SUDAN UNIVERSITY OF SCIENCE & TECHNOLOGY

COLLEGE OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY

DEPARTMENT OF COMPUTER SYSTEMS AND NETWORKS

Secure Electronic Voting

A THESIS SUBMITTED AS ONE OF THE REQUIREMENTS FOR OBTAINING A BACHELOR OF HONOR IN COMPUTER SYSTEMS AND NETWORKS

OCTOBER 2015

بسم الله الرحمن الرحيم

SUDAN UNIVERSITY OF SCIENCE AND TECHNOLOGY
COLLEGE OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS AND NETWORKS

Secure Electronic Voting

PREPARED BY:

ABOBAKR OSMAN GASMALSEED

MAMOON KHALID ABOZAID

MUSTAFA ALJACK EBRAHEEM

ASIM HASSAN MOHAMED

SUPERVISOR:

Mr. MOHAMED OSAMA HEWAITALLA

OCTOBER 2015

الآيـــــــــــة

قال تعالى :

(يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ)

المجادلة 11

الحـمـد لله

إن الحمد لله، نحمده ونستعينه، ونستغفره ونتوب إليه، ونعوذ بالله من شرور أنفسنا ومن سيئات أعمالنا، من يهد الله فلا مضل له، ومن يضلل الله فلا هادي له، وأشهد أن لا إله إلا الله، وحده لا شريك له، له الملك وله الحمد، وهو على كل شئ قدير. وأشهد أن محمدًا عبد الله ورسوله، أرسله الله رحمة للعالمين؛ فشرح به الصدور، وأنار به العقول، وفتح به أعينًا عميًا، وآذانًا صمًا، وقلوبًا غلفًا.

يـا من إلـيه جميـع الـخلق يبتهـل *** وكـل حـيّ علـى رحمـاه يتكـل
يـا من نأى فرأى ما في القلـوب وما *** تـحت الثرى وحجاب الليل منسـدل
أنـت المنـادى بـه في كل حادثـة *** وأنـت ملجـأ من ضاقـت به الحيـل
أنـت الغيـاث لمن سُدَّت مذاهبـه *** أنـت الدليـل لمن ضـلت به السبـل
إنـا قصدنـاك والآمـال واقـعـة *** عليك ، والكـل ملهـوف ومبـتهل
فإن غفـرت فعن طَوْل وعن كـرم *** وإن سطـوت ؛ فأنت الحـاكم العـدل

سبحانك اللهم خير معلم *** علمت بالقلم القرون الأولى
أخرجت هذا العقل من ظلماته *** وهديته النور المبين سبيلا
أرسلت بالتوراة موسى مرشدا *** وابن البتول فعلم الإنجيلا
وفجرت ينبوع البيان محمدا *** فسقى الحديث وناول التنزيل

ACKNOWLEDGEMENT

First and foremost, we thank Allah for granting us knowledge, health, and the patience to Successfully complete this project.

We would also like to show our gratitude and appreciation to the following peoples:

Mr. MOHAMED OSAMA HEWAITALLA

Dr. IZZALDEEN KAMIL AMEEN

Eng. ISAMAIL ALI EBRAHEEM

For their generous and constructive feedback and continuous Encouragement throughout The project.

SPECIAL THANKS AND GRATITUDE TO ALL OF OUR COLLEAGUES AND FRIENDS FOR EVERYONE KNOWS OUR NAMES, THANK YOU.

المستخلص

التصويت هو جزء أساسي من أي حكومة . التصويت في الانتخابات العامة هو وسيلة لمواطني الدولة للتعبير عن رأيهم في اختيار المرشح الأفضل لقيادتهم ، وبدأت فكرت التصويت الإلكتروني عن طريق العالم Chaum في 1980 ، ومنذ ذلك الحين كان هنالك الكثير من العمل الذي أنجز في هذا المجال.

يتطلب التصويت الإلكتروني مستوى عالً جدًا من الأمان، أعلى بكثير من المستخدم في أنظمة التجارة الإلكترونية. هذا المقترح يقوم بدراسة المتطلبات الأمنية للتصويت الإلكتروني.ومن ثم دراسة حوارزمية ال Fujioka, Okamoto and Ohta's scheme (FOO scheme) ، وبعض الخوارزميات الأخرى المستخدمه في هذا المجال.

يقوم النظام المقترح بإستخدام نفس طريقة أنظمة التصويت التقليدية في مرحلة التسجيل ، التي تضمن الأمن وتستخدم هذه الميزه لإعطاء المواطنين الذين يمتلكون حق التصويت رمزاً فريداً يمكنهم من الوصول لنظام التصويت والإدلاء بأصواتهم. و هذه هي العمليه الوحيده التي يقوم بها المواطن في مركز مثل الطريقه التقليديه للتصويت.

وتم عمل تحليل للنظام المقترح لتحديد مدى تحقيقه للشروط المتطلبه في أنظمة التصويت الإلكترونيه .

ABSTRACT

Voting is an essential part of any government. Voting in a general election is the way citizens of a nation express their opinion in selecting the best candidate to lead them. This concept of e-voting was introduced by Chaum in the early 1980s and since then there have been a lot of work done in this area.

Electronic voting requires a very high level of security, much higher than e-commerce. In this thesis the discussion would be start from the security requirements of an electronic voting schema. Then discuss the Fujioka, Okamoto and Ohta's scheme (FOO scheme) and other scheme and perform a security analysis of these schemes against the security requirement of an e-voting scheme to show their limitations. The traditional voting systems have powerful registration way and verify the eligibility and this feature used to give the eligible citizens unique token to access our system and cast their ballot. And this is only physical process in our system.

Finally, make a security analysis of our schema and show how not only improve on the limitations of the FOO schema voting schema but also satisfy all the security requirements of an electronic voting schema that has been discussed.

LIST OF KEY TERMS

Term	Description
Election	**An election is a formal decision -making process by which a population chooses an individual to hold public**
Candidate	**A person who is elected or nominee to a certain position or person seeking or being considered for some kind of position e.g. (to be elected to an office)**
Polling station	**A place where voters go to cast their votes in an election or a venue established for the purpose of polling and controlled by staff of the electoral management body.**
Registration system	**System that use traditional registration way and verify the eligibility to give the eligible citizen unique token to access voting system and cast his/her ballot. And this is the only physical process.**
Ballot	**Is a device used to cast votes in an election, and may be a piece of paper or a small ball used in secret voting.**
Voting schemes	**Scheme prescribes voters and authority's actions and computations during the voting process.**

LIST OF FIGURES

TABLE OF CONTENTS

1.1 INTRODUCTION

Voting in a general election is the way people can express their opinion in selecting the best Candidate to lead, manage and represent them. There are common way of voting such as traditional voting, E-Voting which include online voting.

The traditional way of voting Suffers from many problem such as time consuming, election Fraud, Cost and mobility (ability to vote from anywhere).Therefore People think to improve this by introduce Electronic voting. E-Voting can be useful to reduce traditional problem by using electronic systems to aid casting and counting votes. Technologies that are used by Electronic Voting can include punched cards which is used to store and retrieving information with early computers and which is used to store eligible votes [1], and voting kiosks in which voter then proceeds to a secret ballot stands to cast his vote [2] outside of polling station in an uncontrolled environment on a voting computer. For example in shopping malls or army bases. E-voting also came with its problem such as Errors in programming can be very simple Adding a semi-colon in the wrong place can completely change a program For example, a recent midterm election in Dallas, Texas used touch-screen DRE machines. Voters discovered that no matter where they touched on the Democratic side of the screen, it would vote for the Republican candidate. The Democratic Party went to court, with affidavits demonstrating that the machines were making this error. It was decided that some of the voting machines were misaligned, and those machines were taken out of service. It has also been reported that in one Iowa country a single electronic voting machine miscounted by three million votes due to an error [6].

Although E-voting solve many problems of traditional voting system, mobility problem still arise. As a result, E-Voting has been evolving into Internet voting.

Internet voting or online voting is to vote from any place and any time using public internet and E-voting technologies [3].There have also been other concerns raised about weaknesses of the internet and level of security of PCs such as Sniffing, Spoofing, Denial of service, malware and the difficulty in preventing impersonation (family member voting for another one i.e. brother voting for his sister). These weaknesses must be kept in mind during the process of online voting.

Government elections and referendums in the United Kingdom, Estonia and Switzerland are examples of the use of E-voting , also used in the municipal elections in Canada and party primary elections in the United States and France [4].

1.2 SUDANESE GENERAL ELECTION, 2015

A general election was held in Sudan on 13-16 April 2015 to elect the President and the National Assembly. All citizens above eighteen chose a polling unit that is easily accessible to them to register, and then a voter's card with some relevant details of the voters, along with an image of the voter is produced and given to each voter to be used in voting phase. The President is elected using the two-round system [5].

The two-round system (also known as runoff voting) is a voting system used to elect a single winner where the voter casts a single vote for their chosen candidate. However, if no candidate receives the required number of votes then those candidates having less than a certain proportion of the votes, or all but the two candidates receiving the most votes, are eliminated, and a second round of voting occurs [5]. To win, a presidential candidate must secure more than 50% of the total vote in the first round to avoid a run-off. According to the constitution, a president can serve a maximum of two five-year terms.

The two-round system is used around the world for the election of legislative bodies and directly elected presidents. For example, it is used in France, Argentina, Austria, Brazil, and Bulgaria.

Election observer missions (EOM) were deployed from the African Union (AU), Arab League, Common Market for Eastern and Southern Africa (COMESA), Intergovernmental Authority on Development (IGAD), Organization of Islamic Cooperation (OIC) [7].

1.3 PROBLEM STATEMENT OF THIS RESEARCH

Traditional voting systems also has its shortcomings in terms of lack of Voter's mobility, Cost, lack of human trust, reduce People congestion, no chance to make changes and overhead of voting process, Electoral fraud, time consuming and transmission of votes. These issues have inspired us to research in electronic voting field to propose an E-voting scheme that overcomes the limitations of traditional ones.

1.4 AIM OF THIS RESEARCH

The objective of this project is to define the security requirements of an electronic voting scheme, Applying security Requirements that at least as the same as traditional voting scheme and Produce a trusted System that can be used for general election.

1.5 SCOPE OF THIS RESEARCH

Analysis the traditional voting schemes to understand the whole system and what degree of security it's require in order to produce an electronic voting system that solve traditional problems, adding more convenience to users of system .
Finally analysis our proposed system against the E-voting security requirements then makes recommendations for improvement of the limitations.

1.6 STRUCTURE OF THE RESEARCH

In chapter two the talking will be on general overview of voting, electronic voting, and online voting. Also are talking about the Security requirements of an electronic voting schemes which Provide verifiability and auditability in electronic voting. Chapter 3 introduce E-Voting schemes based on Anonymous Channel, Chapter 4 about the analysis of the E-Voting system using UML. Chapter 5 deal with technique and tools that will be

used to achieve the objectives of the project. Chapter 6 Discuss Sudanese general election then introduce FOO scheme. And chapter 7 is about the conclusion and recommendation.

1.7 RESEARCH METHODOLGY

Starting with traditional Sudanese general election. Did an overview of the election processes. Then discuss the FOO scheme that used in proposal system and why is chosen rather than the other voting schemes, how its work with election processes, what security services property is achieved and discuss the limitations of the FOO-scheme. Then went on to give a more detailed view of the Secure E-Voting (Proposal protocol) and the messages exchanged between the various entities. After which analyzed the scheme and showed how it satisfy the security properties of an E-Voting scheme.

2.1 BACKGROUND

Over the years there has been a lot of election fraud and a steady decline in turnout of eligible voter's .These are part of the major drivers for the push for an electronic voting system which is believed would increase mobility and accuracy of the voting process. The wide spread deployment of the internet and use of computers is an extra reason why there has been a lot of call for the inclusion of an electronic voting system where voters can participate remotely via the internet [2].

-There are typically three different places where electronic voting can be implemented. Two of these three are in a polling place which could either be in a precinct or a kiosk where the voter is supervised by election officials, while the third way is via the Internet which is known as Remote Internet Voting where the voter is unsupervised [7]. (Figure 2.1) below shows the different types of voting both traditional paper voting and electronic voting.

-In this chapter the talking will be about Traditional Voting Equipment's that support a security requirements which are depend on policies and behavior of society, however with this degree of security it has some vulnerabilities so E-voting appear. E-voting solve traditional voting problems that allowing online voting, give us higher degree of security requirements that clarified in example of effectiveness of E-voting (Brazil, Belgium).

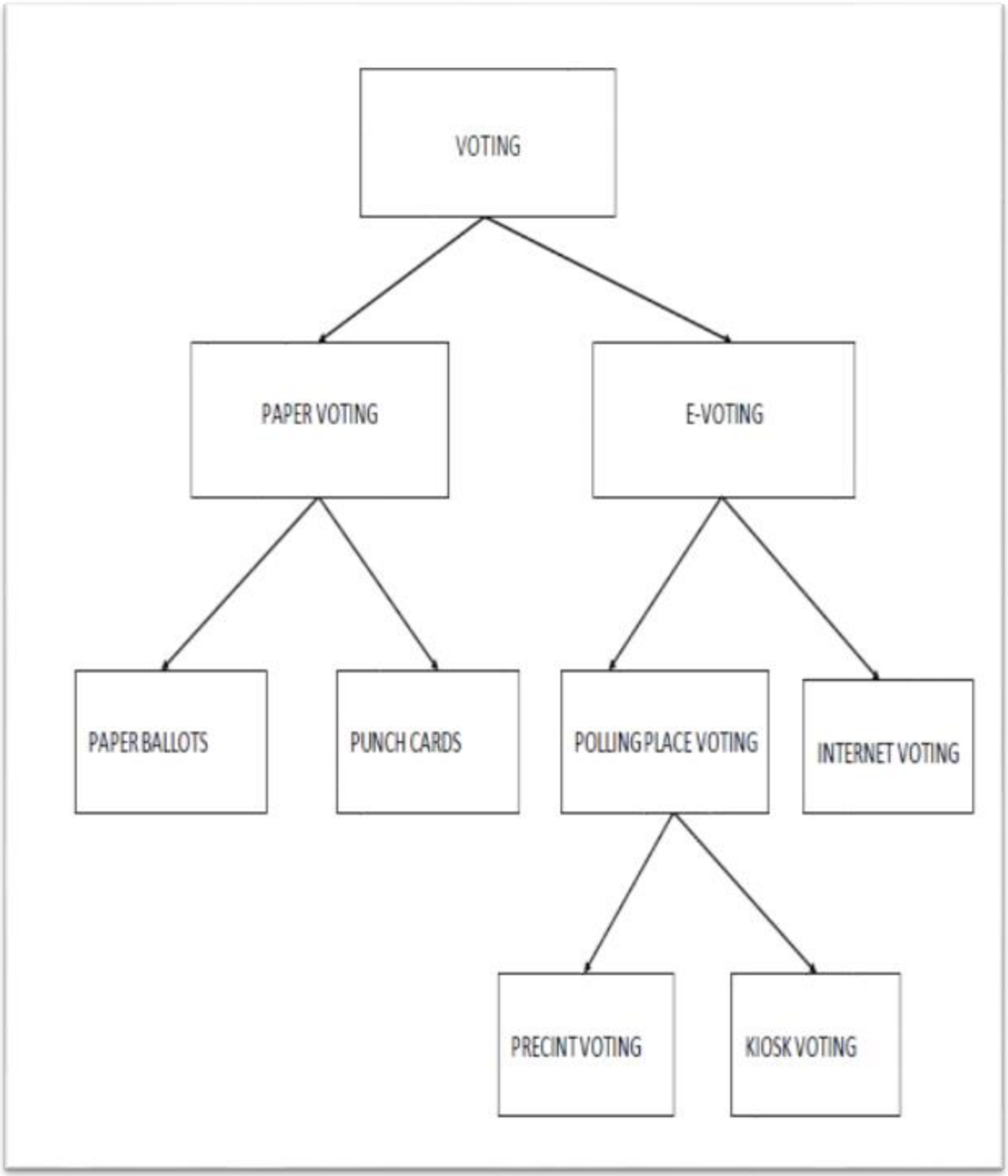


Figure 2.1: Different Types of Voting [2]

2.2 TRADITIONAL VOTING EQUIPMENT'S

In the recent years, voting equipment's which were widely adopted may be divided into five types [8]:

(1) Paper-based voting: The voter gets a blank ballot and uses a pen or a marker to indicate she/he want to vote for which candidate. As shown in (figure 2.2) ballots hand-counting is a time and labor consuming process, but it is easy to manufacture paper ballots and the ballots can be retained for verifying, this type is still the most common way to vote.

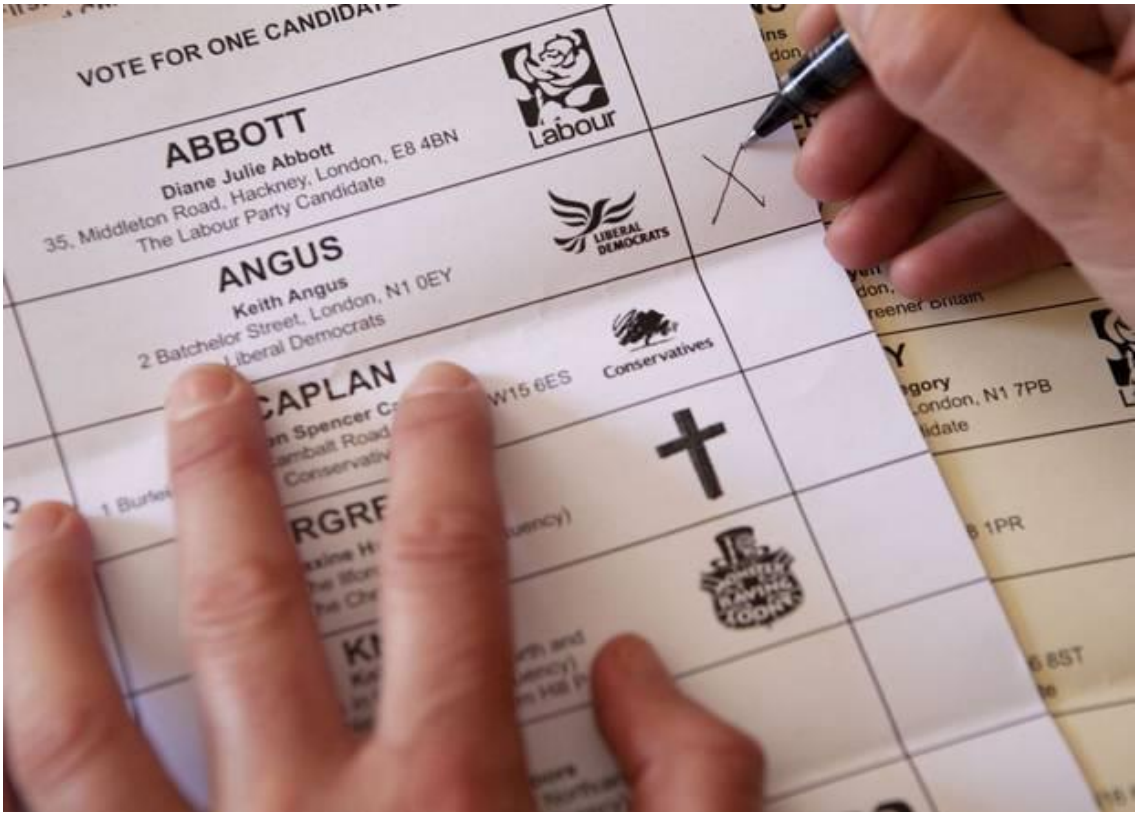


Figure 2.2: Paper-based voting [13]

(2) Lever voting machine: Lever machine is peculiar equipment, and each lever is assigned for a corresponding candidate. The voter pulls the lever to poll for his favorite candidate. This kind of voting machine can count up the ballots automatically. Because its interface is not user-friendly enough giving some training to voters is necessary.

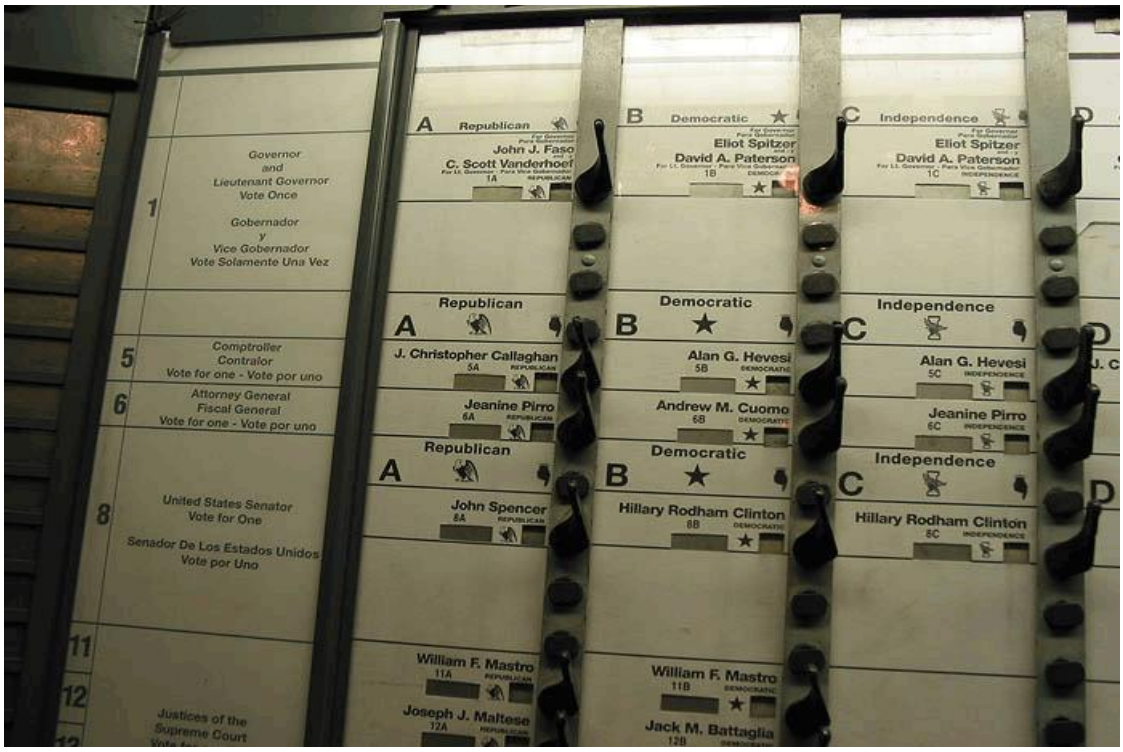


Figure 2.3: Lever voting machine [14]

(3) Direct Recording Electronic Voting Machine [16]: DRE uses a keyboard, touch screen, mouse, pen or other electronic device to allow a voter to record his/her vote electronically. Some machines, including touch screen and selection wheel require voters to insert an access card to initiate the voting process, while others require an electronic ballot or access code. DRE is used in supervised locations – polling stations – rather than unsupervised environments such as Internet or SMS voting. It captures the voters' choices and stores them. The data captured by each individual DRE unit is then transmitted by either electronic means –such as the internet, cellular or memory record – or manually by printing the results from each machine and tabulating them.

Figure 2.4: Direct Recording Electronic Voting Machine [15]

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

Figure 2.5: Punch card [15]

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

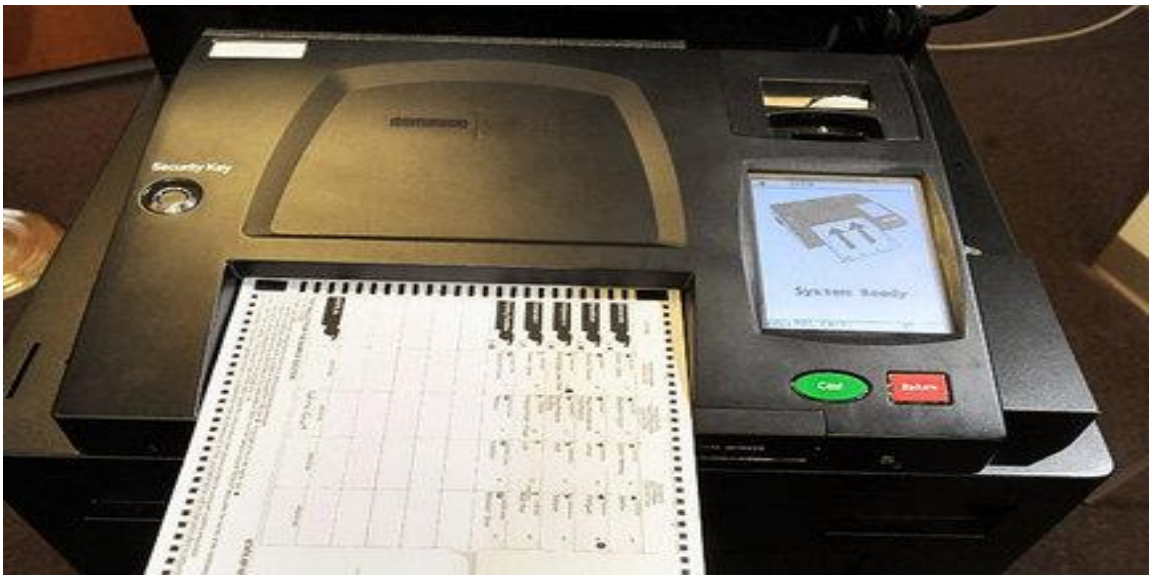


Figure 2.6: Optical voting machine [29]

2.3 ELECTRONIC VOTING

E-voting systems include three actors: voter, registration authorities and tallying authorities. Voters have the right for voting, and registration authorities register eligible voters before the "election day". These authorities ensure that only registered voters can vote and they vote only once on the election's day. Tallying authorities collect the cast votes and tally the results of the election. They may be counter, collector and /or tallies [10].

E-voting system should also involve four phases: Voters register themselves to registration authorities and the list of eligible voters is compiled before the Election Day. On the Election Day registered voters request ballot or voting privilege from the registration authorities and the registration authorities check the credentials of those attempting to vote and only allow those who are eligible and registered before. Voters casts their vote and finally the tallying authorities count the votes and announce the election result [10].

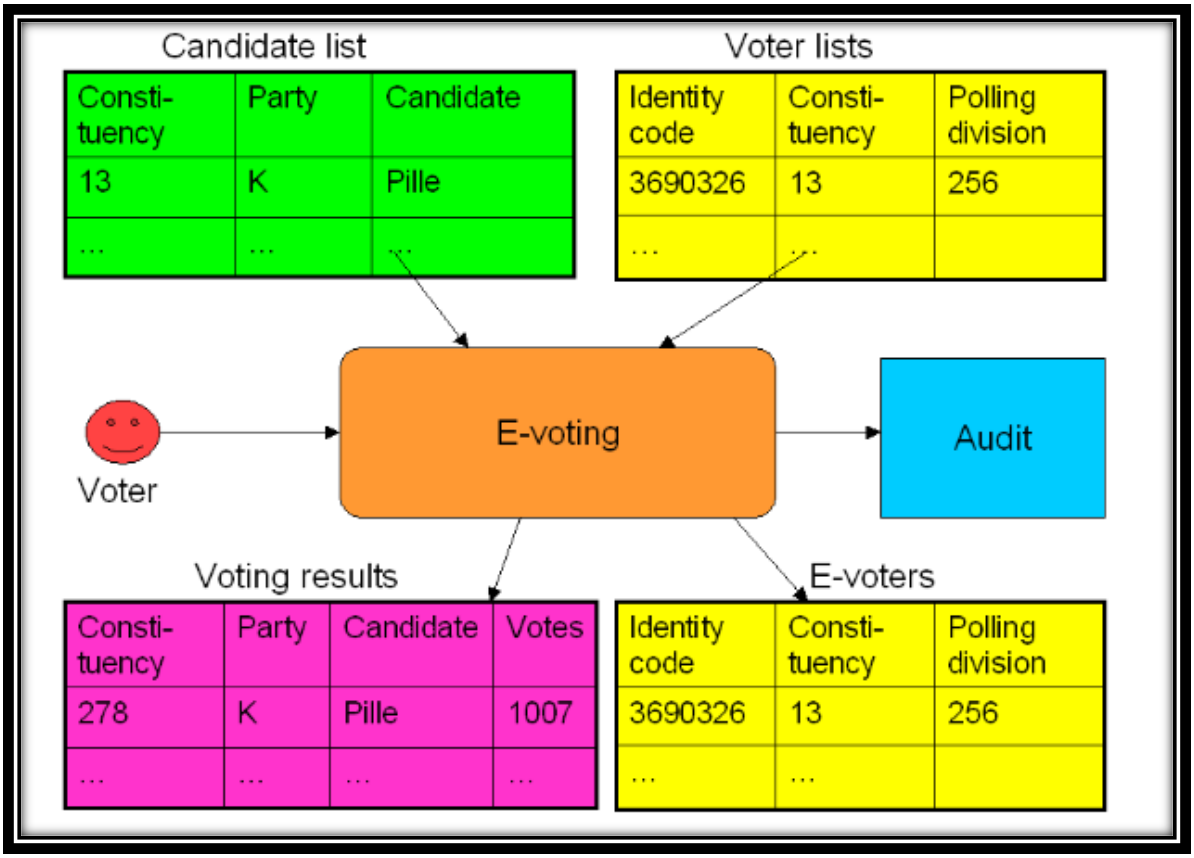


Figure 2.7: The scope of e-voting: input and output [9]

As illustrated in (Figure 7), the elections are made up of the following components:

Calling of elections, registration of candidates, preparation of polling list,

Voting (a subset of which is e-voting) and counting of votes.

The input of the e-voting system is made up from:

1) Voter lists (including the polling division and constituency assigned to the voter).

2) Candidate lists (by constituencies).

3) expressed will of the voters.

And the output is made up from:

1) Summarized voting result of e-voters.

2) List of voters who used e-voting.

-In general, two main types of E-Voting can be identified: [11][12]

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

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, mobile phone, television via the internet (also called I-Voting)).

2.4 EFFECTIVENESS OF E-VOTING AMONG DIFFERENT COUNTRIES

In recent years, a considerable number of countries has adopted E-voting for their official elections. In this section, two empirical examples are enumerated as following [8]:

1- Belgium election for the federal parliament is held in 'May 18, 2003'. In order to assist voters in being familiar with-voting system, electoral center held short-term training. Counting efficiency in the election with E-voting system was faster than convention. Belgium's compulsory voting system and E-voting complement each other, voters' satisfaction and attending willingness of join voting are improved.

2- Brazil used E-voting in 1998. When voters reaches the polling place, they Show their identities card for authenticating; if someone is an eligible voter, he can get the ballot For E-voting. Brazil's E-voting system transmits votes to electoral center immediately, so that the count of votes can announce rapidly during the voting process.

2.5 E-VOTING SECURITY REQUIREMENTS

The voting system should include controls to prevent deliberate or accidental attempts to replace code such as unbounded arrays and strings. The system should have zero-tolerant with regard to compromising. Election process should not be subject to any manipulation including even a single vote manipulation.

The system should provide accurate time and date settings. The system should not allow improper actions by voters and election officials the system should not allow Local Election Officials (LEOs) to download votes to infer how voters in their precinct have voted .The system should provide means for Protecting and securing recounts of ballots cast.

Below are the security requirements electronic voting protocols try to meet: [2]

(1) Privacy: this is the security property which requires that a voter's identity should not be linked to a vote cast for example if a Voter Alice casts a vote XYZ, it should be impossible for an unauthorized 3rd party to link the vote XYZ to Alice. This means that the system shouldn't be able to reveal how the voter voted. This property hence requires the voter's identity to remain anonymous. This voter's privacy should be guaranteed even after the conclusion of the elections.

(2) Democracy: Any electronic voting protocol or system should be able to ensure that only eligible voters are allowed to vote and the protocol should also prevent the eligible voters from voting more than ones.

(3) Receipt-freeness: this is the property that ensures that a voter does not get any information that he could use to prove to a coercer that he voted in a certain way. This property helps to prevent vote selling by eligible voters which would be the adversary in this instance. And also allows the electronic voting meet the security of the secret-ballot election offered by a traditional voting booth.

(4) Verifiability: this is the ability for anyone i.e. voters, public or external auditors, to verify or audit an election to ensure votes have been counted correctly. This type of verifiability is usually known as **public or universal verifiability** which is a much stronger form of verifiability because verification is not limited to the particular voter that cast the vote, anyone including a passive party can observe and be convinced that the election is fair.

(5) Individual Verifiability: this ensures that there are mechanisms in place to enable a voter to verify that his vote has been counted and can file a sound complaint if that is not

the case without revealing the contents of the ballot. This property of an electronic voting system that voters can check that their votes have been counted and tabulated correctly.

(6) Robustness: this property ensures that even if different parties collude the system should still recover from any faulty behavior. This property also means that votes cannot be included my fraudulent authorities for voters that abstain and that the systems should be resilient to any external attack such as a denial of service attack.

(7) Fairness: If voters already have an idea of how votes have gone before they cast their votes it may influence their decision. So this property ensures that all candidates are given a fair chance by preventing the release of any partial tally such that even counting officials have no clue about results and voter's decisions are not influenced.

(8) Accuracy: this property requires that all valid votes should be counted correctly, invalid votes cannot be added and valid votes cannot be modified, removed or invalidated from the finally tally and if this happens it can be easily detected.

(9) Uncoercibility: this property ensures that any coercer cannot force a voter to get the value of his vote, or make the voter to cast votes in a particular way or for a particular candidate. Even authorities should not be able to derive the value of the vote.

2.6 PREVIOUS STUDIES

There are several countries that try to apply the e-voting system, some of them in national election; however, there are some security issue like bot-net, Dos, D-Dos attack, and other network security issues. And discuss the previous studies in this field and describe the achieved security service and the troubles that it face him.

2.7 Estonia [22]

The most widespread use of e-voting has been in Estonia. In the 2011 parliamentary elections, more than 140,000 Estonians voted over the Internet, amounting to nearly a quarter of all votes.

Estonia has allowed its voters to cast a ballot over the Internet in local elections since 2005 and national elections since 2007 as part of the government's e-government strategy.

E-voting is generally seen as secure, because voters utilize a national digital ID card that has also been used for services such as tax filing, insurance and public transportation. Voters use their ID cards to authenticate to the server and to sign their ballots. Each card contains two RSA key pairs, one for authentication and one for making digital signatures.

Certificates binding the public keys to the card holder's identity are stored on the card and in a public LDAP database [21]. The card does not allow exporting private keys, so all cryptographic operations are performed internally. As an added safeguard, each key is associated with a PIN code, which must be provided to authorize every operation.

Additionally, Estonia has taken steps to counter concerns about third parties putting illegal pressure on people casting a vote over the Internet, by allowing them to re-vote [21].

2.7.1 I-Voting Server Infrastructure

- Vote forwarding server (VFS/HES) The VFS (or HES in Estonian) is the only publicly accessible server. It accepts HTTPS connections from the client software, verifies voter eligibility, and acts as an intermediary to the back-end vote storage server, which is not accessible from the Internet.
- Vote storage server (VSS/HTS) The VSS is a back-end server that stores signed, encrypted votes during the on-line voting period. Upon receiving a vote from the VFS, it confirms that the vote is formatted correctly and verifies the voter's digital signature using an external server.

  Log server this server is an internal logging and monitoring platform that collects events and statistics from the VFS and VSS. The source code and design have not been published. While this server is not publicly accessible, it can be accessed remotely by election staff.

- Vote counting server (VCS/HLR) The VCS is never connected to a network and is only used during the final stage of the election. Officials use a DVD to copy encrypted votes (with their signatures removed) from the VSS. The VCS is attached to a hardware security module (HSM) that contains the election private key. It uses the HSM to decrypt the votes, counts them, and outputs the official results.

2.7.2 Voting Processes

Below are the voting Processes steps:

(1) The election authority publishes a set of voting client applications for Windows, Linux, and Mac OS.

(2) The voter begins by launching the client application and inserting her ID card. Which is used to establish a client-authenticated connection to the VFS.

(3) The server confirms the voter's eligibility based on her public key and returns the list of candidates for her district.

(4) The voter selects her choice 'c' and signing it. The signed and encrypted vote is sent to the server.

(5) The server return QR code to client containing 'r' (random number used to pad ballot) and 'x' (ballot ID).

(6) The client can verified her vote by using the QR code to retrieve her vote by using android application.

(7) As a defense against coercion, voters are allowed to vote multiple times during the on-line election period, with only the last vote counted. All earlier votes are revoked but retained on the storage server for logging purposes.

2.7.3 Achieved Properties

1- Eligibility "no one can vote unless eligible".

2-Privacy.

3-Individual Verifiability.

4-multiple layer of security (the success attack must done in both web application that used to perform voting and android application that used to perform client verification).

2.7.4 Drawbacks

1-Inadequate Procedural Controls (some published procedures were not consistently followed and others were dangerously incomplete).

2-Vulnerabilities in Published Code (shell-injection).

3-Insufficient Transparency.

4-Several problems in the official videos of the per-election setup process (workers unintentionally typed passwords and national ID card PINs in view of the camera these included the root passwords for the election servers).

5-lake of universal Verifiability.

2.8 Washington D.C. Internet Voting System [23]

In 2010, Washington, D.C. developed an Internet voting pilot project that was intended to allow overseas absentee voters to cast their ballots using a website. Prior to deploying the system in the general election, the District held a unique public trial a mock election during which anyone was invited to test the system or attempt to compromise its security.

2.8.1 Architecture of D.C. Digital Vote-By-Mail System

The Digital Vote-by-Mail (DVBM) system is built around an open- source web application developed in partnership with the D.C. Board of Elections and Ethics (BOEE) by the Open Source Digital Voting (OSDV) [23].

The software uses the popular Ruby on Rails framework and is hosted on top of the Apache web server and the MySQL relational database. Global election state (such as registered voters' names, addresses, hashed credentials, and precinct-ballot mappings, as well as which voters have voted) is stored in the MySQL database. Voted ballots are encrypted and stored in the file system.

2.8.2 Voting Process

Below are the voting Processes steps:

1- Each eligible voter received a letter by postal mail containing credentials for the system. These credentials contained the voter ID number, registered name, residence ZIP code, and personal identification number (PIN). The letters instructed voters to visit the D.C. Internet voting system website, which guided them through the voting process.

2- The voter then logs in with the credentials provided in the mail, and confirms his or her identity.

3- The voter is presented with a blank ballot in PDF format "server send it to voter". The voter marks the ballot electronically using a PDF reader, and saves the ballot to his or her computer. The voter then uploads the marked ballot to the D.C. Internet voting system, which reports that the vote has been recorded by displaying a "Thank You" page. If voters try to log in a second time to cast another ballot, they are redirected to the final Thank You page, disallowing them from voting again.

2.8.3 Drawbacks

1- Shell-injection vulnerability that can allow attackers to compromise the web application server.

2- Stealing secrets. (By what kind of attack)

3- Changing past and future votes.

4- Revealing past and future votes.

5- Discovering that real voter credentials were exposed.

6- There were other attack base on web security like “session management”

7- Application user had permission to write the code of the web application. This might lead to local privilege escalation vulnerability.

8- Attacking the Network Infrastructure. For example, the ability to discover a Cisco router (8.15.195.1).

9- Infiltrating the terminal server (using HTTP-based administrative interface gain access using the default root password).

10- Compromise unsecured network surveillance cameras of server room.

2.9 CHAPTER CONCLUSION

In this chapter the discussion about the voting types as general (traditional and e-voting), and effectiveness of e-voting among different countries, also e-voting security requirements, and the previous studies in this field and describe the achieved security service and the troubles that it face him.

3.1 INTRODUCTION

In this chapter the introduction has included E-Voting schemes based on Anonymous Channel such as Homomorphic Encryption, MIX-net and blind signature.

Electronic voting scheme consists of three main stages initialization stage, voting stage, and counting stage. The stage can consist of more phases [17].

- **Initialization stage**:

  At this stage, authorities set up the system. They announce the elections, formulate the question and possibilities for an answer, create a list of eligible voters, and so on. They generate their public and secret keys, and publish the public values.

- **Voting stage**:

  Voters are casting their votes. The voter communicates with authorities through the channels he can use, forming a ballot containing his vote. Finally he sends his ballot to its destination.

- **Counting stage**:

  Authorities use their public and secret information to open the ballots and count the votes. They publish the result of elections.

According to chapter 2 there are a number of security requirements electronic voting protocols trying to meet. The most "difficult" property of the voting scheme seems to be privacy If the requirement of the privacy is omitted, it turns out not to be hard to design a voting scheme that achieves the remaining properties.

Privacy means that the link between the voter and his vote is disposed or Inaccessible to everyone (including authority) this can be accomplished in three ways [17]:

1- It is easy to see the vote, but it is impossible to trace it back to the voter.

2- It is impossible to see the actual vote, but it is easy to see the identity of the voter.

3- Both seeing the actual vote and obtaining the identity of the voter is Impossible or computationally infeasible.

3.2 ANONYMOUS CHANNEL

As introduced in chapter 2, voting stage is a composition of the registration Phase and the voting phase. Anonymous channel schemes are very popular in practice due to their efficiency and their support for any type of encryption. They are used to conceal the identity of the sender. Usually ballots and identifying material are passed through anonymous channels. In the voting phase, the voter sends a ballot containing the token and his vote through the anonymous channel to the authority. The authority will not accept the ballot with invalid token or with the token that has already been used. As no one (even the authority) can make any connection between the voter and the token or trace the casted ballot back to the voter, no one can deduce anything about how the voter voted. Hence the privacy is achieved [17].

3.3 MIX-NET AND HOW IT WORKS

A mix net is a multistage system that accepts an input batch of quantities and produces an output batch containing the cryptographically transformed, permuted input batch.

The change of appearance and the random reordering of the batch by the mix net prevents trace back from output to input, hence achieving untraceability between the input and output batches [20].

MIX servers protect anonymity of voters from adversaries eavesdropping (or actively plotting) on communication channels linking these servers. They cannot protect against adversaries with access to communication channels linking voters with the first MIX server. MIX-nets implement an anonymous channel which is able to satisfy many voting properties. See Primitive 1 for description anonymous channel used in these voting schemes [18].

Primitive 1: MIX-nets channel

Parties: n senders, one receiver

- Each sender starts with a message.
- Each sender sends his message to the first MIX server.
- The last MIX server sends all the messages to the tally.

Abstractly a mix-net should achieve these 3 goals: A mix-net should ensure that the output corresponds to the input (the correctness property); an observer should not be able to link an input element to a given output element this property is known as privacy; a mix-net should be robust i.e. provide a proof that it has operated correctly which can be verified by all parties [2].

3.3.1 Application to Electronic Voting

When processing votes, it is desirable that once the encrypted votes are un-encrypted, no one will be able to match the unencrypted vote with the voter, not even the authorities responsible for decrypting and tallying. Mix-nets, is able to achieve this [19].

3.3.2 Advantages

The use of mix-nets can allow for privacy property. In the scheme described above, compromised voting equipment will be unable to match a particular vote to a voter. In addition, since the vote will be encrypted with multiple mix server keys, it will take more than a single malicious mix server to compromise a voter's vote [19].

3.3.3 Drawbacks

Tallying cannot begin until all voters have cast their vote [19].

3.4 HOMOMORPHIC ENCRYPTION

In our terms, homomorphic encryption is an algebraic way of implementing very special anonymous channel. The scheme is only computationally secure which practically means

that is it very hard to make it receipt-free. For our purpose all the need is description of the anonymous channel, See primitive 2 [18].

Primitive 2: Homomorphic channel

Parties: n senders, one receiver

- Each sender starts with a message $m_i \in \{-1,1\}$.
- Sender i sends $E_i(m_i)$ to the tally.
- Tally computes $\sum_i m_i$ which is a result of the elections.

Primitive 2 does not evade our definition because it's made it very open, hence can consider homomorphic channel as an anonymous channel. It clear that it can be useful in designing voting schemes, on the other hand, it can be used in a different situation. Even in voting schemes it can be used only for elections with two candidates [18].

3.4.1 Application to Electronic Voting

The schemes based on homomorphic encryption use homomorphic methods to encrypt the votes. Then the voter sends his vote through public channel. To get the sum of the votes, authorities simply multiply the votes [19].

3.4.2 Advantages

The biggest advantage of using homomorphic encryption is that the tallying procedure is very simple. In addition, another advantage over mix-net based voting schemes is that the votes can be tallied before all the votes have been cast without losing any security properties [19].

3.4.3 Drawbacks

The main issue in this scheme is to achieve receipt freeness [19].

3.5 BLIND SIGNATURES

The concept of blind signature was introduced by Chaum in his paper "Blind Signatures for Untraceable Payment" [2] as a form of digital signature in which the message is authenticated without knowing the content of the message. The signer of the message cannot derive the correspondence between signing process and the signature which is later publicly available hence making this type of signature unlink able [2].

Blind signatures allow a person to sign an encrypted message without decrypting it. In the voting schemes an authority signs the vote and sends it back to the voter as a proof that his vote is valid and was kept a secret. The authority must have a unique signature. Anyone can verify that the signature is correct [19]. See Primitive 3 [18].

Primitive 3: Blind signatures

Parties: n senders, one receiver

- Each sender starts with a message; he blinds the message.
- Each sender sends his message to the receiver.
- Receiver sings each message and sends the signature back.
- Sender removes blinding from this message obtaining a valid signature for his message.

3.5.1 Application to Electronic Voting

An authority assists the voter in creating a token, which will be used later to vote. This interaction can be done only once, so that the voter obtains only one token. The token stays private only to the voter. The validity of the token is verifiable by anyone. The voter sends his token and his vote through anonymous channels to the authority. To ensure that the voter is eligible to vote and has voted only once, the authority will verify that the token is not broken or already in use.

The structure of the token is specified in the voting schemes and the token might contain various encrypted information about the user. However it must not be possible to extract information about the voter's identity. Each voter must obtain a unique token [19].

3.5.2 Advantages

The biggest advantage of blind signatures is efficiency. The voting phase as well as tallying phase is more efficient when compared to other schemes [19].

3.5.3 Drawbacks

Despite the increase in efficiency, there is less interest in blind signatures as a whole compared to mix-nets. One drawback is that many common voting schemes using blind signatures are unable to ensure the universal verifiability property. This is due to the inability to handle voters who abstain from voting. In this case, malicious authorities may impersonate the voter. It fails universal verifiability because an outsider will not be able to notice this [19].

3.6 CHAPTER CONCLUSION

In this chapter the definition of Anonymous Channel and three schemes for electronic voting based on it (Homomorphic Encryption, MIX-net and blind signature) and how it's work and what security services that achieved on each one.

Describe three the main stages of any Electronic voting schemes (initialization stage, voting stage, and counting stage).

How authenticated message without knowing the content of the message by Blind Signature.

4.1 INTRODUCTION

This chapter about the analysis of the E-Voting system using the Unified Modeling Language.

4.2 ANALYSES

Figure 4.1: Describe the operations that can be performed by System users.

- Voter operations include:

  - Registrations, Login, Voting, Getting Signature, Provide key, Verify vote counting.

- The Administration operations include:

  - Login, Provide elections result.

Figure 4.1: Describe the operations that can be performed by System users.

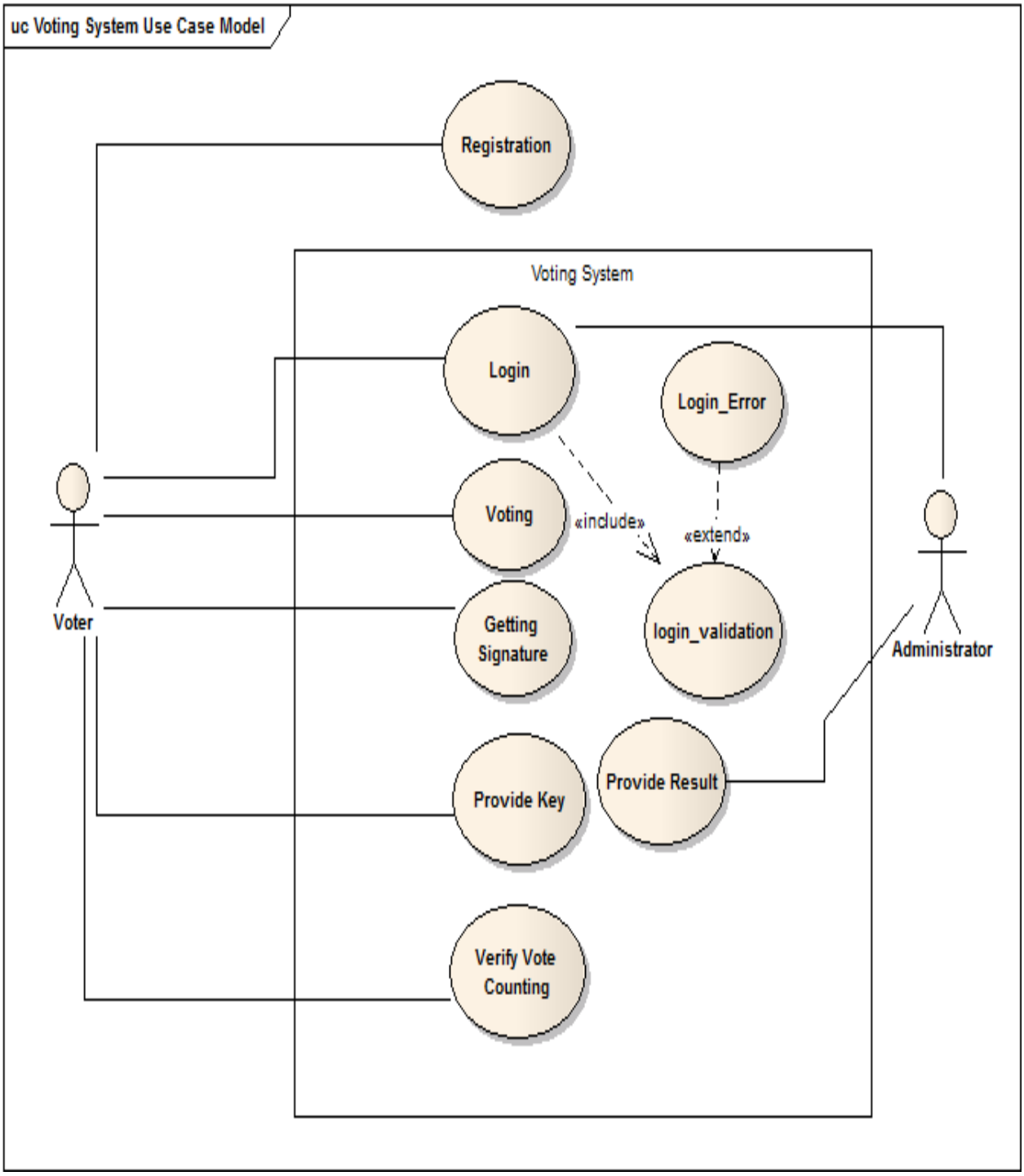


Figure 4.2: Illustrate the sequence of Registration process

- The GUI send Registration form to voters.
- The voter fill registrations form with credential data and send information to administrator via GUI.
- The Administrator server verify that voter is eligible (Sudanese, 18 years of age or above, to be mentally fit, etc.) then save data in Database or deny the registration process.

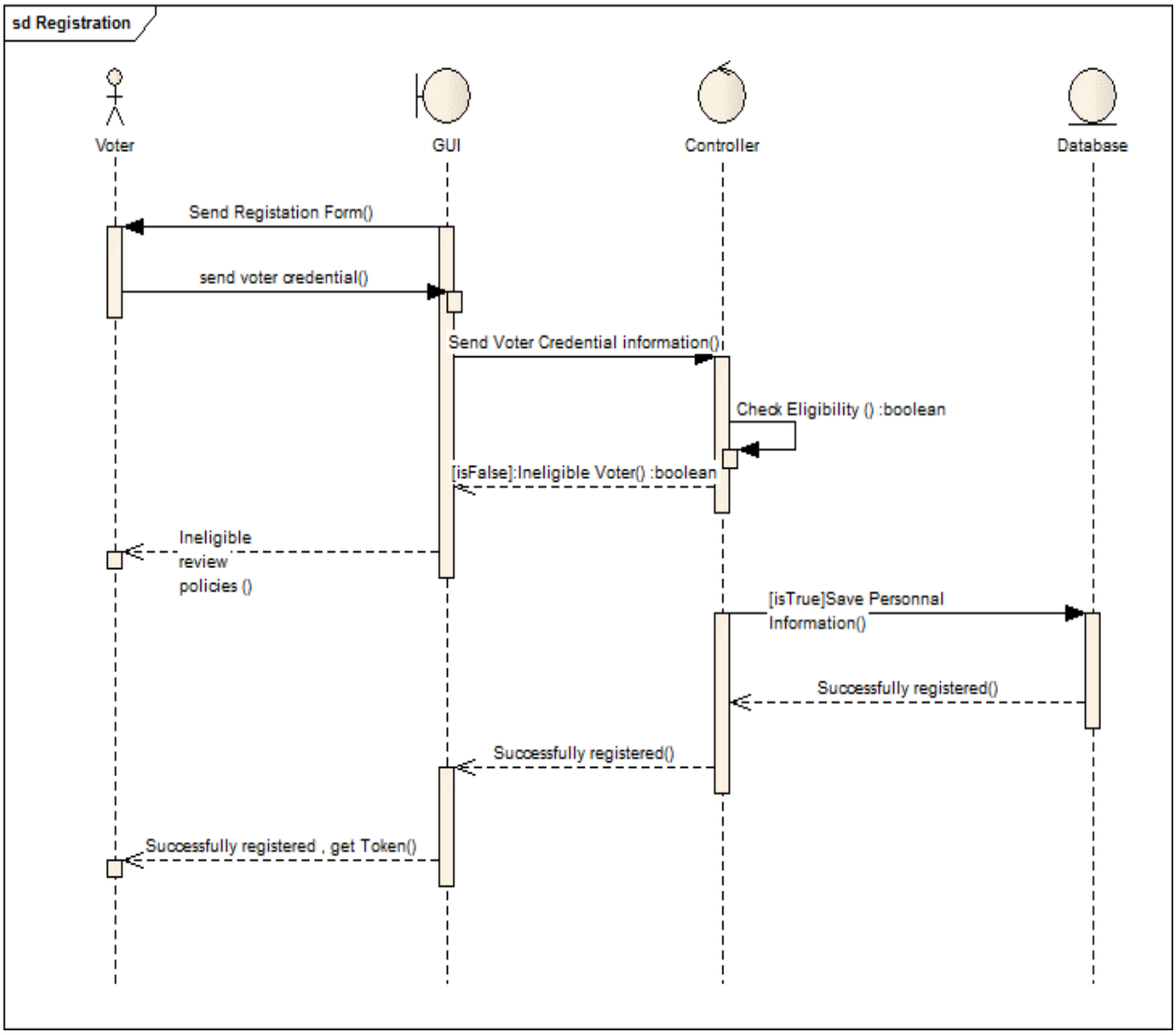


Figure 4.3: Illustrates the sequence login process.

- The GUI send Login form to users (Administrator or Voters).
- The users enter the National number and password and then send it to administrator Server via GUI.
- The administrator Server check authority by searching database to allow or deny login.

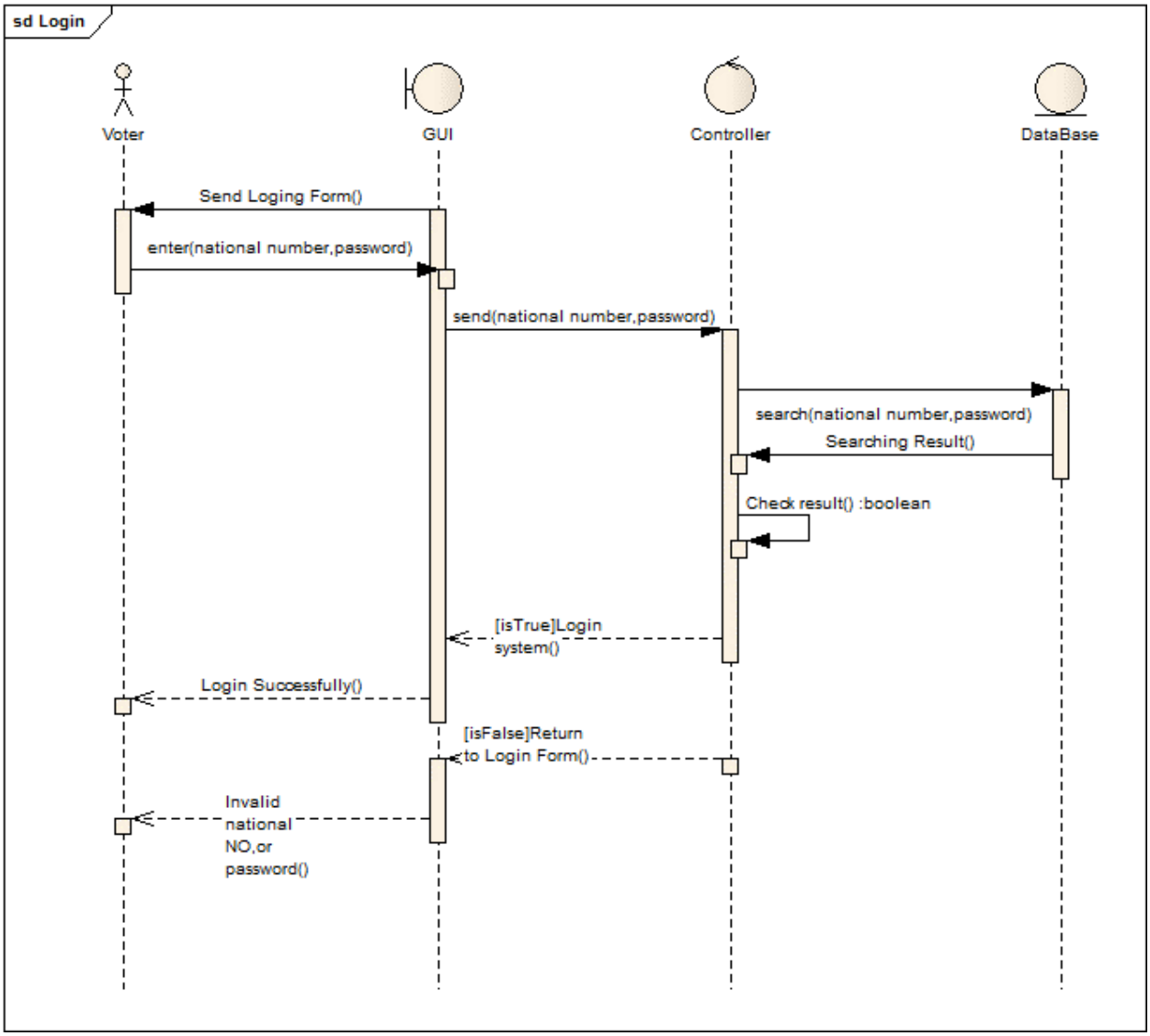


Figure 4.4: Illustrates the sequence voting process.

- The GUI send Candidate list to voters.
- The voter choose his candidate and send encrypted blinding vote together with national number to administrator server via GUI interface.
- The administrator server generate signature, send it back to voter and update data base with generated signature.

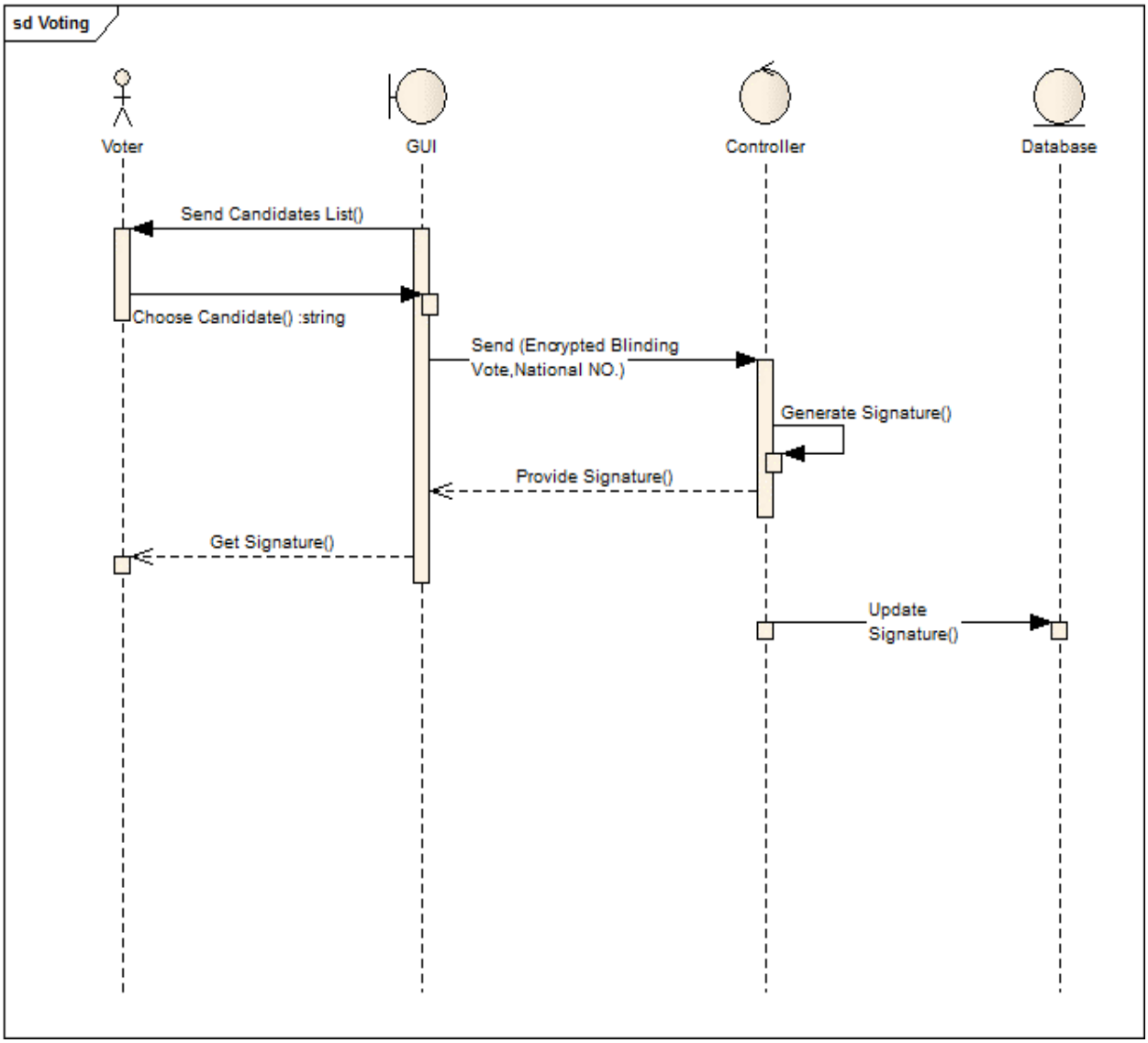


Figure 4.5: Illustrates the sequence of providing vote to collector server (opening phase).

- Voter remove blind and send encrypted vote and his signature to collector server.
- The collector server verify the signature then saving (encrypted vote, signature, list No.) on data base return successfully operation to voter or false in case invalid signature.

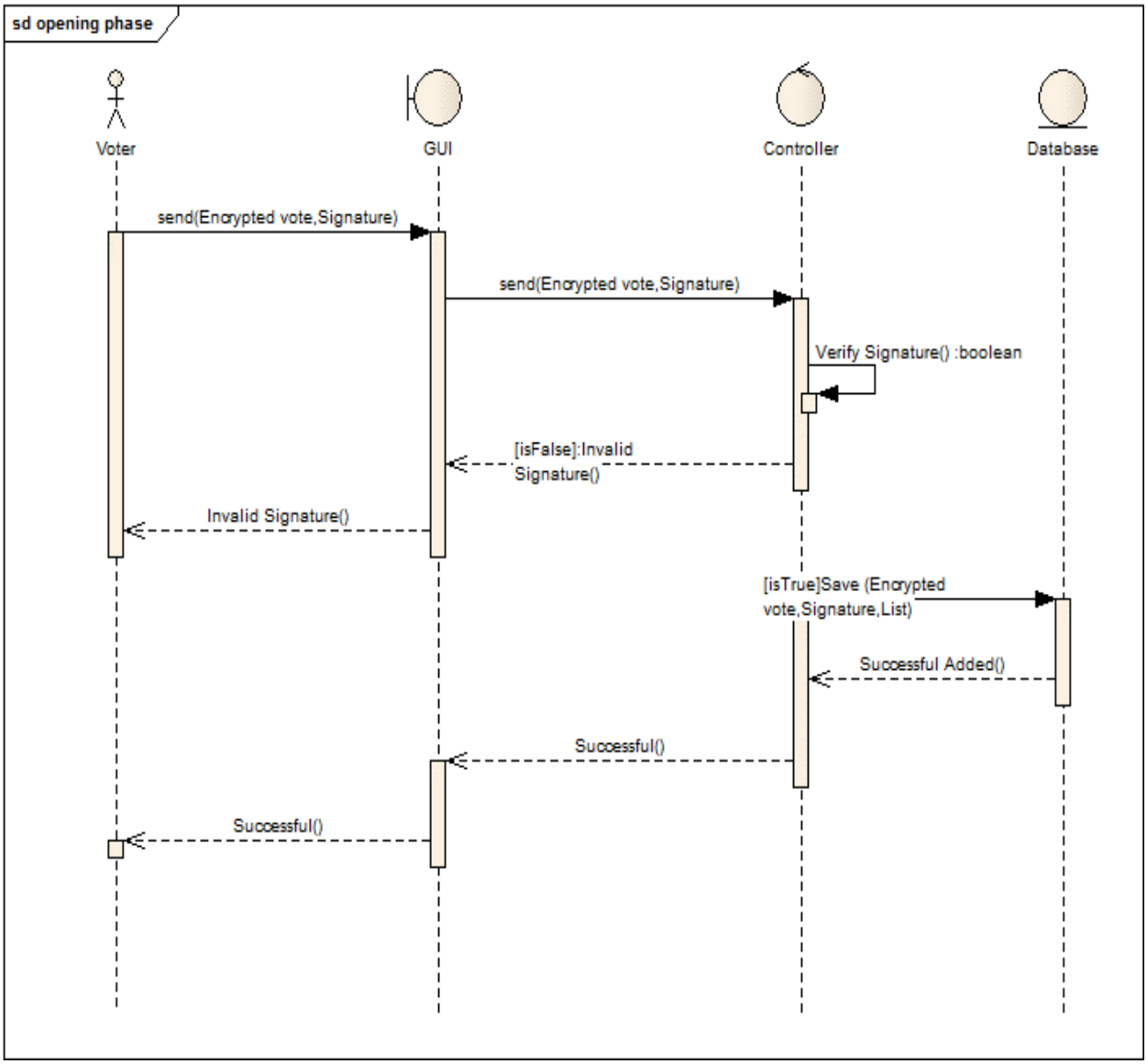


Figure 4.6: Illustrates the sequence of decryption process (counting stage).

- The GUI send Decrypt form to voter.
- The voter enter (list number, key) and then send it to collator server.
- The collector server using list number to find encrypted vote to decrypted then increasing percentage to corresponding candidate and acknowledging to success to voter or replaying invalid key or list number.

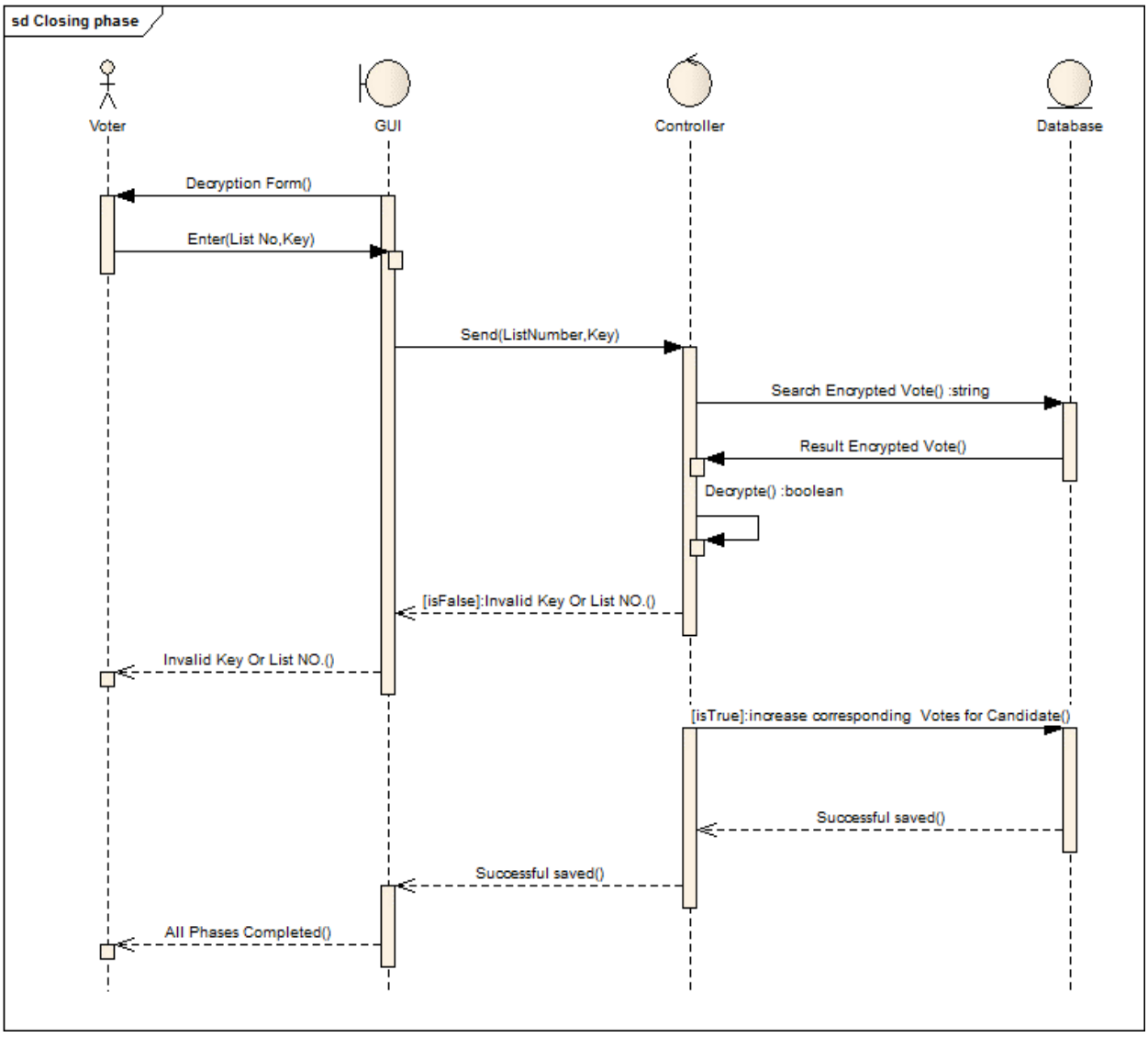


Figure 4.7: Illustrates the sequence of verifying process.

- The voter send signature to collector server.
- The collector search the signature in database then return found or not to voter.

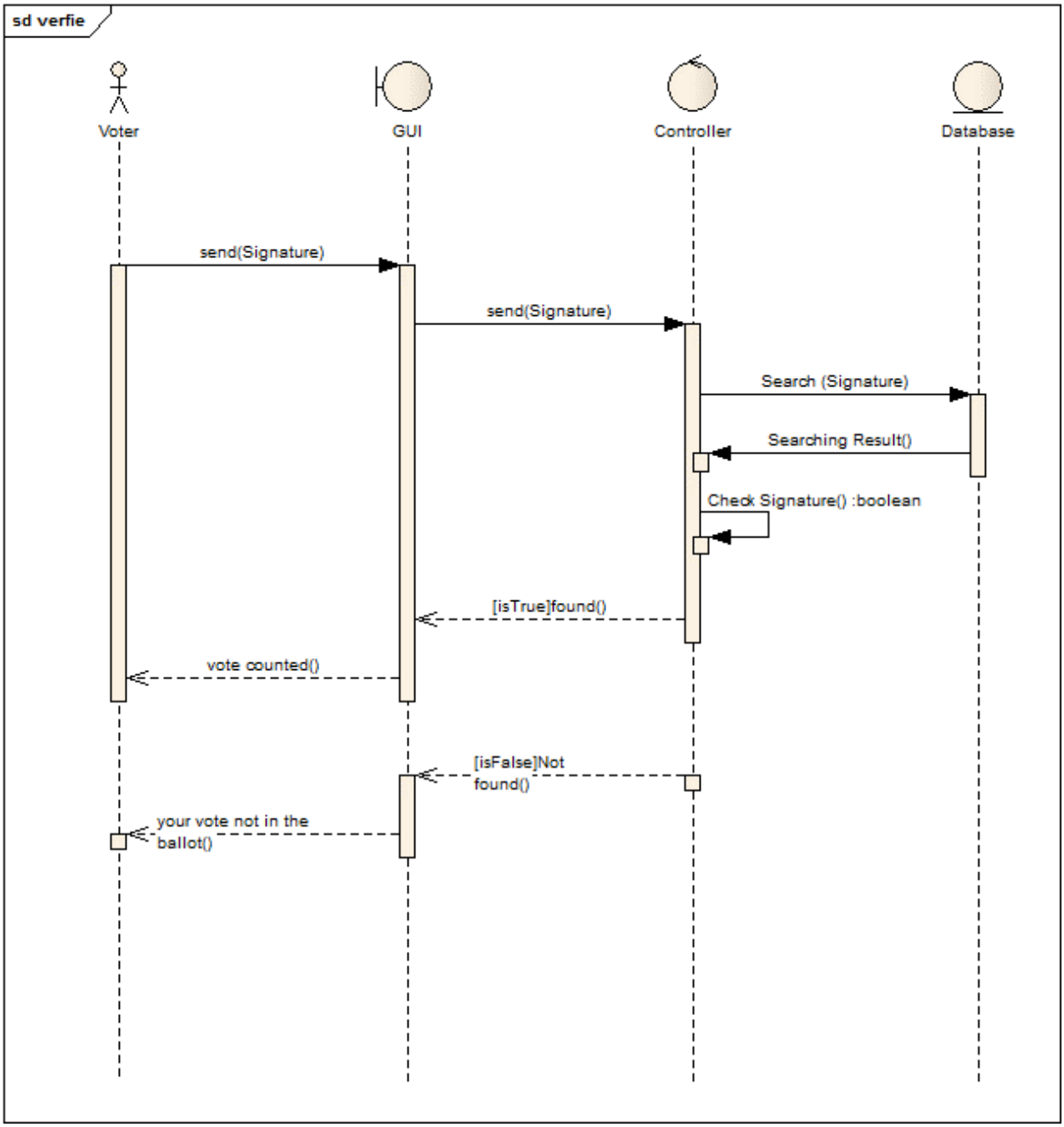


Figure 4.8: Illustrates the sequence of election result process (the basic operations between administrator and collector server).

- GUI send result interface to the administrator which then request for result from collector server.
- The collector counting votes and send result back to the administrator as list of candidate with their vote percentage.
- Then the admin display this result to public.

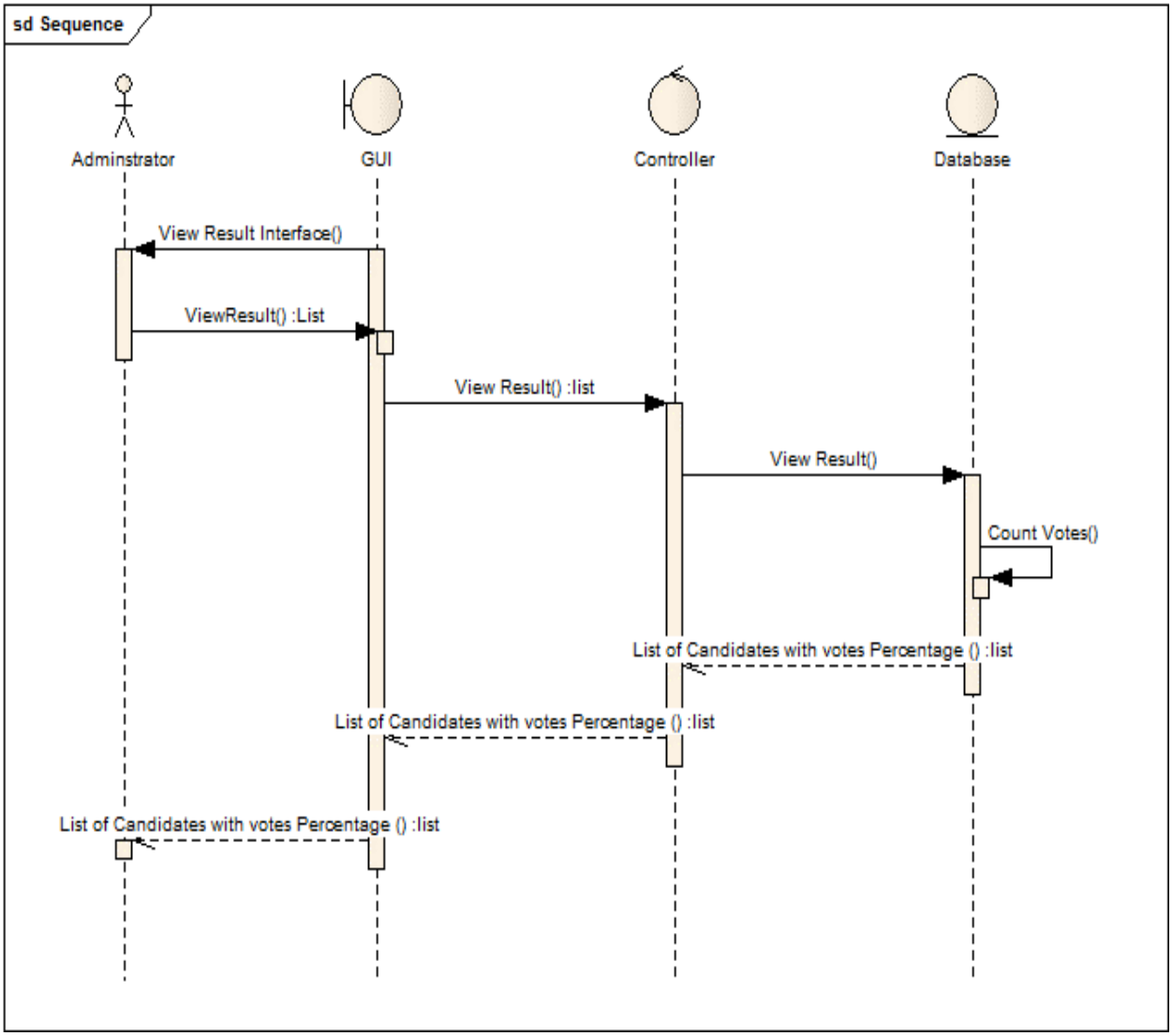


Figure 4.9: Illustrates group of Activity that users of system use it in registration process.

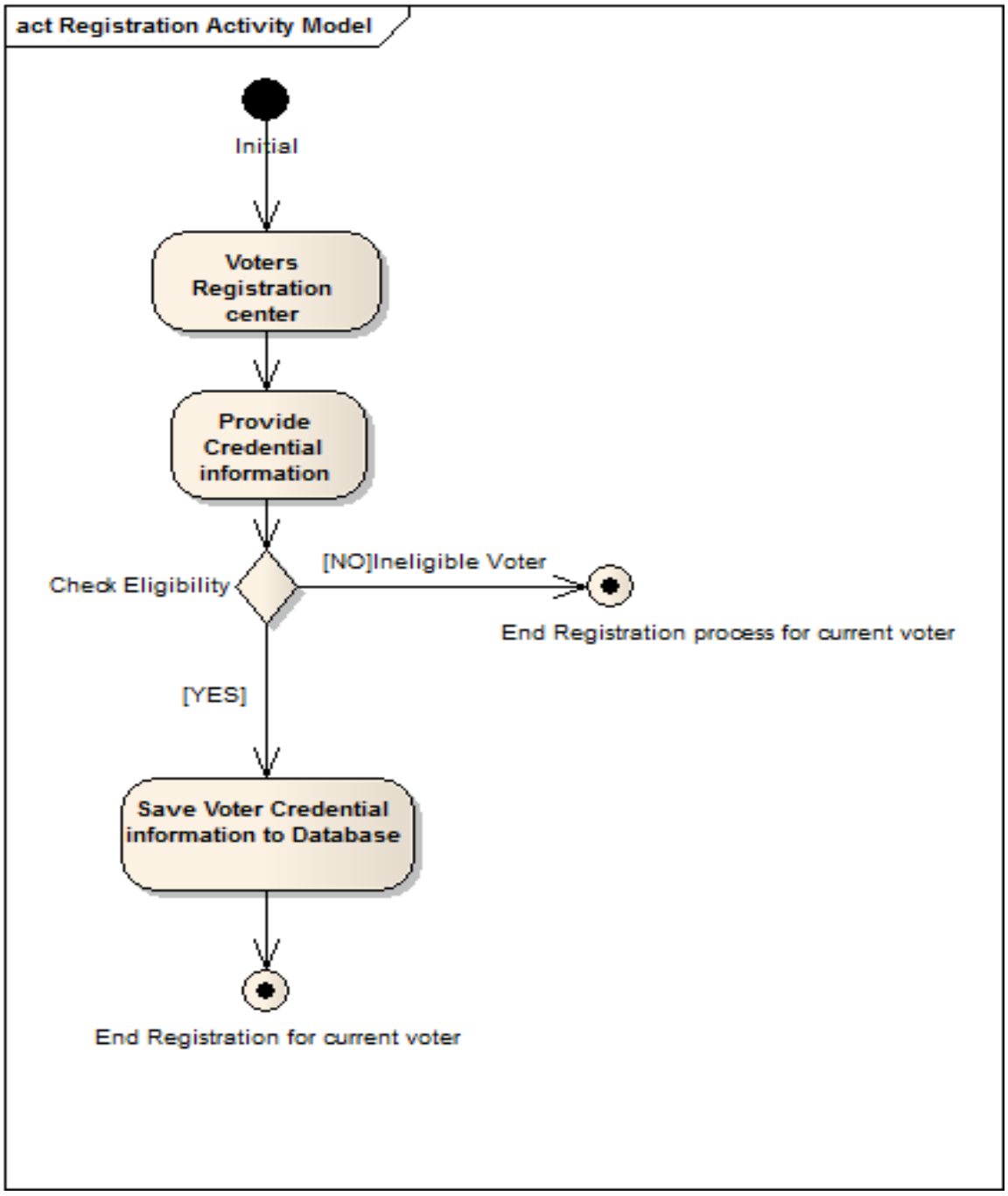


Figure 4.10: Getting signature

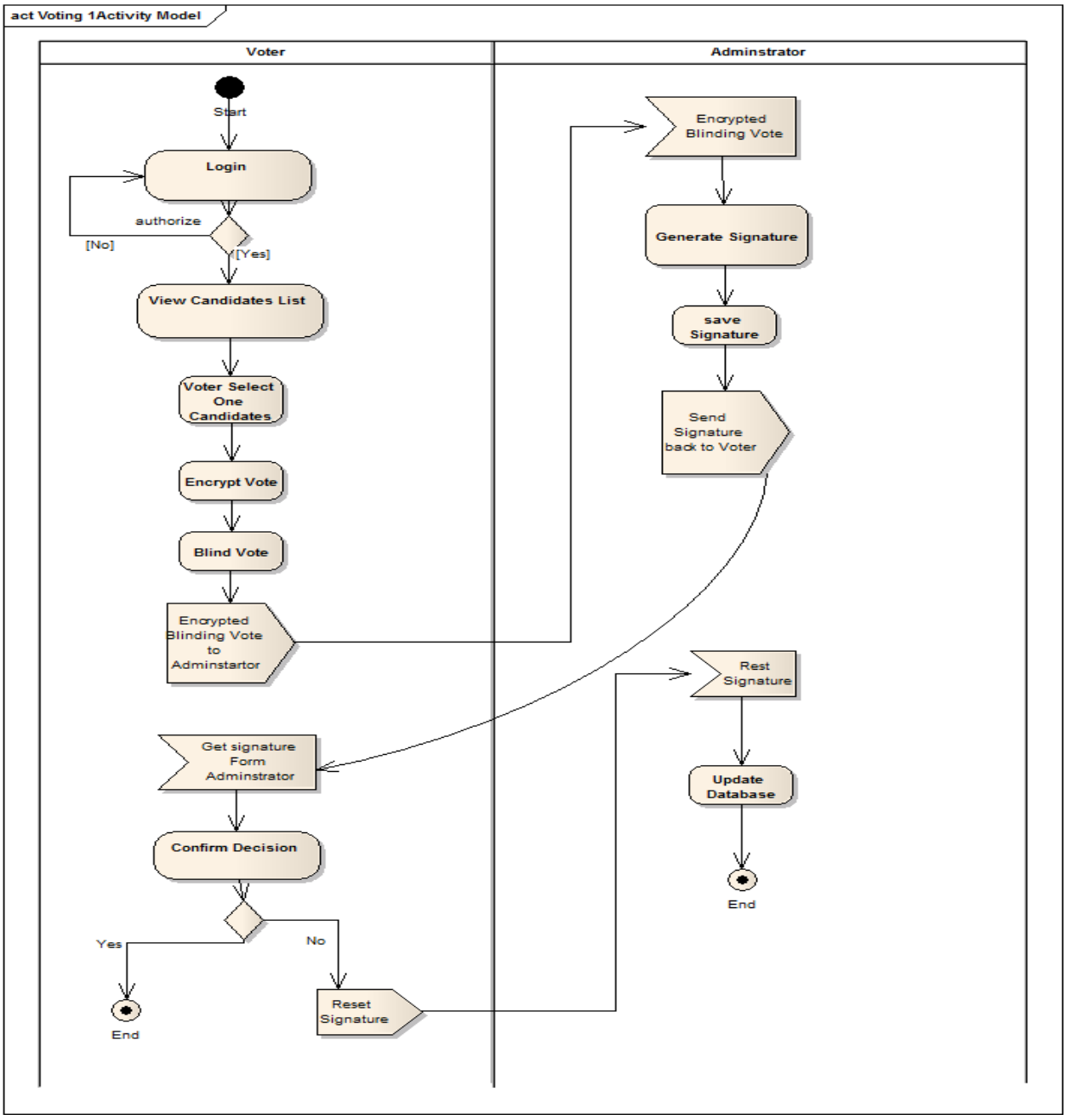


Figure 4.11: Opening phase.

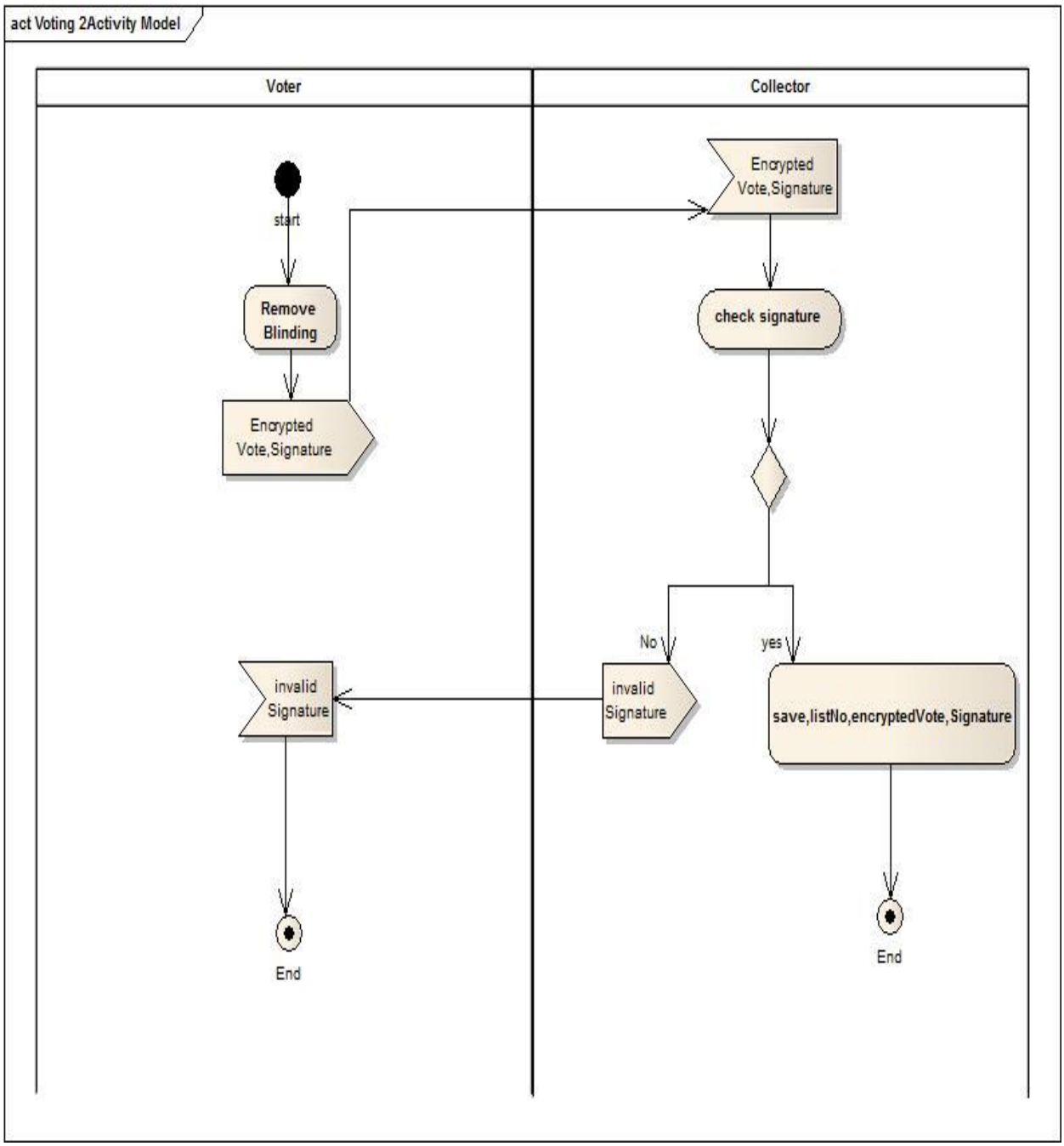


Figure 4.12: Counting phase.

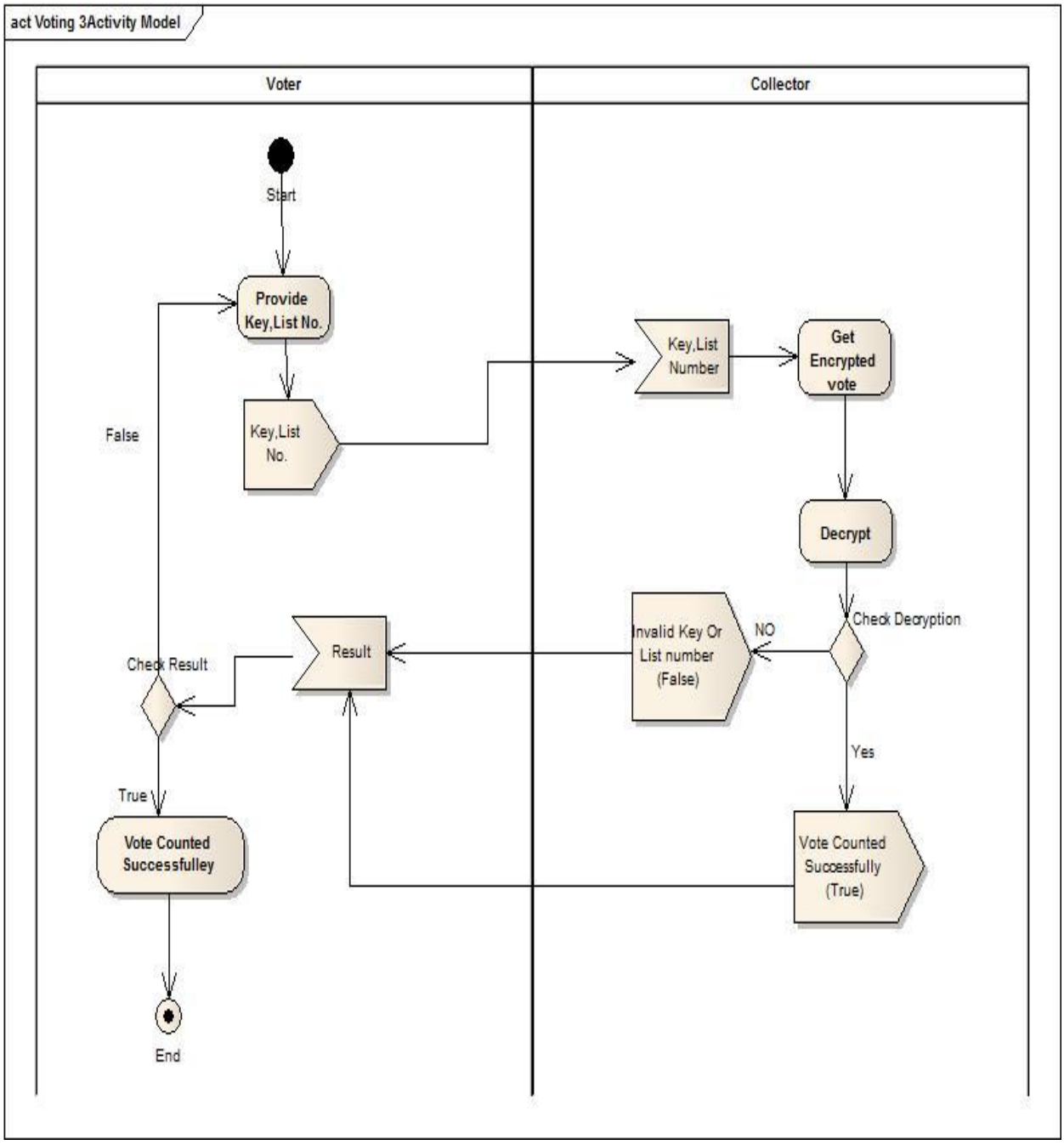


Figure 4.13: Illustrates group of Activity that provide voter to verify his vote counting.

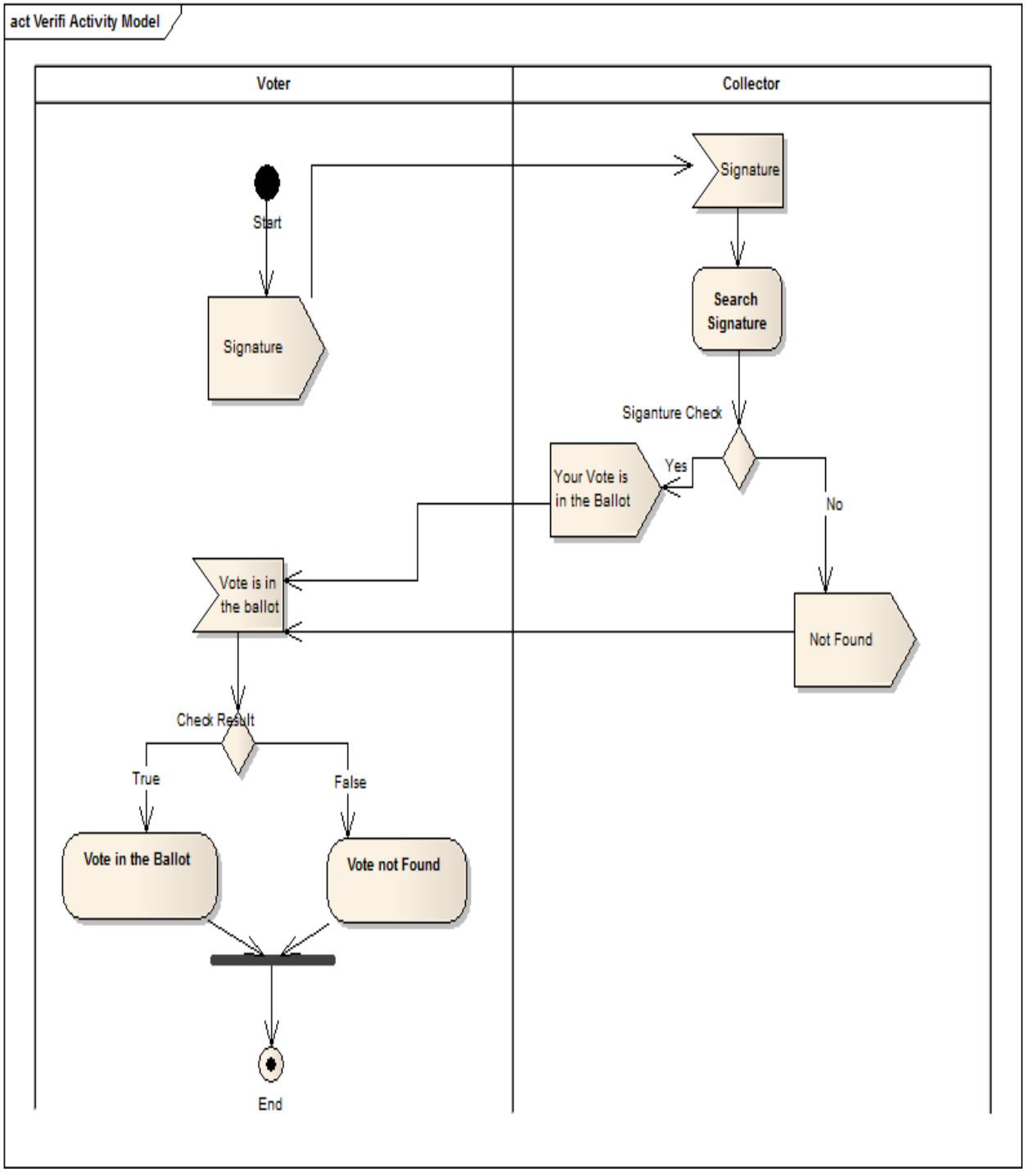
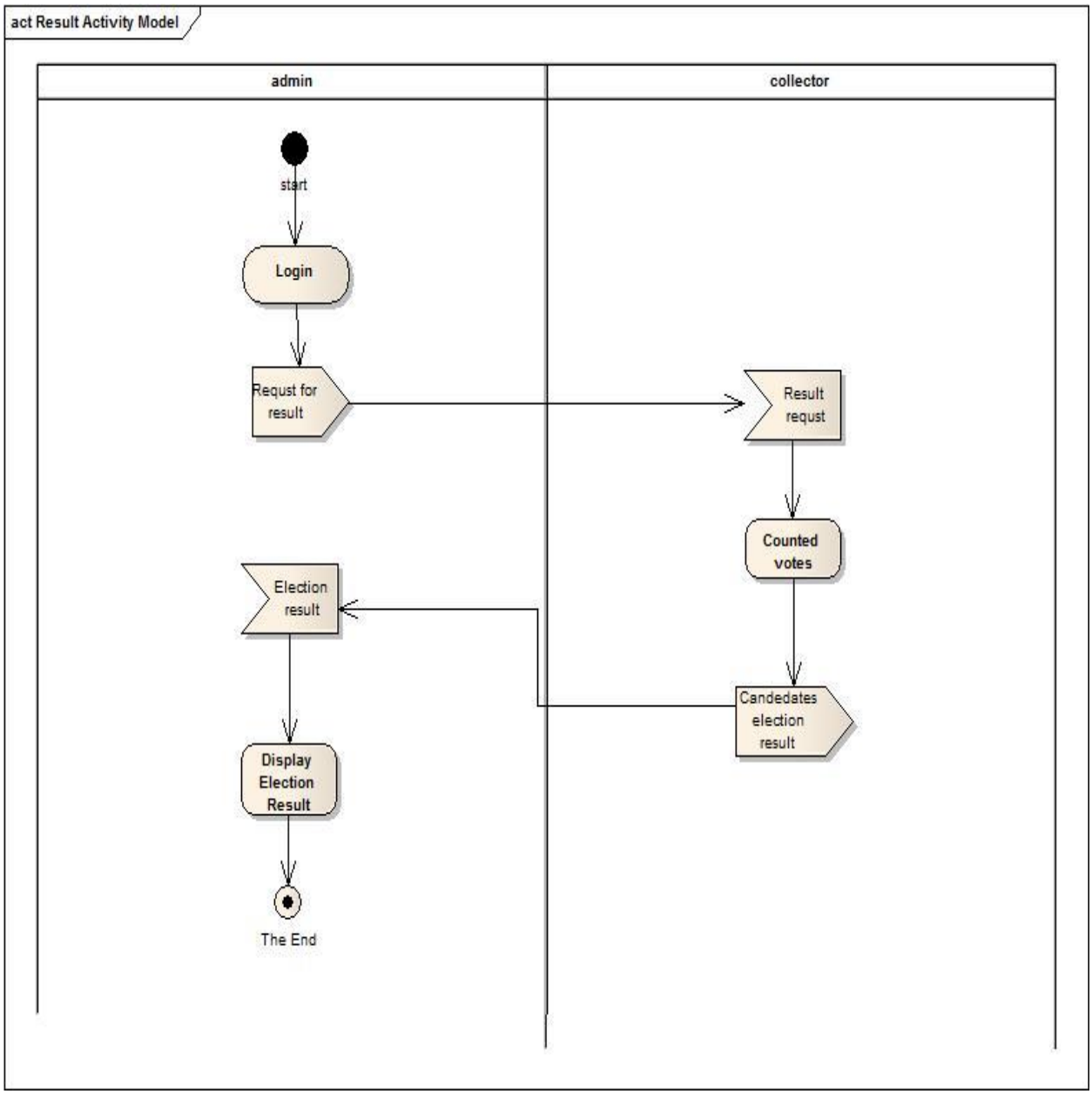


Figure 4.14: Illustrates group of Activity that support the admin to display final election result.



5.1 INTRODUCTION

This chapter discusses the tool and technologies used in the study.

5.2 MVC [25]

The Model-View-Controller (MVC) pattern is an architectural design principle that separates the components of a Web application. This separation gives you more control over the individual parts of the application, which lets you more easily develop, modify, and test them. ASP.NET MVC also improves the testability of ASP.NET Web applications by supporting test-driven development (TDD).

ASP.NET MVC is part of the ASP.NET framework. Developing an ASP.NET MVC application is an alternative to developing ASP.NET Web Forms pages; it does not replace the Web Forms model.

5.3 C#

C# is intended to be a simple, modern, general-purpose, object-oriented programming language.

It is a multi-paradigm programming language encompassing strong typing, imperative, declarative, functional, generic, object-oriented(class-based), and component-oriented programming disciplines. It was developed by Microsoft within its .NET initiative and later approved as a standard by Ecma (ECMA-334) and ISO (ISO/IEC 23270:2006). C# is one of the programming languages designed for the Common Language Infrastructure.

Writing in C# also gives one access to all the .NET Framework class libraries, which are quite extensive. Also it easy to integrate with components written in other languages

5.4 JAVA SCRIPT

Is a high level, dynamic, untyped, and interpreted programming language. Alongside HTML and CSS, it is one of the three essential technologies of World Wide Web content

production; the majority of websites employ it and it is supported by all modern web browsers without plug-ins. supporting object-oriented. JavaScript is also used in environments that are not web-based, such as PDF documents, site-specific browsers.

5.5 BOOTSTRAP

Is a free and open-source collection of tools for creating websites and web applications .It contains HTML- and CSS-based design templates for typography, forms, buttons, navigation and other interface components, as well as optional JavaScript extensions. It aims to ease the development of dynamic websites and web applications.

Bootstrap is a front end framework, that is, an interface for the user, unlike the server-side code which resides on the "back end" or server, and using **CSS3** to be suit with mobile devices with a variant size.

5.6 ENTERPRISE ARCHITECT

Enterprise Architect is Visual Modeling Platform for Comprehensive UML analysis and design tool, modeling for business, software and systems. It provide full life cycle modeling and traceability for requirements analysis and design effective, verification and validation and models to entire life cycle, for business, software and Systems.

It is used to assist management to formulate, communicate and govern the strategic change agenda from the high-level purpose and vision through to a detailed technology program and project delivery.

5.6.1 UML

UML is an international industry standard graphical notation for describing software analysis and designs. When a standardized notation is used, there is little room for misinterpretation and ambiguity. Therefore, standardization provides for efficient communication and leads to fewer errors caused by misunderstanding

5.7 CRYPTOGRAPHIC PRIMITIVES

5.7.1 RSA Algorithm

RSA is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers.

5.7.2 Digital Signature

A digital signature is a cryptographic primitive that is used to provide an assurance that the message has not been altered (Integrity) and it comes from a particular signer (Data Origin Authentication). A digital signature also provides non-repudiation service which means that a signer cannot deny signing a message, and a recipient of a signed message can always present it to a third party in cases of misunderstanding to prove the origin of the message.

A digital signature has a signature key which is a secret parameter known only to the signer this is what guarantees the non-repudiation service [24]. It also has a verification key which the recipient can use to verify the legitimacy of the signature.

5.7.3 Blind Signature

It is a form of digital signature in which the content of a message is disguised (blinded) before it is signed. Blinding Signature allow the requester to hide the message from everyone, including the signer. The signer is requested to sign a message blindly, not knowing what he signs.

5.7.4 Advanced Encryption Standard

It is a symmetric encryption algorithm based on a design principle often referred to as a substitution-permutation.

This is simply means that the design is based on a serious of linked operations, some of which involve replacing inputs by specific outputs (substitution) and others involve shuffling bits around (permutation).

AES performs all its computation on bytes rather than bits.

5.7.5 Cryptographic Hash Function

It is a hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone. The input data is often called the message, and the hash value is often called the message digest or simply the digest.

5.7.6 Wireshark

It is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development.

6.1 INTRODUCTION

In this section, the talking will be about Sudanese general election from the registration phase to the tallying phase and during the Pre electoral period, Electoral period and Post-electoral period.

General elections were held in Sudan on 13-16 April 2015 to elect the President and the National Assembly. As it mentioned in **chapter 1,** the President is elected using the two-round system; if no candidate gains a majority of the vote in the first round, a run-off will be held.

6.2 PRE- ELECTORAL PERIOD

6.2.1 Registration phase [26]

The basic component of a credible electoral is voter registration in accurate and comprehensive manner.

This phase starts with determining the eligibility of voters:

1- Voter registration determines, prior to polling date, who is eligible to vote and who is not. Ineligible voters will not be authorized to register. Only those persons whose names are found in the register are allowed to vote.

2- This phase has many benefits. For instance, some of the questions that can be answered are: how many polling centers, their location and consequently the number of staff and materials needed. Thus determining the eligibility of voters facilitates operational planning. Another benefit of this phase is make it easier (or voters to know the location of polling centers on Election Day as most registration centers will become polling centers on Election Day).

6.2.2 Sudanese registration process principle [26]

1. Registration is personal and proxy registration is not allowed. Anyone who wishes to register should come in person for registration. No proxy can represent another person in

registration.

2. Registration occurs only once. A person can only register once. Registration by the same person in more than one registration center is not permitted. If the voter has a house in more than one constituency, he/she must choose only one location to register and it must be where he/she was residing during the three months preceding the registration period.

3. Registration is a prerequisite for voting in elections Inclusion In the voters register is a prerequisite for exercising the right to vote.

4. Inclusiveness. Voting is a constitutional right for all eligible citizens. The voters' register must include as many eligible voters as possible and registration must be accessible to all eligible citizens who are willing to participate in the elections.

5. Registration is public. Registration is conducted in public which will allow monitoring by national and international observers, party agents and representatives of the media as per the rules and procedures set forth by The National Elections Commission (NEC).

6. Registration centers are polling centers. In general, registration centers will become polling centers on the Election Day. Voters should go to the same center where they registered.

7. Head of registration center team determines a person's eligibility to register. The head of the registration center team has the final say to determine whether the person is eligible to register or not. A person deemed ineligible has the right to lodge a complaint.

8. Registration is preliminary and can be challenged during the exhibition period. After the close of the registration process, the preliminary voters register will be publicly displayed. Registered voters can check their names and request corrections on any inaccurate information. Registered voters can object to the inclusion of those they deem ineligible to vote.

6.2.3 Who can register and vote

Anyone who meets all the requirements below has the right to be registered:

1. To be a Sudanese National.
2. 18 years of age or above.
3. To be mentally fit.
4. Resident of The geographical constituency where he/she wishes to register for at least three months before the registration closing date.
5. Not to be registered in any other geographical constituency.

6.3 ELECTORAL PERIOD [27]

Political parties and/or individuals submit to Election Management Body (EMB), which is responsible for planning, organizing and managing elections in the Sudan), names of candidates for the elections. This is done through a formal procedure called **Nomination of Candidates**. The EMB verifies that the candidates meet the criteria specified in the Electoral Law and that there are no public objections to their nomination before placing their names on the ballot.

On the day of the election, each voter goes to the polling center which they did their registration if they intend to vote. As it mentioned it is not possible to register in one polling center and vote in another. The highlight of most elections is when people go to the polls to cast their votes.

For an election to be free and fair, the polling must follow democratic principles (freedom of expression and movement, secrecy of the vote, etc.). Polling sites should be safe, accessible and neutral. The ballots used should reinforce the integrity of the process by providing safeguards against fraud. At polling stations, trained workers are present to ensure that voting takes place in compliance with the electoral law.

Party agents and independent observers can help detect Potential problems, such as discrimination, intimidation and fraud.

Vote counting. It is one of the most crucial stages in the election process.

Failure to complete the count and transmit results in a transparent and accurate manner can jeopardize public confidence in the elections and will directly affect whether candidates and political parties accept the final results.

In the Sudan, party/candidate agents and observers are entitled to watch the counting process. Rules established by **NEC** will also provide for the recording of any complaints about the counting Process. The responsibility and authority to announce election results rests with the EMB.

When counting has been completed, **NEC** will declare preliminary results of the election. Candidates or political parties participating in Sudan's elections have the right to appeal those results to the Court.

According to Sudan's electoral law, **NEC** shall immediately after the appeals process, prepare and declare final election results within 30 days of polling. The results will be published in the official Gazette and in the media.

6.4 POST-ELECTORAL PERIOD

After the end of one electoral process, it is desirable that the EMB evaluate and review the entire process and start preparing for the next electoral event, by proposing necessary charges in the laws and procedures.

6.5 OVERVIEW OF FOO-SCHEME

This section will take a more detailed look at the voting protocol used in this e-voting scheme using the **FOO-SCHEME**. First defining why this scheme has been chosen instead of other voting schemes, and then the full scheme implementation.

6.5.1 Why Foo Scheme

In **Chapter 3** the introduction has mentioned that E-Voting schemes based on **Anonymous Channel** (Homomorphic Encryption, MIX-net, and blind signature). Of

course this is not all proposed voting scheme but this is the most important ones of them, schemes introducing new ideas and the schemes efficient in practice.

Schemes using homomorphic encryption have more security properties than FOO (our proposal scheme), but communication complexity is quite high, and also these schemes were designed mainly for yes-no voting.

Schemes using MIX-nets based on idea that in practice can rely on some set of trusted authorities, although the trust into these authorities is not absolute, it require multiple server to be implemented well to provide privacy of voter.

Because of these the focusing in schemes based in blind signature.

6.5.2 Schemes Based On Blind Signatures and Anonymous Channel

Schemes using anonymous channel and blind signatures are very popular in practice due to their efficiency and their support for any type of the voting. A price is paid for this efficiency: the voter has to act in more rounds (registration, voting, counting, verifying whether his vote has been counted, complaining...).

Since **Chaum** introduced the concept of blind signature [28] a lot of electronic voting schemes have been proposed based on this blind signature (FOO-Scheme, JL-Scheme and Radwin-Scheme).

FOO chosen based on of achieved properties (Privacy, Eligibility, Individual Verifiability etc.), efficiency, and also it has modification allowing to achieve more security requirements than JL-Scheme and Radwin-Scheme.

6.5.3 Foo Scheme

The main entities of this scheme are the voters, an administrator and a counter who is responsible for vote tallying. The voter and the counter communicate through an anonymous channel, this counter can be a public board and the anonymous channel allows the communicating party to remain anonymous throughout the communication.

In this scheme [2] different cryptographic primitives were used such as digital signature, blind signatures and hashing function. Below is an outline of all the stages and processes involved in this scheme [2]:

Preparation Phase: The voter fills the ballot, using the blind signature technique, the voter blinds the message and sends to the administrator to get the administrator's signature.

Administration Phase: the administrator signs the message in which the voter's ballot is hidden and returns the signature to the voter.

Voting Phase: On receiving the ballots signed by the administrator, the voter sends it to the counter anonymously.

Collecting phase: The counter publishes a list of received ballots, this list could be published on a bulletin board for example.

Opening Phase: The voter opens his vote by sending his encryption key anonymously.

Counting phase: The counter counts the vote and announces the result.

6.5.4 Achieved Properties

Notations of the protocol

IDi: Identification of the voter V_I.

Ki: Voter key.

V: The vote.

Eligibility. Only eligible voters are allowed to gain the token. Invalid tokens and invalid votes will be detected. The token cannot be used multiple times, so the voter can vote at most once. Therefore, the eligibility is achieved.

Privacy. The voter's privacy is preserved even if the administrator and the collector conspire: the relation between the **voter's ID** and his ballot is hidden by the blind signature scheme. The voter sends his **ballot** as well as the **key** through anonymous channel, so no one can trace it back.

Individual Verifiability. The scheme is individually verifiable: the voter can check whether his ballot is on the list published by the collector, and whether his **Ki**, vote **V** has been added to the list.

Universal Verifiability. The scheme is not universally verifiable – if some voters abstain from voting after the registration phase, the administrator can add its own votes instead of theirs. The voter has to participate in three rounds: registration, voting and opening.

Fairness. This election scheme is fair – counting of the ballots does not affect the voting, as the counting stage comes after the voting phase.

Receipt-Freeness. Anyone who gets to know the voter's token can easily find out his vote in the list published by the collector at the end of the election. Therefore, the receipt-freeness is not achieved.

6.5.5 Limitations of the Foo Scheme

This scheme requires voters to participate at all stages of the election. The too much involvement by voter's requirement is not practical especially the fact that the scheme expects voters who did not vote in the first instance to monitor the election to ensure votes were not added for them. This implies that if a voter abstains from voting a malicious authority can stuff the ballot by adding votes for voters, this violates the accuracy property of an electronic voting scheme [7].

6.6 OVERVIEW OF THE SECURE ELECTRONIC VOTING USING FOO-SCHEME

This section do a high level overview of the voting scheme. The process is divided into two main Phases:

1. Registration Phase.
2. Voting Phase, and the Tallying Phase.

6.6.1 Registration Phase

As mentioned at the start of this chapter an accurate and comprehensive voter register is a basic component of a credible electoral. The first problem is how to do an online authentication since proposal solution present a full online voting system.

There is a lot of research and methodologies in online authentication such as Fingerprint, Voice Recognition or special devices given to authenticated user. All this procedures require special devices and need more cost to implemented .so there is a need for another way to do the registration and corresponding authentication in full trusted manner.

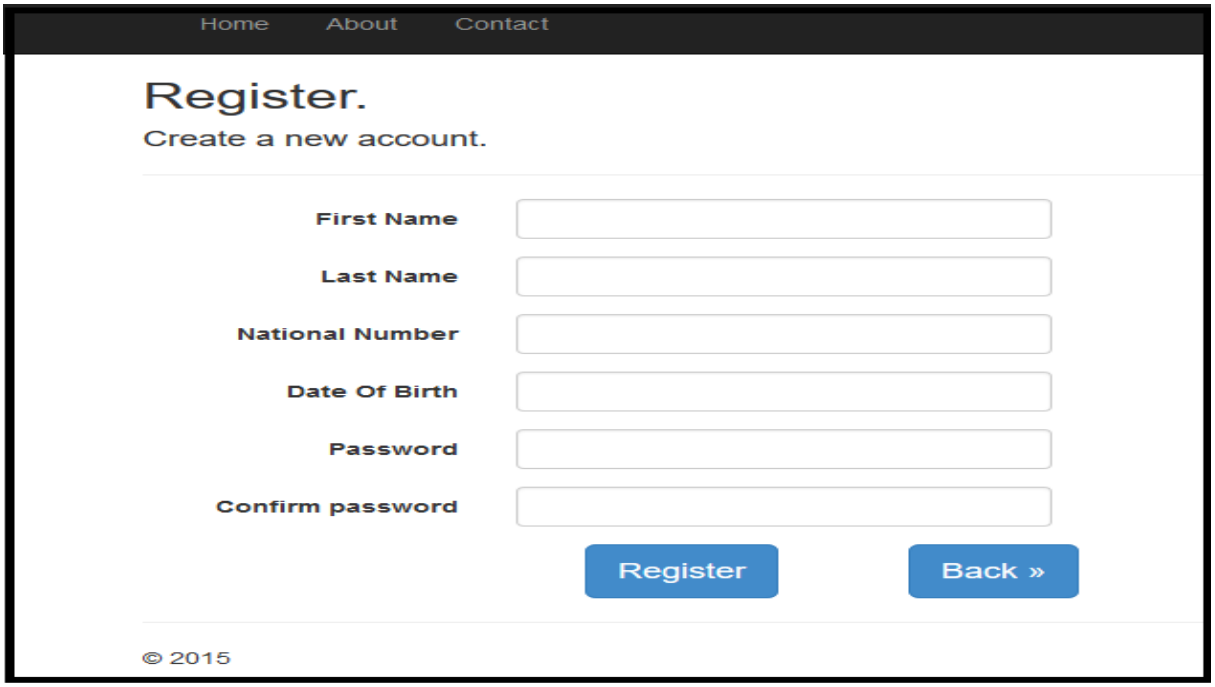
Proposal solution is to separate the registration phase in special system implemented in the registration center.

Registration System

Create a complete registration system that well be implemented in the registration center. In this system the following actions are carried out:

1. Voter goes to the Registration center with his legitimate credentials and Registration Authority (RA) verifies the credentials to check if the voter is eligible.
2. After RA verifies eligibility the voter now enter to registration system provide credentials information.
3. Voter choose a unique password and this well be its token to login to voting system.
4. This will be the only process performed physically, all this to provide an authentication and to be sure only eligible voter will vote (Sudanese, 18 years of age or above, to be mentally fit, etc.).

Figure 6.1: Registration System.



6.6.2 Voting Phase

Create another system for voting which involve:

1- Authentication process.

2- Voting phase.

3- Opening phase.

4- Counting phase.

Authentication Process

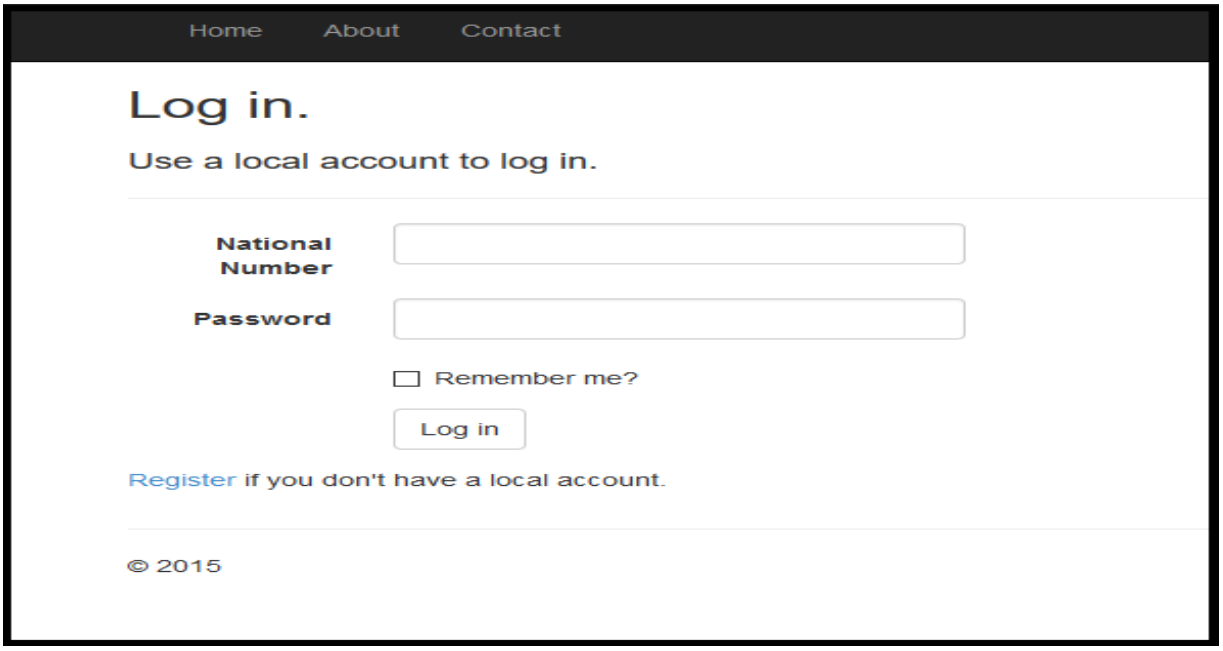
After the voter complete the registration process, and get his/her token he/she is now allow to vote in any time and any place accessing online voting system and perform authentication process:

1- Administrator server send login interface to the voter.

2- Voter proved his/her token (National number, password).

3- Administrator server check and verify token.

Figure 6.2: Authentication process.



Voting Phase

After administrator verify and validate token, provide list of candidate.

In this process the following actions are carried out:

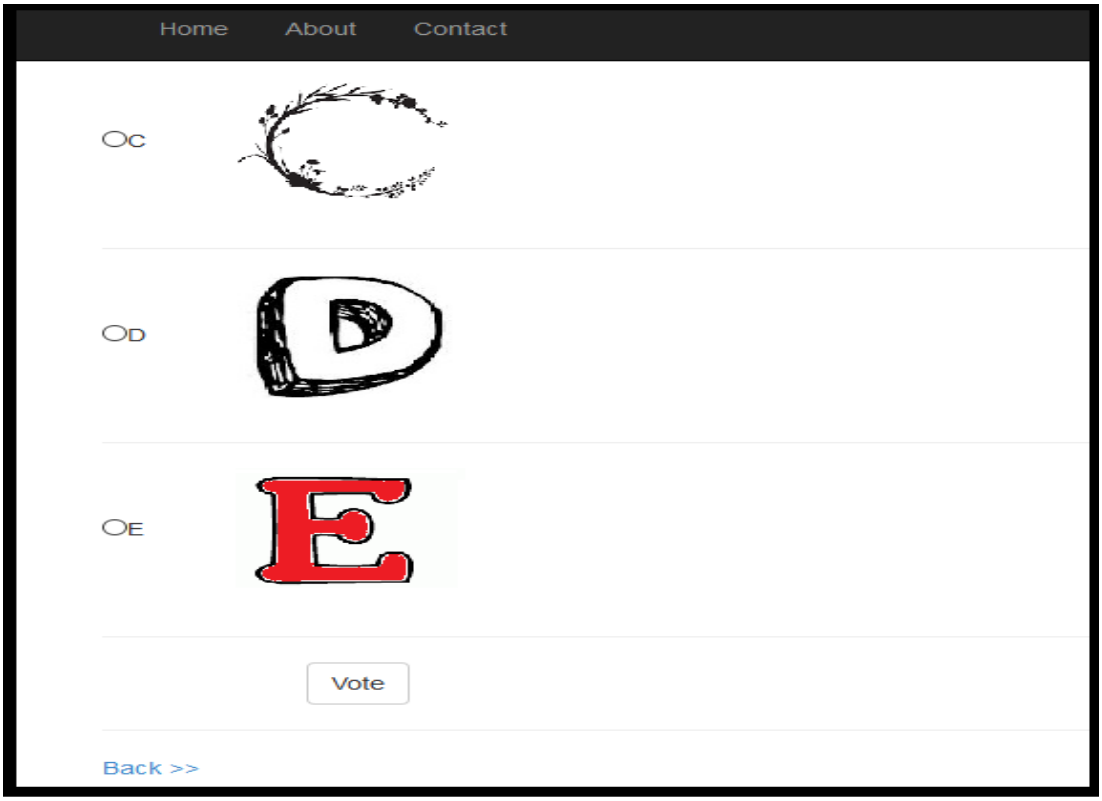
1-Voter Select his/her Candidate.

2-From voter token a symmetric key is generated.

3-Voter encrypt vote, and then blinded with blinding technique.

4-Then Encrypted blinding vote together with national number sending to the administrator server.

Figure 6.3: Voting Phase.



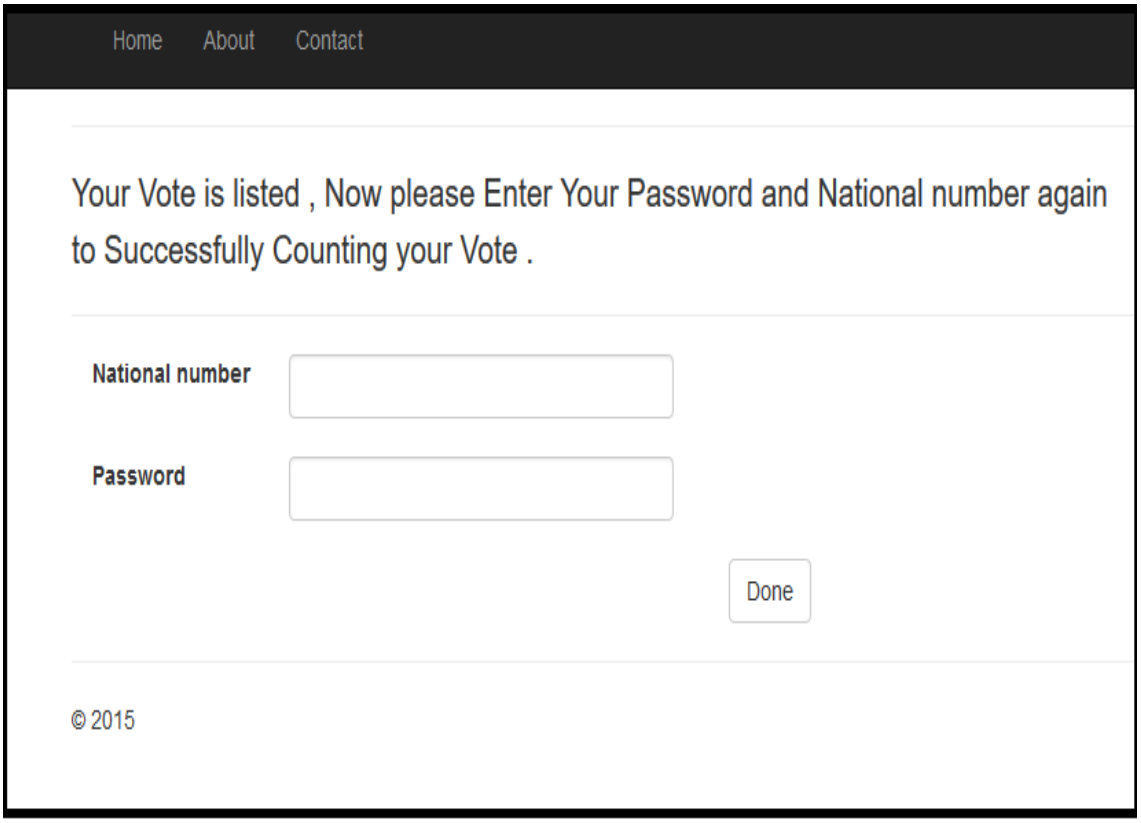
Administrator server generate signature and send it to the corresponding voter. Then the system in background release blinding and send encrypted vote together with signature to the collector server.

Collector server check signature and then insert encrypted vote with signature in the database.

Opening Phase

Voter provide his/her key to collector server to successfully decrypt vote and added to corresponding candidate.

Figure 6.4: Voter provide key.



Counting Phase

After opening phase completed, administrator server send to the collector server to count vote and publish result.

Figure 6.5: Election Result.

6.7 PROPOSAL SYSTEM AGAINST ESTONIA VOTING SYSTEM

There are many aspect that can be looked to E-Vote system and the most important is the security service that secure the system. Despite extensive work on the voting schemes, no complete solution has been found in either theoretical or practical domains. A number of practical voting schemes have been proposed, with widely differing security properties. This is of course not all proposed voting schemes just here is compare of proposal system by the schema that was used by Estonia and Washington D.C system.

6.7.1 Estonia

- From Security Perspective

1- Estonia was used well known schema "**mix-net**" and it has well known security service and security troubles.

2- Use National ID Cards to verify system from voters and it good idea to take advantage of existing infrastructure and it more secure.

3- Use android application to allows voters to confirm that their votes were correctly recorded, by using this application they increase the security level.

4- Receipt-Freeness not included in schema (mix-net) however they use re-voting to deny that.

- From Infrastructure Perspective

1- There are complicity and extensive transaction, administration work, and security service "encryption and description" between mix-servers to hide voter identity.

- From Voter Perspective

1- The system is too simple and there no complicity and there are higher transparency.

2- The voters must have National ID Cards reader.

6.7.2 Proposal System

- From Security Perspective

1- The system based on Blind Signatures and it suffer from all schema troubles and provide all schema properties "discussed in chapter 3".

2- The system use unique token "that provided to voters after registration phase" to verify system from voters.

3- Provide re-vote ability unless submitting your vote.

4- The voter can confirm his/her or her vote by using unblinding signature.

5- Provide no universal verifiability.

- From Voter Perspective:

1- Schemes using blind signatures are very popular in practice due to their efficiency and their support for any type of the voting price is paid for this efficiency: the voter has to act in more rounds (registration, voting, counting, verifying whether his/her vote has been counted, complaining...).

2- Voters must have token that provided in registration phase to be able to vote, and have browser software and Internet access.

3- Voter must perform registration process in registration center.

- From Infrastructure Perspective

1- The system too simple from infrastructure perspective and there are no complicity and little administration work compared to Estonia.

2- Database is distributed among administrator and collector server, which provide privacy for voter.

6.8 CHAPTER CONCLUSION

This chapter talk about Sudanese general election. Did an overview of the election processes. Then discuss the FOO scheme that used in proposal system and why is chosen rather than the other (Homomorphic Encryption, MIX-net), how its work with election processes, what security services property is achieved and discuss the limitations of the

FOO-scheme. Then went on to give a more detailed view of the Secure E-Voting (Proposal protocol) and the messages exchanged between the various entities. After which analyzed the scheme and showed how it satisfy the security properties of an E-Voting scheme. Finally given an overview of proposal system against Estonia voting system.

7.1 THE RESULT

After all implantation of the work that have been done and analyses, achieving that make voting processes more convenient for voters, save money in the long run and time, achieving Security requirements except universal varying and recipient freeness and mobility by allowing the voters to vote from anywhere.

7.2 FUTURE WORKS

Firstly, this thesis used high level cryptographic primitives like digital signatures, encryption algorithms, public key cryptography, blind signature schemes and threshold cryptography however in actual implementation the exact type of cryptographic primitive used goes a long way in determining the efficiency and security requirements of the scheme proposal scheme can satisfy. Hence in future works more details should be given about the exact primitives and how they enhance the overall security and practicability of the scheme.

In the secure electronic voting scheme proposed in this thesis present that the trust place on the various authorities especially the trust placed on the physical Registration centers which are not suitable way.

However, the further work has to be done is to make online registration center to utilized network features and much more convenient for voters.

Also need to investigate how long it would take each voter to complete the voting process and if it is an acceptable time in a real world election with large amount of voters.

Finally, further works need to be done in implementing universal verifiability and recipient freeness to achieve all security requirements.

7.3 CONCLUSION

This thesis did an overview of the existing literature on electronic voting. It's discuss the security requirements of electronic voting and highlighted the contradiction in some of these requirements. Then looked at the FOO scheme which is branch of blind signature. Also did an analysis of our scheme and their limitations.

Then went further to propose an electronic voting scheme based on the national number. shown how proposal scheme uses the National number Authentication and Password authentication of the registration centers system to authenticate a voter's identity and this authentication enhances voter's mobility since voter's can now vote anywhere provided there is an available terminal that is part of the that is part of the voting system.

Then analyzed proposal scheme and showed how it satisfied the security requirements of electronic voting.

BIBLIOGRAPHY

1- computerhope, 1998. *computerhope*. [Online]
Available at: http://www.computerhope.com
[Accessed 1 May 2015].

2- Augoye, V., 2013. *Electronic Voting: An Electronic Voting Scheme using the Secure Payment card System*. London: Royal Holloway, University of London Egham, Surrey TW20 0EX, [Accessed 20 May 2015].

3- AggelosKiayias, M. K. D. W., 2006. *An Internet Voting System*, United States: University of Connecticut [Accessed 2 June 2015].

4- REMOTE VOTING TECHNOLOGY by Chris Backer, E-Voting Conslutant [Accessed 20 July 2015].

5- IFES, E. f. P., 1998. *ElectionGuide*. [Online]
Available at: http://www.electionguide.org
[Accessed 5 June 2015].

6- pitt, W. R., 2003. *Electronic Voting: What You Need to Know*. [Online]
Available at: http://www.truth-out.org/
[Accessed 4 May 2015].

7- Orhan Cetinkaya, A. D., 2007. *A Practical Verifiable e-Voting Protocol for Large Scale Elections over a Network*, Ankara: Turky [Accessed 15 August 2015].

8- Jung-Ying Lai, C.-F. L. C.-H. Y., 2008. *Design and Implementation of* , Taiwan: National Kaohsiung [Accessed 4 August 2015].

9- Commite, T. N. E., 2005. *E-Voting system*. 1 ed. Tallin: The National Election Commite [Accessed 2 September 2015].

10- Emad ABU-SHANAB, M. K., 2010. *E-VOTING SYSTEMS: A TOOL FOR E-DEMOCRACY*. 2nd ed. Jordan: Yarmouk University [Accessed 27 August 2015].

11- Buchsbaum, T. M., 2004. *E-Voting: International Deve*. 1 ed. Vienna, AUSTRIA: Federal Ministry for Foreign Affairs [Accessed 1 August 2015].

12- Lekkas, D., 2011. *researchgate*. [Online]
Available at:
http://www.researchgate.net/publication/257244640_Lekkas_D._Securing_e-Government_and_e-Voting_with_an_open_cloud_computing_architecture._Gov._Inf._Quarterly_28_239-251
[Accessed 13 April 2015].

13- Tall, S., 2015. *independent*. [Online]
Available at: http://www.independent.co.uk/voices/general-election-2015-the-ins-and-outs-of-tactical-voting-nose-pegs-optional-10156287.html
[Accessed 5 April 2015].

14- Stephen D. Ansolabehere, 2006. *votingmachines.procon*. [Online]
Available at: http://votingmachines.procon.org/view.resource.php?resourceID=000274
[Accessed 19 June 2015].

15- verifiedvoting.org, 2012. *Election Systems and Software (ES&S) iVotronic*. [Online]
Available at: https://www.verifiedvoting.org/resources/voting-equipment/ess/ivotronic/
[Accessed 22 July 2015].

16-IFES, 2014. *Electronic Voting Machines*. 1 ed. Pakistan: IFES [Accessed 2 May 2015].

17- Diplomovapraca, 2002. *Electronic Voting Schemes*. 1 ed. Bratislava: Comenius University [Accessed 14 June 2015].

18- Sprojcar, J., n.d. *The Primitive beyond Voting Schemes*. 1 ed. Czech: Masaryk university [Accessed 15 August 2015].

19- Kyle MacNamara, I. I., 2012. *A Survey of Electronic Voting Schemes*. 1 ed. United States: University of California [Accessed 1 August 2015]..

20- Sampigethaya, K., 2006. *A Survey on Mix Networks and Their Secure Applications*. 1 ed. United States: University of Washington [Accessed 6 June 2015].

21- Schwartz, B., 2013. *Establishing a Legal Framework for E-voting in Canada*, Canda: Universty Of Manitoba [Accessed 6 June 2015].

22- Drew Springall, T. F. Z. D. e., 2014. *Security Analysis of the Estonian Internet Voting System*, United States: University of Michigan, Ann Arbor [Accessed 30 August 2015].

23- Scott Wolchok, E. W. D. I. a. J. A. H., 2010. *Attacking the Washington, D.C.*, United States.: University of Michigan [Accessed 19 September 2015].

24- Martin, K. M., 2012. *Everyday cryptography: Fundamental principles and applications*. 1 ed. London: Oxford University Press [Accessed 7 August 2015].

25- Microsoft, 2013. *ASP.NET MVC 2*. [Online]
Available at: https://msdn.microsoft.com/en-us/library/dd394709%28v=vs.100%29.aspx
[Accessed 16 September 2015].

26- Sudan, N. E. C. f., 2015. *National Election Commission for Sudan*. [Online]
Available at: http://nec.org.sd/en/voters/voter-registry/
[Accessed 27 August 2015].

27- Sheet, F., 2015. *National Election Commission for Sudan*. [Online]
Available at:
(http://nec.org.sd/en/wpcontent/uploads/sites/2/2013/09/nec_factsheet_05_national_election_act_en.pdf.).
[Accessed 27 August 2015].

28- D, C., 1982. *Blind signatures for untraceable payments*. 1 ed. New York: Plenum Press [Accessed 23 July 2015].

29- Knauss, T., 2013. *syracuse*. [Online]
Available at:

http://www.syracuse.com/news/index.ssf/2010/09/for_tuesdays_primary_onondaga.html [Accessed 4 May 2015].