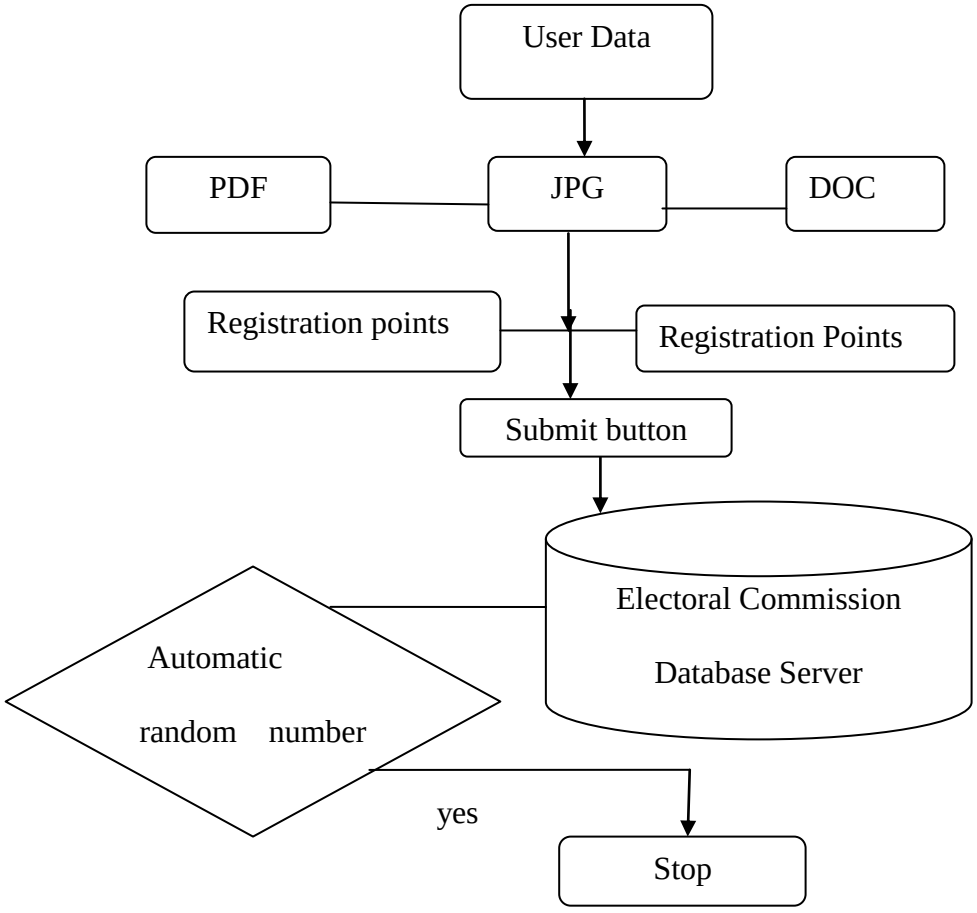


Figure3.4. Voters random registration Number chart

Figure 3.4 explains how the random number is automatically generated once the registration form is submitted. This registration number will be sent to the registered voter through the voter's email address and phone number.

The generated unique registration number is stored in a table known as admin in the database and map to the corresponding national identity number for each registered voter. The table (admin) has two fields known as Registration number and National identity number; these two unique identifiers with biometric character will be used for access in to electronic or virtual ballot form.

.

3.4 User authentication

User authentication is the process of verifying the identity of a user to establish whether someone (or something) is what it claims to be.

Authentication technology provides the basis for access control in computer systems.

A user has to authenticate to a system to convince the system of his identity before the system grants the user access to system resources.

In private and public computer networks (including the Internet), authentication is commonly done through the use of secret login passwords, but sometimes it also requires stronger security with accompanying mechanisms.

This can be the use of smart card, generated PIN codes, certificates, etc.

Sometimes it requires that the user's computer also verifies its identity together with the user.

User authentication methods are divided into three categories:

1. What you know
2. What you have
3. What you are

What you know is the same as providing a password or a PIN code. What you have is regarding the use of a token you possess, like the extra mean of a card reader or a code calculator. The identity is then based on possession of some object, often also combined with a password. What you are means identity verification based on physical characteristics or involuntary response patterns known as biometrics.

This can be fingerprints, speech, signature, face profile and more.

In a voting system, as with any computer system to handle personal information, authentication is an extremely important mean to ensure the correct function of the system and gaining the user's trust. The obvious mean is that the user has to authenticate to cast a vote in the system, but is also desirable that the vote recorder authenticates to the user so that the voter would know it is not a false or phishing site system claiming to be the voting system.

3.4.1 Password Authentication

To access the system as shown in figure 3.5 and figure 3.6, the user will supply his login name, password, and then the identity of the user is verified by checking that he has provided the correct password.

The passwords are usually not stored in the clear, to avoid a compromise of all the users of a system in the case of intruders.

A secret password scheme relies on the user to carefully select a strong password to reduce risk of exhausted search.

Passwords transferred over an insecure network (wireless network, Internet) are vulnerable.

3.4.2 Smart Cards Authentication

Smart card in authentication context is a type of token-based authentication where the token is the plastic card containing a microprocessor, that the user possess. The smart card chip can contain specific user authentication information coded that can be recognized by the system, and work like an electronic ID. This can be used to gain access to systems as well as for digital signing purposes.

To authenticate using a smart card, the user at least needs his card and a card reader that can interface with a computer using a USB port. The smart card chip can store multiple identification factors like password; fingerprint which when put into the card reader it can implement multiple factors of authentication providing two-factor authentication (for instance the card information and the user’s password or pin code).

In a smart card authentication scheme, the card reader and the user's computer can communicate with the microprocessor.

The microprocessor controls the computer's access to the data on the smart card. The data on the smart card can be encrypted, and additionally a password can be employed to prevent unauthorized reading of the data. The interaction between the user's computer include steps to determine if the card is authorized to be used in the system, and checks if the user can be identified and authenticated.

.

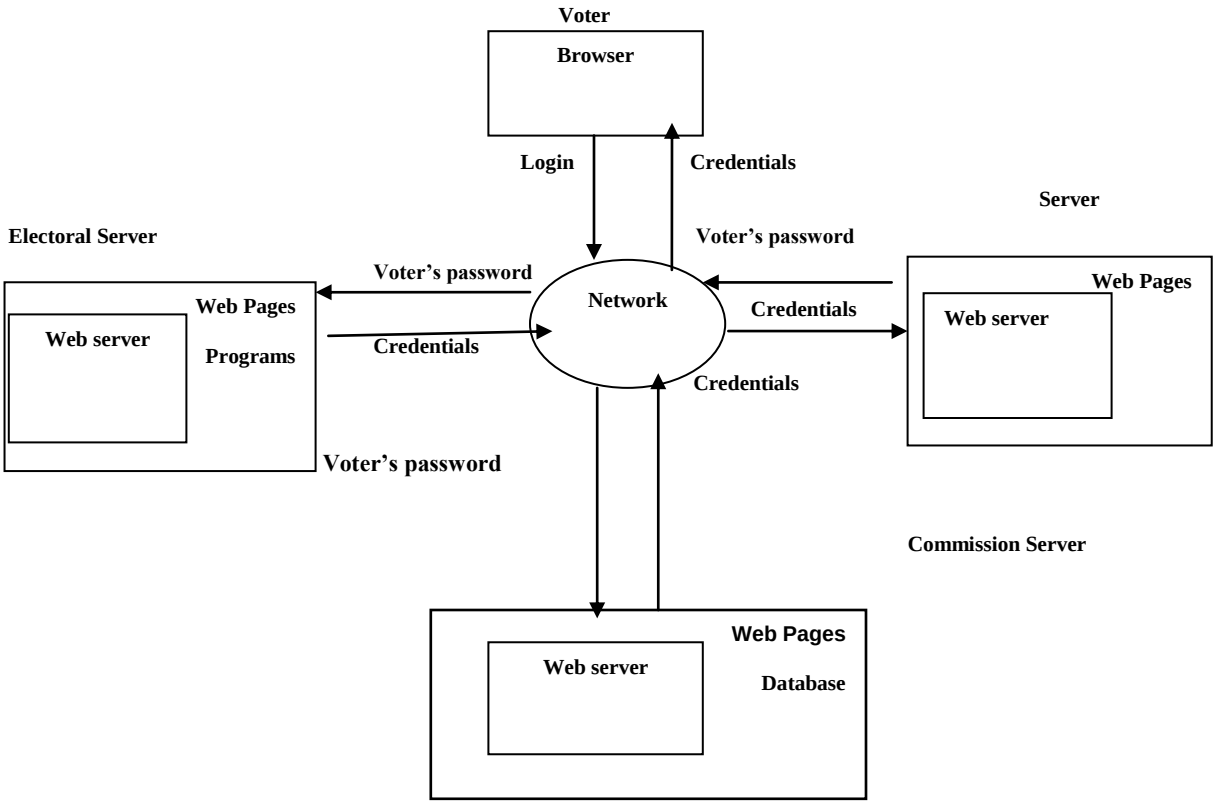


Figure 3.5. Voter's password Authentication

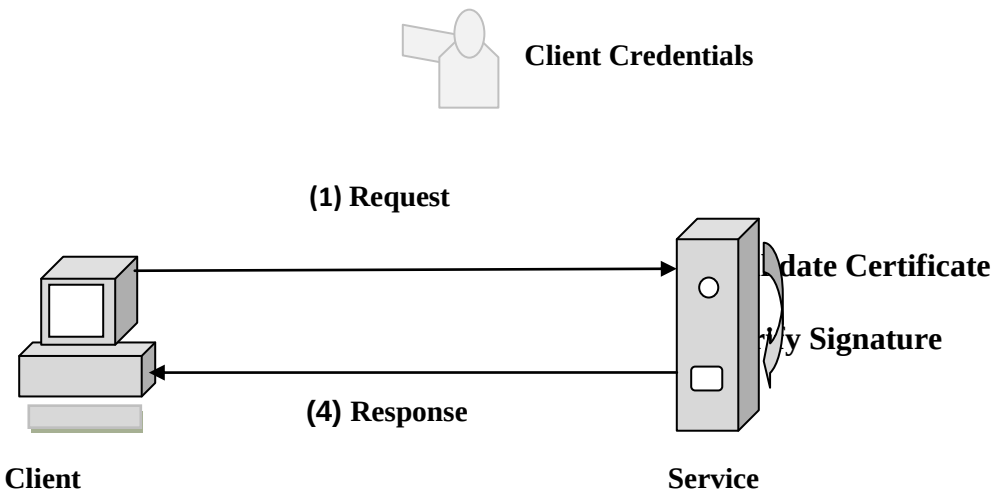


Figure 3.6 Password Access control

3.4.3 BankID Authentication

Bank Identity is a mean to provide digital signatures and identification of a user on the Internet. It works as an electronic ID when the user logs in to a resource with BankID, and can work as a digital signature when used to sign a deal or perform for instance a money transfer. BankID can be seen as a substitute for a Public Key Infrastructure. The mechanism is widely deployed by Norwegian banks and approximately 2.5 million people users have a BankID.

To authenticate with BankID, the user have to provide his social security number, together with a code retrieved from a security card and a personal password chosen by the user. The security card can be a plastic card with pre-printed codes, an electronic code calculator generating security codes, or a card used together with a card reader.

The technology is based on PKI, using key pairs (one private and one public) for security functionalities together with a digital certificate for electronic ID.

The authentication scheme is shown in Figure3.6.

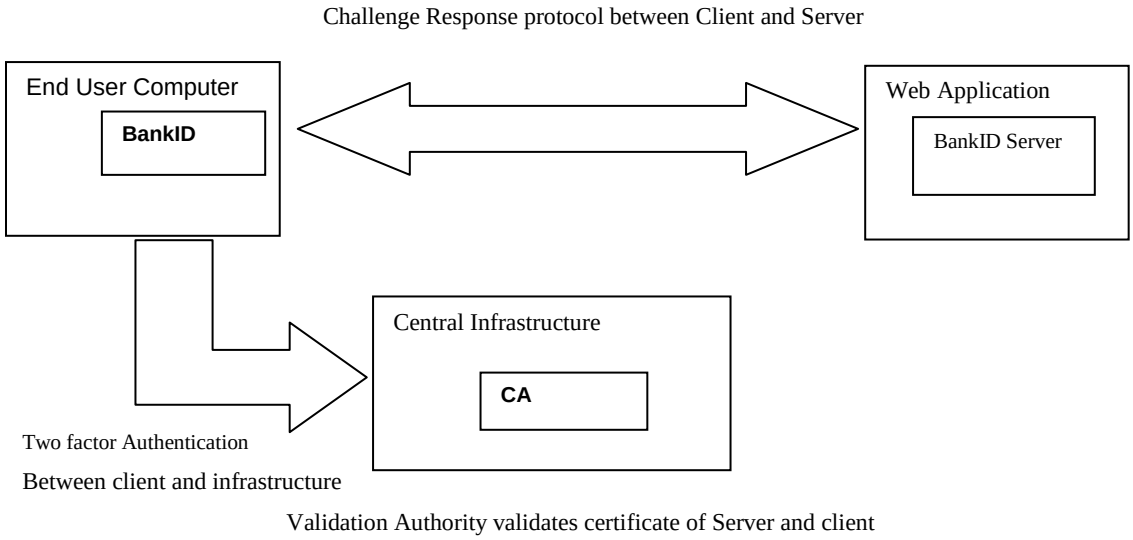


Figure 3.7. The BankID Authentication Procedure

The user's keys are stored in the central infrastructure, and the certificate authority (CA) creates signatures on behalf of the user when this is requested.

To make the CA create signatures, the user must authenticate self.

This is done through a two-factor authentication where the user provides a password and a onetime pin (from the security card or generated by a code calculator).

3.4.4 Biometric Authentication

Biometrics is physical characteristics or involuntary response patterns.

Authentication by biometrics verifies the identity based on some of these characteristics, including signature, fingerprint, speech, face profile and so on. Biometrics provides a very high level of security because the authentication is directly related to a unique physical characteristic of the user which is more difficult to imitate.

The unique pattern that identifies a user is formed during an enrolment process, producing a template for that user. If a user wants to authenticate to a system, a physical measurement is done to obtain a current biometric pattern for the user.

This pattern (for instance a fingerprint) is then compared against the enrolment template to verify the user's identity.

Smart cards can provide me mechanisms to securely store biometric templates and perform biometric matching functions. These features can be used to improve privacy in systems that utilize biometrics. For instance, storing fingerprint templates on a smart card rather than in a central database can be an effective way of increasing privacy in a single sign-on system that uses fingerprint biometrics as the single sign-on credential.

The simplest pattern to use for authentication is the fingerprint, and this is used for check-in at some airports. Then, the only computer connected to the airlines system, biometrics software and a fingerprint scanner is needed to authenticate.

In Bulgaria, biometric authentication to voting schemes has been introduced, and thereby calling it biometric voting [42].

The mechanism was introduced to make it impossible to vote with some other persons voting card. The electronic voting machine at the polling stations authenticates the user with biometrics using a connected finger reader.

3.5 Vote Capturing System

The vote capturing system is the part of the voting system that presents the platform for eligible voters to cast their votes. The electronic ballot interface present voter authentication phase to electorate requesting for voter’s registration number, national identity number and finger print as access control mechanism. Once the access is granted, the voter is presented with the list of political parties from which the voter will check the appropriate party representing the candidate of his choice.

At this stage, once the voter gain access to the voting platform; he sees the number of votes each contestant has gotten so far before casting his vote. After casting his vote and click submit button, the system refreshes and shows increase in the number of votes of the candidate he did cast his vote for and then gets short message service (sms) confirmation as verification means.

3.6 Electronic voting system Description

The electronic (internet) voting system includes all the four phases of an election process; necessary preparations before the poll, the actual voting process, counting of votes during and after closed poll and the settlement.

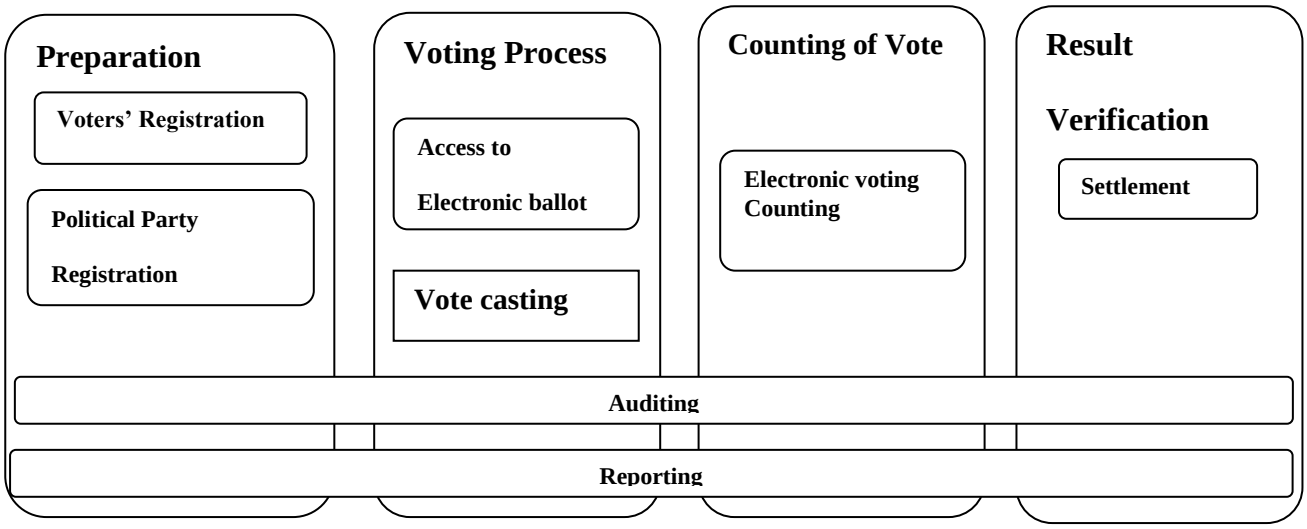


Figure 3.8. Election Life Cycle

The system has mechanisms to audit every phase of the entire election, to ensure everything works as intended. The overview of the four phases are showed
In figure 3.8, but counting and settlement will not be further covered in this thesis.
In this chapter the e-voting system is described, including authentication mechanisms and the voting protocol.

3.7 Internet Voting Architecture

The Internet voting system is a system that employs the use of electronic ballots.
The system offers the voter two options on how to cast his vote; through a computer set up at the polling station, or from any remote personal computer, GSM and PADs connected to the internet.

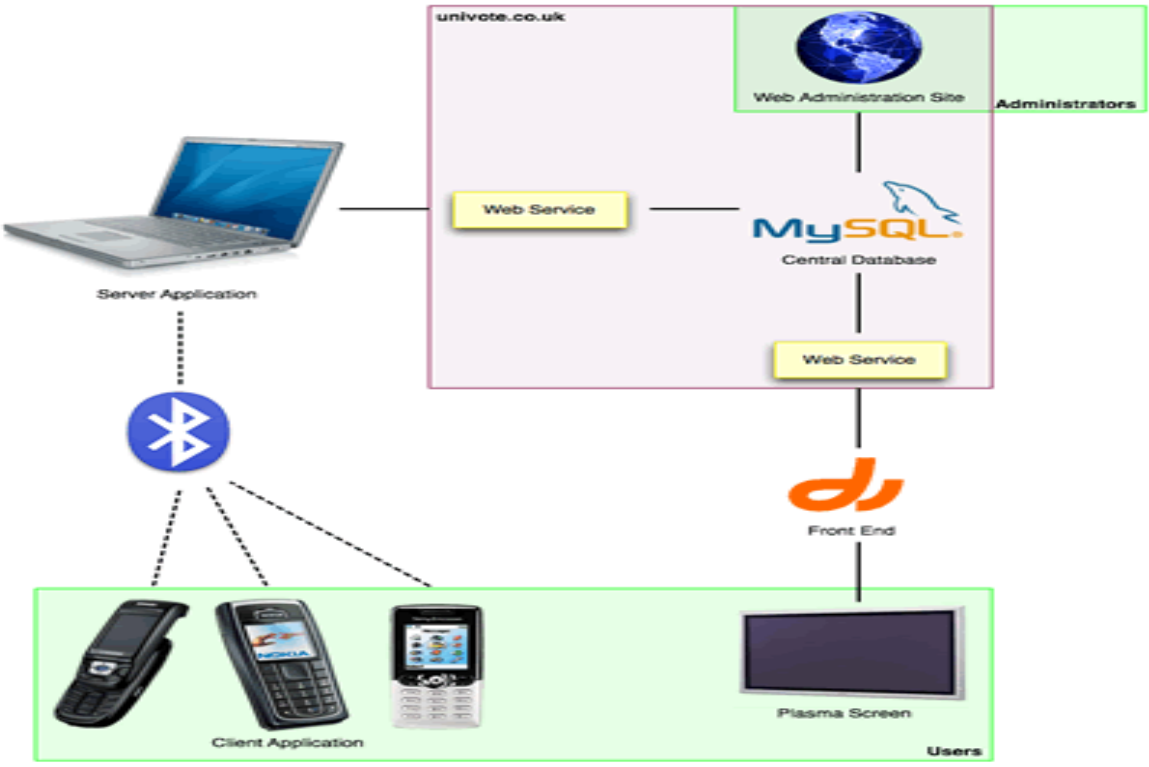


Figure 3.9 Cooperate e-voting system

Figure 3.9 shows the cooperation of the electronic voting system, including electronic voters casting ballots from computers and phone from both controlled environments (polling station) and remote locations, and e-counting.

3.8 Electronic Voting process

The process of casting a vote in the electronic voting system starts with the voter filling the online form and receiving a voting registration number by e- mail some time ahead of the election period. The e-mail contains all the necessary information like voter registration number and national identity number for accessing electronic ballot where voters cast vote.

When the period of the voting online opens, an eligible voter can use his browser to visit the election web site to cast a vote.

The voting processes are as listed below:

1. The voter provides his electronic identity credentials and the voting application (Voting Client) authenticates the voter to the voting server.
2. The Voting Client displays the list of parties which represent candidates in the election the voter has permission to participate.
The voter mark options to issue his choices for party of the preferred candidate.
3. When issued his choice of candidate or party the voter clicks to submit his or her vote. Once this is done, the electronic page displays updated result and sends bulk messages to all voters indicating who has just voted and each party's latest number of votes.

3.9 The voting protocol

An Internet voting system depends on a secure and robust cryptographic protocol. Security of the protocol is the necessary factor to get people to trust the voting solution. In this section I will explain a simplified Internet voting protocol to be implemented in the electronic vote solution. The cryptographic protocol is invisible to the voter; to cast a vote, as already described, the voter uses his computer to submit a vote to the election infrastructure and then receives a feedback of updated votes to verify his vote.

It is the voter's computer that encrypts the ballot and submits it to a ballot box in the election infrastructure. The crypto-protocol has to have functions to allow the voter to submit repeatedly ballots consisting of a sequence of options chosen from a set of options to the infrastructure, prevents multiple registration by a single voter and casting of double votes by a single voter for same candidate. The essence of this is to prevent election fraud.

voter_id	1	2	3	4	5	6
first_name	John	Musa	James	Mariam	Habibat	Comfort
middle_name	Peter	Issa	Paul	Fati	Carol	Jane
last_name	Joe	Aliu	Scole	Aliu	Usman	Mark
date_of_birth	21-05-80	02-11-78	23-03-83	13-08-82	10-09-65	24-02-79
Sex	Male	Male	Male	Female	Female	Female
state_of_origin	Lagos	Kano	Imo	Sokoto	Niger	Oyo
Nationality	Nigerian	Nigerian	Nigerian	Nigerian	Nigerian	Nigerian
Religion	Christian	Islam	Christian	Islam	Islam	Christian
national_id_no	62344555	87349703	15628793	34217854	98765021	87041287
Phone_no	01234455	05134568	03456721	04876540	07896543	02134569
Email	jp@aol.com	mia@ymail.com	jscole@aol.com	faty@aol.com	carol@aol.com	jane@aol.com

Table 3.1 Sample voter registration table that captures voter's registration details

3.10 Electronic ballot Authentication form/ Virtual ballot Authentication Form

The electronic ballot authentication form (virtual ballot authentication form) is the access control to voting platform through which electorates cast their votes online. This page has access control fields that require national identity number, voter registration number and finger print for authentication.

The sample form below shows what the authentication page looks like.

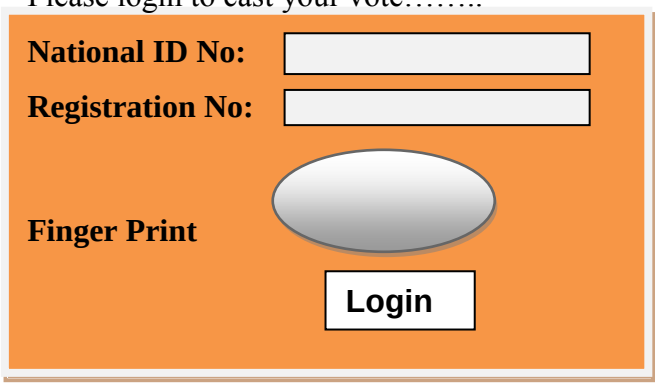


Figure 3.10. E-ballot authentication form

3.11 Access Control (Admin) table:

The admin table (Table 3.2) stores all the registration numbers with their corresponding national identity numbers and finger prints for session authentication.

admin_id	registration_no	national_id_no	Finger Print
1	NEC67889GT	NG47891234	
2	NEC78904MH	NG55723149	
3	NEC23784JY	NG90833126	
4	NEC72408YT	NG01284568	
5	NEC93578JY	NG10230498	
6	NEC70982HY	NG20134189	
7	NEC67894JU	NG32076840	
8	NEC23876HI	NG02321340	
9	NEC09871JM	NG32098972	
10	NEC56782M N	NG31276290	

Table 3.2 Admin Table

3.12 Secure login attempts

Secure login attempt table (Table 3.3) captures number of time an electorate has successfully logged in to the electronic ballot form. The table has two fields namely user id and number of time logged in.

user_id	No of time

1	1
2	2
3	1
4	0
5	1
6	3

Table 3.3 Secure login attempts table in the database

3.13 Global configuration

The global configuration file contains global configuration variables. Things like whether anyone can register, whether or not it's a secure (HTTPS) connection as well as the database details are contained in the global configuration file. It is designed to filter access.

3.14 The Login function on the electronic ballot form

Login function is an application that monitors the voters input in to the text feeds provided by the electronic ballot access control page. The application checks if the voter has put all the right credentials by querying the admin table in the data base for credential confirmation. If all the credentials are correct, it grants electorate the access to the electorate ballot page

Please tick the box for your choice candidate and click show updated results to cast your vote

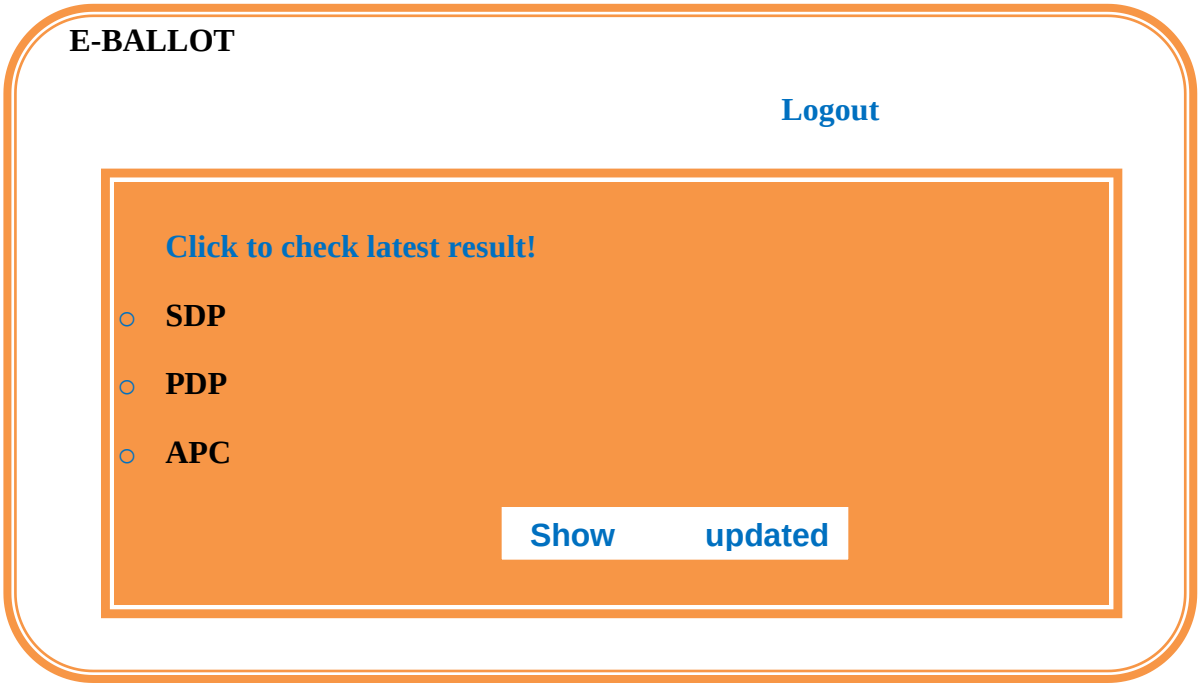


Figure 3.11. e-ballot

3.15 Poll Table

```
CREATE TABLE `evote`.`poll` (
    `party` VARCHAR(30) NOT NULL,
    `votes` int(30) NOT NULL
    )
ENGINE=InnoDB Script
```

Party	Votes
Sdp	
Pdp	
Apc	

Table 3.4 poll table

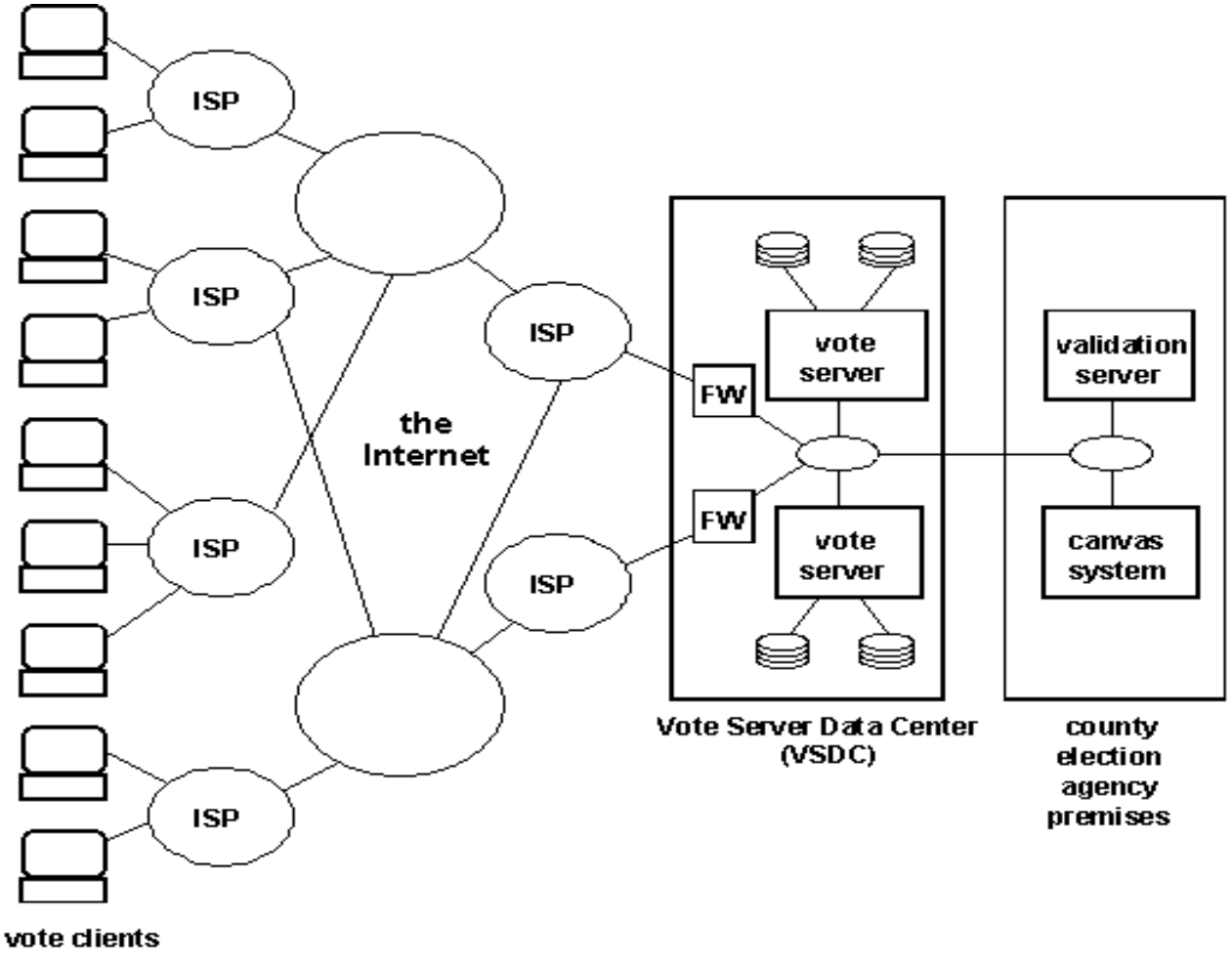


Figure 3.12 Network Topology for internet voting system.

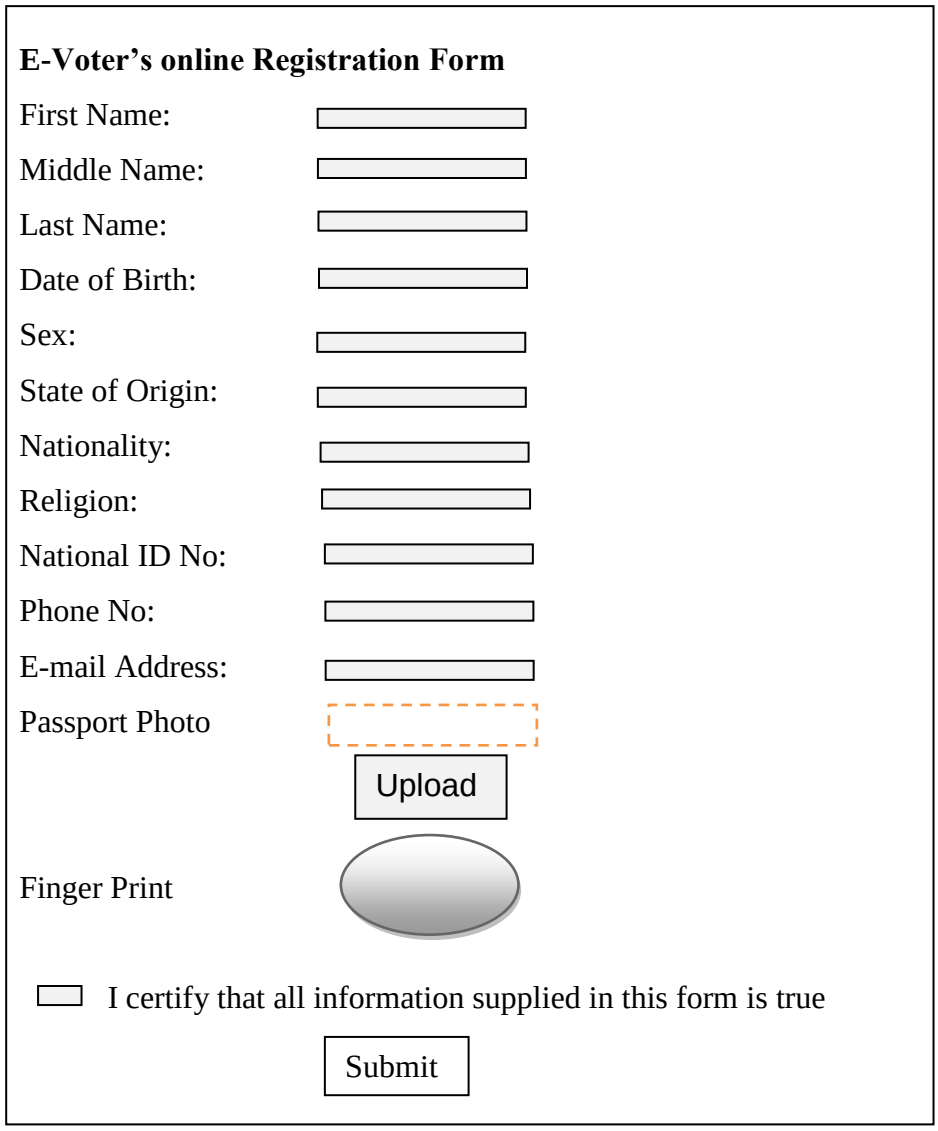


Figure 3.13 Internet voter's registration form

Figure 3.12 describes the network topology of the internet voting system. Vote clients are voters' computers that run application which access the electronic forms on the vote server through their various internet service providers (ISP). The validation system validates electorate votes on the central database system while canvas system quarries the central database through the validation system to update the result.

Figure 3.13 is a sample electronic registration form which is the first stage in every election. Once the voter fills all the form fields and hit the submit button, it submits the form and the system generates a unique voter's registration number.

Figure 3.10 is the authentication form which gives access to voting section. National ID number or social security number, registration number and finger print are used as primary keys to avoid multiple casting of votes.

Figure 3.11 is the form section where voter casts his or her vote and verifies that his or her vote counts. This page gives voter updated number of votes cast for each contestant before he or she casts the vote and refreshes once the voter casts his or her own vote to give the latest update.

3.16 System feature

The system captures all the biometric characters, National identity numbers of eligible voters and maps it to individual's given registration number. The system is designed to prevent multiple voting by querying the database once the voter clicks the vote button and check if same credentials (Finger print, National identity number and registration number) have been used earlier to cast vote.

An integrated System application with backend database and support for multi-computer programming languages for update feedback and is used for the design of electronic voting system.

Security is the key feature of this system so as to prevent fraud.

3.17 Chapter Summary

Internet voting could represent an effective way to improve the accessibility of voting, and contribute to an increase in electoral turnout amongst the young people. But while the internet is sufficiently safe for conducting bank transactions, this is not yet the case for politically binding elections. However, with research into the areas of concern progressing quickly, that will not be the case indefinitely.

The voter registration process may seem simple to most voters. They give their names, addresses, birth date, and in some cases party affiliations to election officials with the expectation that they will be able to vote on Election Day. In reality, election officials must oversee a complex system managing this process. They must ensure that the voters' information is accurately recorded and maintained, that the system is transparent while voter information is kept private and secure from unauthorized access, and that poll workers can access this information on Election Day to determine whether or not any given voter is eligible. A well-managed voter registration system is vital for ensuring public confidence in elections.

A user has to authenticate to a system to convince the system of his identity before the system grants the user access to system resources (Voting platform).

In private and public computer networks (including the Internet), authentication is commonly done through the use of secret login passwords, but sometimes it also requires stronger security with accompanying mechanisms.

This system requests for voter's National identification number and unique given voter's registration number given during registration for voting access.

One of the major concerns of remote voting in general is the lack of means for the voter to verify the correct reception and count of his or her vote. The introduction of remote electronic voting needs provide to the voters some means to individually verify the voting process, providing more confidence and detecting possible attacks.

Just like other information systems, an electronic voting system is also vulnerable to computer attacks. Although Internet voting may improve several election factors, there are concerns that the benefits are overshadowed by the issues of many potential security threats.

This work explains an instant graphical verification of vote by voter which follows by receipt of short message service. Ability to verify that the voter's vote is counted as cast raises the confidence of electorate in the internet voting and thus increases its global acceptance.

CHAPTER FOUR

RESULT AND DISCUSSION

4.1 Result

The designed verifiable electronic voting system made the voting exercise to be more transparent, reliable and trustworthy. It allows flexibility, cost effectiveness, proper time management and encourages more people to participate in the election process.

The different component of the system performs different function. The electronic form (data capturing interface) is the first human interface to the system which accepts electorates' bio data and biometric. Each voter's data collected at this stage was stored in the central database. The database with aid of java scripts filtered all the voters' input data with respect to their eligibility factors which include age and Nationality. The system also prevent multiple registrations from one voter by querying the system data base to check if such finger print and national identity number have been registered earlier.

For every registered voter, a unique registration number is generated:

$$X_{n+1} = ({}_aX_n + c) \mod m$$

Where X is the sequence of pseudorandom values, and

m, $0 <$ m – the "modulus"

a, $0 <$ a – the "multiplier"

c, $0 <$ c – the "increment"

X_0, $0 \leq X_0 < m$ – the "seed" or "start value"

The registration number serves as unique identifier or primary key for a registered voter.

Voter uses his national identity number, unique registration number and finger print as authentication credentials for accessing voting platform on the system.

At the voting platform (electronic ballot), there are logos representing different political parties under which different candidates is contesting for a political office. At this page, voters get to see updated votes count before casting his vote and an increment after voting which helps to verify that his vote was counted as did cast. The updated votes count is followed by short message service (sms) which further boost the confidence of voters and makes them believe in the system.

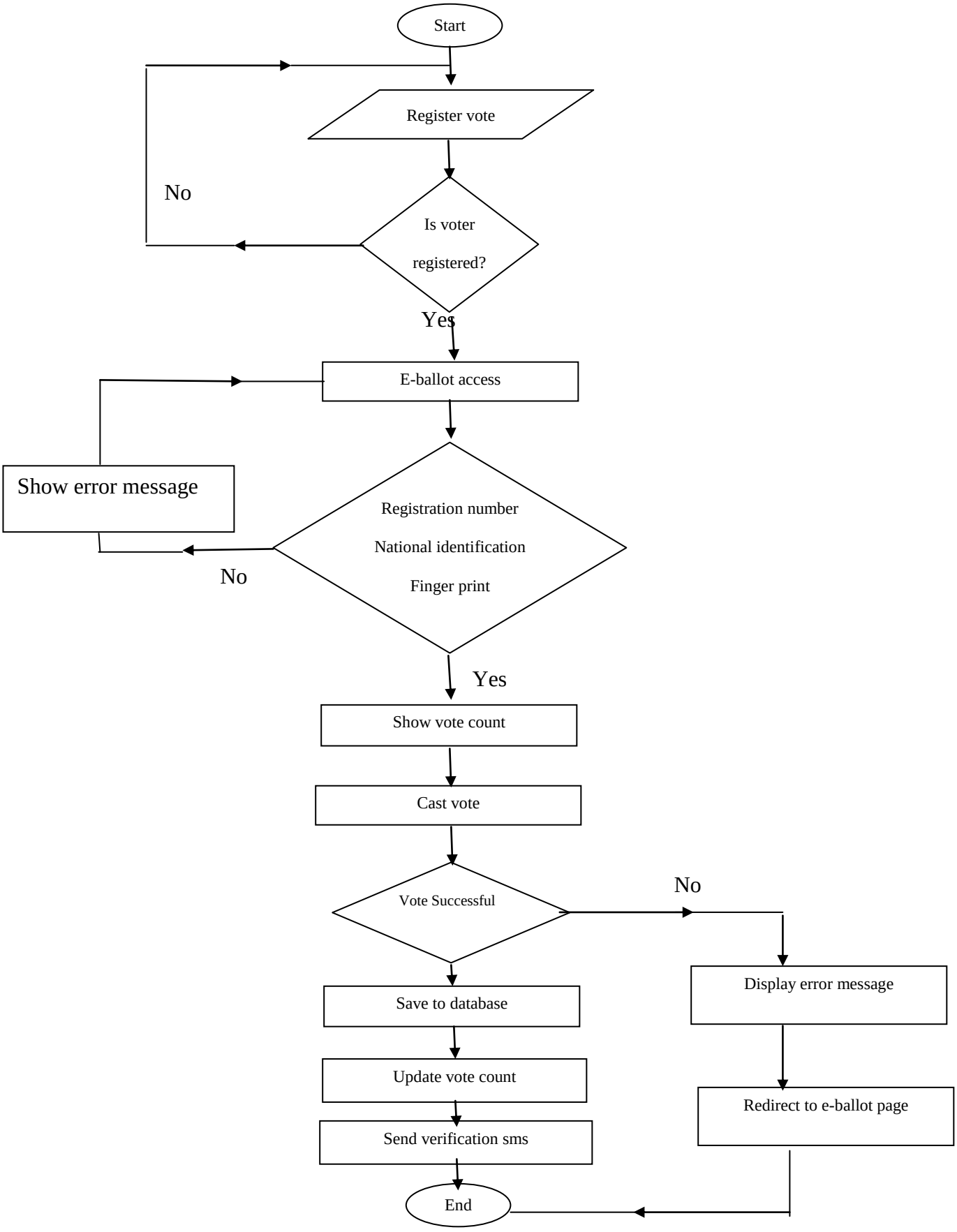


Figure 4.1. Flow chart for verifiable electronic voting system

4.2 Discussion

This work has discussed the challenges in designing a verifiable secret electronic voting scheme and presented the design philosophy. This system has sought to illustrate the key steps in the evolution of verifiable electronic voting system and the motivation, without seeking to give an exhaustive history.

This evolution has been driven in part by a desire to improve participation and trust in electronic voting system.

In response to the identification of vulnerabilities in previous works, some design decisions lead to clear-cut improvements; some give rise to rather subtle trade-offs.

A prime example is the trade-off between sending bulk short message service (sms) to voters after the whole election which shows the receipt (codes) of their votes counted as cast and being able to instantly see the updated result just immediately the voter casts the vote which is later followed by bulk short message service (sms).

The design has been driven by the aim to make the voter experience as simple and familiar as possible while providing high levels of transparency and auditability.

The verifiability electronic voting approach has spawned a suite of trustworthy schemes while also providing voters with a voting experience almost identical with currently existing manual systems. It is also very flexible and adaptable, being capable of supporting a number of different tallying methods. As such, it would appear to be one of the strongest contenders for a deployable scheme.

Attempts were made by previous researchers to address electronic vote verifiability problem by sending return codes through short message system after election as a means of assuring the electorates that their votes were counted. A careful study of this verifiability method shows that room is given for manipulation of result.

The model applied in this work allows voter to see current inconclusive result of the election (that is, the number of votes cast for each contestant before he or she cast own vote) and the updated increment in the number of votes cast for the electorate's preferred candidate. This builds the confidence of the voter and makes electorate to believe in the integrity of the system.

The beauty of this system is that it allows expatriate workers to exercise their civic right away from home country. Internet voting allows electorates to vote at the comfort of

their houses using phone, computers and other electronic devices to access the internet without compromising election secrecy. The election is to be conducted simultaneous within a specific period of time interval.

The Norwegian system presents all the phases of an election scenario, starting from preparing an election, casting a ballot, tallying and presenting the result. In the phases of a voting scenario and tallying, mechanisms for providing the requirements of authentication, secrecy, integrity and verifiability are included.

The system for the test pilot, is probably providing access control with an electronic ID (MinID) a method most Norwegian citizens have used before and are familiar with. It is assume the voters in a larger degree will trust the security of access control in the system, when using this kind of mechanism. The problem with trusting the system will probably in a larger degree be regarding privacy, verifiability and ballot tampering; if anyone (outsider or election authority) can see what ballot the voter cast, and that the vote is recorded as intended.

The double envelope scheme alone is not sufficient in an Internet voting application. In such an approach to e-voting, the voter’s computer is fully trusted in the system. This is not considered to be sufficient in an election scenario, because (as mentioned earlier in this thesis) the voter's computer can easily be compromised. When casting a ballot, the ballot information would be available in the voter's computer memory in plaintext for a period of time, making it possible for any attacker dropping malicious application to retrieve the information. Trojan could be used to expose parties that candidates voted for on the bulletin board.

Therefore additional security mechanisms in the system are needed. The potential voter himself is not able to do any computations, so everything has to be delegated to the voter's computer. Compromised computers is one of the most dangerous threats to an Internet voting system and therefore the Norwegian voting scheme puts no trust in the voter's computer. The Norwegian voting protocol uses mechanisms of proofs to ensure components are behaving as intended and users have possibilities of verification to ensure the ballot is recorded properly. Secrecy is provided with El-Gamal encryption and a mix net providing proofs of operation that can be validated for the tallying process.

The compromised computer problem can in a certain degree be solved using the cryptographic receipt method, but relies on voters actually auditing the voting process. To detect if a compromised computer has altered the ballot, the ballot box and the receipt generator cooperate to compute a sequence of receipt codes for the submitted ballot. These codes were sent to the voter through an independent channel (SMS). The method of verification in the Norwegian voting protocol relies on a cryptographic assumption from the receipt generator. For this method to work sufficiently, the receipt generator has to be very well protected, so a compromise of the receipt can be assumed to be very rare.

Secrecy and means of integrity and verification is in the Norwegian system provided by cryptographic mechanisms. These mechanisms are considered and analyzed and appeared very strong, but there are still other issues that needed to be considered. The verifying part of the system depends on the receipt generator, which could be compromised by the third party. So, this thesis has provided alternative means of voter verification method which involves graphical interface that shows the result before the voter casts his or her vote and later show the updated value (increase in the number of votes of the voter's preferred candidate) just immediately the voter clicks the submit button.

Verifiability is an important factor to consider when creating an internet voting system for the public to use.

In the Norwegian system they assume the voter would verify his vote with the SMS received after casting ballot, but this could be delayed or intercept by service provider.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATION

This chapter concludes the research thesis by providing a description of the contributions of the research; it also provides some suggestions to possible future research directions.

5.1 Conclusion

The ability of electorate to verify that his or her vote counts during election and that he or she is not short changed helps to believe in the credibility of the election. This curtails violence that always erupts after election in most developing countries and stops legal tussle at the election tribunal.

The area of electronic voting is an enormous field. Electronic voting has developed since the early 1900s. Several methods, with their strength and weaknesses have evolved. Electronic means of counting votes are widely used but the mean of casting electronic ballots keeps the discussion going.

There have been series of concerns with respect to all kinds of voting technologies; erroneous punch cards systems and criticized direct recording electronic voting machines. The latest development of Internet voting, are a topic of great concern.

Advantages and benefits of internet voting systems, like the efficiency and accessibility, could be outweighed by the issues of vote verifiability problem, the many potential security threats and secrecy of voter. There are critical security threats to electronic voting systems, but developed secure cryptographic methods can provide secrecy, integrity and proofs of correctness, countering many of these potential attacks. Other will argue the benefits of electronic voting outweigh the risk.

It is impossible to create a generic voting system for political elections. Countries are different, have different elections with different ballots and this require different systems. Each election is a significant project on its own, and systems have to be created and adapted to the specific country's electoral system.

The Helios system offers a good scheme for low-coercion elections without the highest stakes at risk, introducing people to the possibilities of open audit systems.

This is a scheme easily adaptable to different organizational elections.

The Norwegian voting system created for political elections, deploys strong cryptographic mechanisms for secrecy, integrity and verification providing a promising scheme for Internet voting.

To deploy Internet voting schemes, sacrifices have to be made. Even if the Norwegian voting system has the strongest cryptographic mechanisms it cannot protect against coercion attacks, affecting the democratic purpose of elections. An Internet voting system will never be perfectly secure. The importance of sacrifices has to be considered, like trading verifiability against the potential exposure to coercion. Verification by voters is key to the integrity and acceptability of the electronic voting system.

The internet voting platform is the best in term of convenience, general participation of all citizens in the election irrespective of their locations, cost effectiveness, safety, and fraud prevention through: 'one man one vote'.

This research work discuss the problem associated with internet voting verifiability method which affects the trust of electorate in the system, touches security issues without compromising global acceptable practice.

This research provides visual means of voters votes verification just immediately the vote is cast. Voters have the privilege of knowing the election result as soon as the election ends and thus prevents fraud.

5.2 Recommendation

The integrity of election is as important as the integrity of the democracy itself. To ensure this, the election process must be free and fair by ensuring that all the security loops are closed and rooms are not given to election malpractices or fraud. People should be allowed to be ruled by the leader of their choice without any influence or trading of conscience. For this system to work perfectly, especially in the developing countries;

- All the necessary infrastructures should be in place,
- Awareness should be given on the use of information and communications technology,
- The system should be made secure to prevent multiple votes by a single registered voter and prevents results manipulation by election fraudsters.

If all the above recommendations are adhered to, it will help build the integrity of internet voting system, makes it more popular and acceptable method of conducting election.

REFERENCES:

1. https://github.com/vvk-ehk/evalimine. Retrieved 10th June, 2013.

2. Silver et al. (1995): Information System

3. Saltman (2004) Assuring Accuracy, Integrity and Security in National Elections
4. ACE (2006) The Electoral knowledge Network: http://aceproject.org/ace-en/topics/et/onePage

5. http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics Retrieved 11th June, 2013

6. Stuart Gorin. Presidental race statistical tie in swing state Florida. Amer-ica.gov, 2008.
7. Douglas W. Jones, On Optical Mark-Sense Scanning, Towards Trustworthy Elections, Lecture Notes on Computer Science Vol. 60, Springer, 2010. (author's copy)
8. Gerald Holzer, Norman Walker and Harry Wilcox, Vote Tallying Machine, U.S. patent 3,218,439, Nov. 16, 1965.
9. Steve Bolton, Tim Cordes and Herb Deutsch, Method of Analyzing Marks Made on a Response Sheet, U.S. Patent 6,854,644, Feb. 15, 2005.
10. AVANTE Precinct-Based Optical Scan Solution http://www.avantetech.com/products/elections/optical/
11. The Harri Hursti Hack and its Importance to our Nation http://www.votetrustusa.org/index.php?option=com_content&task=view&id=798&Itemid=51
12. Comparing Tabulation of Paper Ballots using Optical Scanning Electronic and Tabulation of Direct Recording Electronic with Voter Verified Paper Ballots, AVANTE International Technology, Inc.March 1, 2007

13. Randolp C. Hite. Elections: electronic voting offers opportunities and presents challenges. United States General Accounting Office, 2004.
14. Kevin Bonsor and Jonathan Strickland. How e-voting works: Voting over the internet. How stuff works.com, March 2007.
15. Program and presentations at nist e2e workshop.http://csrc.nist.gov/groups/ST/e2evoting / program_E2E.html.
16. Jordi Barrat et al: Internet Voting and Individual Verifiability: The Norwegian Return Codes, 2011.
17. David, Jandura et al (2012), Internet voting and individual verifiability.
18. Josef Stalin (www. votefraud.org)
19. Government Accountability Office (May 2004) "Electronic Voting Offers Opportunities and Presents Challenges"
20. Thompson, Ken (August 1984) Reflections on Trusting Trust
21. Mary Bellis. The history of voting machines. About.com:Inventors, 2000.
22. http://www.eui.eu/news/2013/02-12/internetvotingasuccessintwoeuropeancountries.aspx
23. Orhan Cetinkaya at el: Electronic Journal of e-Government Volume 5 Issue 2 2007 (117-126)
24. Delaune et al. 2006 e-voting requirements
25. http://internetvotingforall.blogspot.com/2011/11/cyber-bullying-in-connecticut.html
26. Ben Adida. http://adida.net
27. Helios: Web-based open-audit voting. 17th USENIX Security Symposium, 2008
28. http://code.google.com/appengine/docs/whatisgoogleappengine.html
29. http://www.serveusa.gov/
30. www.verifiedvoting.org/projects/internet-voting-statement/ retrieved on 12/04/2014

31. Padilla, E. “Election Board proposes more efficient system.” The Diamondback, September 17, 1998. Retrieved April 18, 2000 from the World Wide Web: http://www.inform.umd.edu/News/Diamondback/1998-editions/09-Sept/17-Thursday/News10.html
32. Lavin, C. “Internet Voting and Preserving Anonymity.” San Francisco Chronicle: April 17, 2000; A23
33. www.unc.edu/courses/2008spring/law/357c/001/onlinevotingsite/technology.html
34. Internet policy institute. Report of the national workshop on internet voting: Issues and research agenda. Internet policy institute, 2009
35. Svetlana Z. Lowry and Poorvi L. Vora. Desirable properties of voting systems. presentation, E2E workshop NIST, 2009
36. Ronald L. Rivest. Perspectives on end-to-end voting systems. NIST E2E Workshop, October 13, 2009
37. Estonian National Electoral Committee. Internet voting in estonia. http://www.vvk.ee/public/dok/Internet_Voting_in_Estonia.pdf, 2008
38. Website of federal voting assistance program, us. http://www.fvap.gov/.
39. www.howstuffwork.com
40. ErgoGroup/Project E-vote. Project e-vote 2011: Contractor solution specification. "E-vote 2011"
41. http://www.evalgbloggen.no
42. http://www.novinite.com/view_news.php?id=112540.
43. W. Aspray et al. Computing before computers (Chapter 4). Iowa State University Press, 1990.
44. http://www.technikum29.de/en/computer/punchcard.shtm, 2003-2010.
45. Kathy Gill. An illustrated history of voting methods and systems. http://uspolitics.about.com/od/elections/ig/History-of-Voting-Systems, About.com.
46. Michael Shamos. Optical scan systems. Lectures, Institute for Software Research International Carnegie Mellon University, 2004.
47. http://www.sequoiavote.com/, Last visited Oct 2013

48. Matt Blaze et al. Source code review of the sequoia voting system. Technical report, University of California, Berkeley, July 2007.
49. Government Accountability Office (September 2005) "Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to Be Completed"
50. http://whatis.techtarget.com/glossary/e-voting-glossary.html.
51. Schneier, Bruce (September 2004), openDemocracy What's wrong with electronic voting machines?
52. http://www.notablesoftware.com/evote.html
53. "http://post-journal.com/articles.asp?articleID=6218". The Post-Journal
54. "Protecting the Integrity and Accessibility of Voting in 2004 and Beyond". People for the American Way
55. "Disability Access to Voting Systems" Verified Voting Foundation
56. California Internet Voting Task Force. A report on the feasibility of internet voting. http://www.sos.ca.gov/elections/ivote/final_report.htm\#final-3, 2000.
57. "Ballot Templates." (tactile ballots) International Foundation for Election Systems
58. Juels, Ari; Dario Catalano and Markus Jakobsson (November 2002). "Coercion-Resistant Electronic Elections". Cryptology ePrint Archive (165). Retrieved 2 Nov 2013.
59. Chaum, David; Peter Y. A. Ryan and Steve Schneider (2005). "A Practical Voter-Verifiable Election Scheme". ESORICS'05: 10th European Symposium On Research In Computer Security. LNCS **3679**: 118–139.

60. Kremer, Steve; Mark Ryan and Ben Smyth (2010). "Election verifiability in electronic voting protocols". ESORICS'10: 15th European Symposium on Research in Computer Security **6345**: 389–404.

61. "ORG Election Report highlights problems with voting technology used". Openrightsgroup.org. Retrieved 2013-06-24.

62. http://www.openrightsgroup.org/2008/07/02/org-verdict-on-london-elections-insufficient-evidence-to-declare-confidence-in-results/

63. "Ruling of the Second Senate of the Federal Constitutional Court of Germany, 3 March 2009". Bundesverfassungsgericht.de. Retrieved 2013-06-24.

64. "German Federal Constitutional Court, Press release no. 19/2009 of 3 March 2009". Bundesverfassungsgericht.de. Retrieved 2013-05-24.

65. "Draft white paper on VVPR" (PDF). Retrieved 2013-05-24.

66. Questions and Answers on the Draft Report: "Requiring Software Independence in VVSG 2007: STS Recommendations for the TGDC"

67. "Pilot Study of the Scantegrity II Voting System Planned for the 2009 Takoma Park City Election"

68. Hardesty, Larry. "Cryptographic voting debuts". MIT news. Retrieved 2013-10-30.

69. Haynes, D. "Hackers reveal Internet flaws." Kansas City Star, January 26, 2000; A1.

70. Arent, L. and McCullough, D. "A Frenzy of Hacking Attacks." Wired News, February 9, 2000. Retrieved April 10, 2000 from the World Wide Web: http://www.wired.com/news/business/0,1367,34234,00.html

71. See the "Attrition" Web site at http://www.attrition.org/

72. "What Impact do the Internet and new communications technologies have on political campaigns and elections?" in American Bar Association News, par. 1

[online journal] (January 1997 [cited 11 March 2000]) available from World Wide Web: http://www.abanet.org/media/jan97/cyberre.html

73. http://blog.heliosvoting.org
74. http://www.math-cs.gordon.edu/courses/cs323/FORTRAN/fortran.html