Table of Content

Table of Contents

LIST OF FIGURE

Abstract

Electronic voting has a lack of transparency that makes its use controversial. In our opinion, the lack of transparency of electronic voting systems can be overcome to a great extent by using adequate security measures (technological, physical and procedural). Such security measures would provide clarity to the process and avoid the need to rely on complex and/or networked systems and/or proprietary closed systems. This research proposed a reliable cost effective secure electronic voting system that can be used in cost effectively way in many development countries. The important obstacle in any e-voting system across the world is the security issue. Election's results may be modified when delivered to the Higher Elections Committee, unauthorized voter may vote instead of the eligible voter, a vote may not be calculated; also the voter has to ensure that nobody has the possibility to know his ballot data. The proposed Voting Model System overcomes these obstacles. Security evaluation experiments are performed successfully to the proposed system proving that it satisfies privacy, accuracy, reusability, eligibility and integrity. This research proposes a secure electronic voting system that provides enhanced security by implementing cryptography and steganography in JAVA. As a preliminary investigation.

المستخلص

من اكثر مشاكل التصويت الإلكتروني انعدام الشفافية التي تجعل استخدامه مثيرا للجدل. وفي رأينا، يمكن التغلب على انعدام الشفافية في نظم التصويت الإلكتروني إلى حد كبير باستخدام تدابير أمنية كافية (تكنولوجية ومادية وإجرائية). ومن شأن هذه التدابير الأمنية أن توفر الوضوح للعملية وتتجنب الحاجة إلى الاعتماد على النظم المعقدة و / أو الشبكات و / أو النظم المغلقة الملكية. واقترح هذا البحث نظاما موثوقا من حيث التكلفة والسرية وموثوقا بالنسبة للتصويت الإلكتروني يمكن استخدامه بطريقة فعالة في العديد من بلدان التنمية. وإن العقبة الهامة في أي نظام للتصويت الإلكتروني في جميع أنحاء العالم هي الأمن والنزاهة. فيمكن تعديل نتائج الانتخابات عند تسليمها إلى لجنة الانتخابات العليا، يجوز للناخبين غير المصرح لهم التصويت بدلا من الناخب المؤهل، في هذه الحالة لا يجوز حساب التصويت؛ كما يجب على الناخب التأكد من أن لا أحد لديه القدرة على معرفة بيانات اقتراعه. يتغلب نموذج نظام التصويت المقترح على هذه العقبات. حيث تمت إجراء تجارب تقييم الأمن بنجاح للنظام المقترح تثبت أنه يرضي الخصوصية والدقة وإعادة الاستخدام والأهلية والنزاهة. يقترح هذا البحث نظام التصويت الإلكتروني الآمن الذي يوفر تعزيز الأمن من خلال تنفيذ التشفير وإخفاء المعلومات في JAVA.

Chapter 1

Introduction

1.1 Introduction:

Electronic voting is now a reality—and so are the many errors and vulnerabilities in commercial Electronic voting systems. Voting systems are hard to make trustworthy because they have strong, conflicting security requirements:

- Integrity of election results must be assured so that all voters are convinced that votes are counted correctly. Any attempt to corrupt the integrity of an election must be detected and correctly attributed.
- Confidentiality of votes must be assured to protect voters' privacy, to prevent selling of votes, And to defend voters from coercion.

1.2 Voting:

Voting is a method for a group, such as, a meeting or an electorate to make a decision or express an opinion, usually following discussions, debates or election campaigns. Democracies elect holders of high office by voting. Residents of a place represented by an elected official are called "constituents", and those constituents who cast a ballot for their chosen candidate are called "voters". There are different systems for collecting votes.

In a democracy, a government is chosen by voting in an election: a way for an electorate to elect, i.e. choose, among several candidates for rule. In a representative democracy voting is the method by which the electorate appoints its representatives in its government. In a direct democracy, voting is the method by which the electorate directly make decisions, turn bills into laws, etc.

A vote is a formal expression of an individual's choice for or against some motion (for example, a proposed resolution); for or against some ballot question; or for a certain candidate, selection of candidates, or political party. Many countries use a secret ballot, a practice to prevent voters from being intimidated and to protect their political privacy.

1.3 E-voting Problem:

First, let’s consider the international standards an election has to meet to be considered free and fair:

- Individuals have to be accurately identified as eligible voters who have not already voted.
- Voters are only allowed one anonymous ballot each, which they can mark in privacy.
- The ballot box is secure, observed and, during the election, only able to have votes added to it by voters. Votes cannot be removed.
- When the election ends the ballot box is opened and counted in the presence of observers from all competing parties. The counting process cannot reveal how individual voters cast their ballots.
- If results are in doubt the ballots can be checked and counted again by different people.

1.4 Problem Statement:

- Possibility of stolen voter packages or identification cards (Confidentiality).
- Misuse of elector's ID card and personal information voting by others without the knowledge of the elector (privacy).
- Possible pressure on electors to vote a certain way if in the presence of others (Confidentiality).
- Hacks or viruses attacking the system and altering election results.
- Inaccuracies on the voters' list, resulting in one elector receiving a card intended for another elector (Integrity).

1.5 Research Objectives:

- Prevent possibility of stolen voter packages or identification cards
- Prevent voting by others without the knowledge of the elector
- No possibility to pressure on electors to vote a certain way if in the presence of others
- Minimize the possibility of hacks or viruses attacking.
- Flagging of ballot errors.
- Elimination of long line-ups.

1.6 Research Methodology:

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.

1.7 Research Layout:

In this research in first chapter we will start talk about, Introductions in voting (voting general), and then will preview problem of an e-voting and the objective we are try to get it, research Methodology. In second chapter we will talk about e-government, electronic voting, voting system requirements, e-voting security requirements, E-voting challenges, and overview of foo-scheme, related work, and then finally proposal system compare with Estonia. In chapter three will analyses the proposed system. Then we will go to chapter four and we will talk about this topic pre- electoral period, post-electoral period, overview of the secure electronic voting using foo-scheme, tool and technologies used in the study, cryptographic primitives, and result and discussions. And in last chapter we will talk about conclusion, future works.

Chapter 2

Literature review & related work

2.1 Introduction:

In this chapter reviewed and analyzed several remote electronic voting models with respect to security. Strengths and weaknesses of each model were identified. Based on this review and analysis the most secure models (Swiss and Estonian) were customized and enhanced to produce a secure model that suite the requirements. This section gives a detailed review and analysis of the selected models with respect to security

2.2 E-Government:

As governments in developing countries make choices to pursue public administration reforms, many are using ICTs to offer e-Government services. E-Government is the centerpiece of information systems-supported reforms to digitize the delivery of services and the process of governance occurring across all levels of government. E-Government utilizes the Internet and the World Wide Web for both service delivery and information dissemination. For this report, e-Government is defined as: the use of information and communication technologies in government to provide public services to improve managerial effectiveness and to promote democratic values and mechanisms; as well as a regulatory framework that facilitates information intensive initiatives and fosters the knowledge society (Gil-Garcia and Luna-Reyes 2003). E-Government is broadly defined because governments themselves serve multiple roles. By using ICTs in this way, governments expect to improve the quality of services and reduce the costs of delivering services. Other e-Government goals are to improve the utilization of scarce resources, enhance accountability And transparency, expand the role of markets, and restore citizen trust and faith in government.

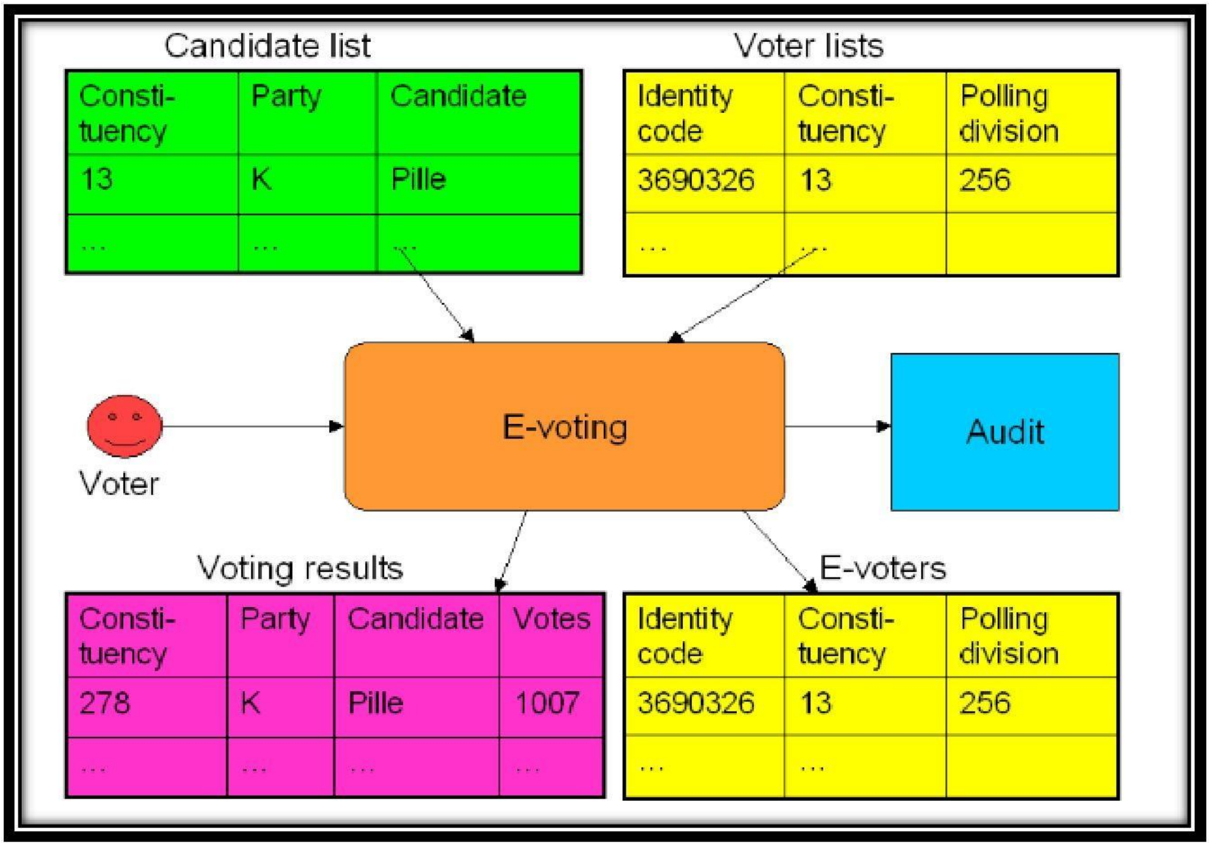
Government-to-Citizen e-Government focuses on making information accessible to citizens online. This is referred to as a citizen-centric e-Government when governments take further steps to provide online services organized around citizen needs. Many early designs of e-Government web sites organized the content, particularly the hyperlinks to government services, around the pre-existing structure of the ministry and its bureaucratic procedures. This proved to confuse citizens. Citizens would spend time searching to find information through a labyrinth of web pages that mirrored the organization and structure of the ministry.

Since most citizens do not understand how the internal operations of a government ministry functions, the bureau-centric organization of a government web Electronic Government for Developing Countries 17/59site caused greater levels of dissatisfaction with early-Government sites. Web visitors would use trial and error methods to navigate from page to page on the web site and not know for certain if the next click would lead them to the information they needed or to a dead end. Learning lessons from e-commerce sites, developers of e-Government services adopted customer-centric approaches to help citizens become more satisfied with their online experience at government web sites. Typical practices of citizen-centric approach to e-Government include: organizing content around citizen needs; aligning the structure of the pages in the web site to reduce the number of clicks it takes to find information, access a service, or to complete a transaction; improving the affective qualities of the site; adding functions to facilitate the communication between citizens and the government; and, enabling the user to customize the site contents. A related Government-to-Citizen relationship is when the citizen is also interacting with government as a political actor and participant in democratic processes. E-voting and E-democracy systems support this type of relationship. [1]

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 [2]

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.



Candidate list

Constituency	Party	Candidate
13	K	Pille
...	...	...

Voter lists

Identity code	Constituency	Polling division
3690326	13	256
...	...	

Voting results

Constituency	Party	Candidate	Votes
278	K	Pille	1007
...	...	...	...

E-voters

Identity code	Constituency	Polling division
3690326	13	256
...	...	

Figure 2-1: The scope of e-voting: input and output [3]

As illustrated in (Figure 1), 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: [4] [5]

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 Voting System Requirements:

A voting system, whether using paper, electronic recording or networks such as the Internet, needs thus to satisfy various requirements, which are summarized in 16 main points. [6]

1. Fail-safe voter privacy. Definition: “Voter privacy is the inability to link a voter to a vote.” Voter privacy must be fail-safe – i.e., it must be assured even if everything fails, everyone colludes and there is a court order to reveal all election data. Voter privacy must be preserved even after the election ends, for a time long enough to preserve backward and forward election integrity (e.g., to prevent future coercion due to a past vote, which possibility might be used to influence a vote before it is cast).
2. Collusion-free vote secrecy. Definition: “Vote secrecy is the inability to know what the vote is.” Vote secrecy must be assured even if all ballots and decryption keys are made known by collusion, attacks or faults (i.e., vote secrecy must not depend only on communication protocol and cryptographic assumptions, or on a threshold of collusion for the key holders).
3. Verifiable election integrity. Definition: “Election integrity is the inability of any number of parties to influence the outcome of an election except by properly voting.” The system must provide for verifiability of election integrity for all votes cast. For any voter the system must also provide for direct verifiability that there is one and only one valid ballot cast by the voter at the ballot box.
4. Fail-safe privacy in verification. If all encrypted ballots are verified, even with court order and/or with very large computational resources, the voter’s name for each ballot must NOT be revealed.
5. Physical recounting and auditing. Must provide for reliability in auditing and vote recounting, with an error rate as low as desired or, less strictly, with an error rate comparable or better than conventional voting systems. The auditing and vote proofs must be capable of being physically stored, recalled and compared off-line and in real-time during the election, without compromising election integrity or voter privacy, and allowing effective human verification as defined by election rules.

6. 100% accuracy. Every vote or absence of vote (blank vote) must be correctly counted, with zero error
7. Represent blank votes. must allow voters to change choices from ‘vote’ to ‘blank vote’ and vice-versa, at will, for any race and number of times, before casting the ballot
8. Prevent over votes. As defined by election rules. Must provide automatic “radio button” action for single-vote races. If over voting is detected in multiple-vote races, must warn the voter that a vote has to be cleared if changing choices is desired. This warning must be made known only to the voter, without public disclosure.
9. Provide for null ballots. As defined by election rules, may allow voters to null races or even the entire ballot as an option (e.g., to counter coercion; to protest against lack of voting options). Over voting, otherwise prevented by Requirement #8, may be used as a mechanism to provide for null ballots.
10. Allow under votes. As defined by election rules, the voter may receive a warning of under voting. However, such a warning must not be public and MUST NOT prevent under voting.
11. Authenticated ballot styles. The ballot style and ballot rotation to be used by each voter must be authenticated and must be provided without any other control structure but that given by the voter authentication process itself.
12. Manifold of links. Must use a manifold **Invalid source specified.** Of redundant links and keys to securely define, authenticate and control ballots. Must avoid single points of failure –even if improbable. If networks are used, must forestall Denial-of-Service (DoS) and other attacks with an error rate comparable or better than conventional voting systems [7].
13. Off-line secure control structure. Must provide for an off-line secure end-to-end control structure for ballots. May use digital certificates under a single authority. Ballot control MUST be data-independent, representation- independent and language-independent.
14. Technology independent. must allow ballots and their control to be used off-line and/or in dial-up and/or in networks such as the Internet, with standard PCs or hand-held devices used to implement their components in hardware or in software, alone or in combination for each part.
15. Authenticated user-defined presentation. must enable the ballots to dynamically support multiple languages, font sizes and layouts, so that voters could choose the language

and display format they would be most comfortable with when voting as allowed by law and required by voters with disabilities, without any compromise or change to the overall system, from an authenticated list of choices defined by election rules.

16. Open review, open code. Allow all source code to be publicly known and verified (open source code, open peer review). The availability and security of the system must not rely on keeping its code or rules secret (which cannot be guaranteed), or in limiting access to only a few people (who may collude or commit a confidence breach voluntarily or involuntarily), or in preventing an attacker from observing any number of ballots and protocol messages (which cannot be guaranteed). The system should have zero- knowledge properties (i.e., observation of system messages do not reveal any information about the system). Only keys MUST be considered secret.

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: [8]

(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.

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

(4) 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.

2.7 E-Voting challenges:

From a technological perspective e-voting in uncontrolled environments faces two substantive challenges: one is to know who the voter is (identification and authentication), the other involves the registration, transmission and counting of the voters' electronic ballots with a hundred per cent accuracy. Voter identification and authentication can be obtained with the help of something the voter owns (e.g. a smart card), knows (a PIN-code, for example) or is (a physical property which may be read off, such as for example the voter's finger print or retinal pattern). The working committee is of the opinion that e-voting specific identification procedures should be avoided. At present PKI solutions have been chosen at security level "Person High" for electronic communication with the public sector.

The working committee is of the opinion that the technology currently used in uncontrolled environments does not provide a sufficient level of security with respect to registration and the transmission of cast votes. However, there is good reason to believe that better solutions will be available on the market in due course.

The working committee suggests that a voter should have the right to withdraw a ballot that has been cast electronically in an uncontrolled environment. A cast ballot may be cancelled either by the submission of a new electronic ballot, or by the submission of a vote by traditional procedure in a polling station on Election Day. In order to make this feasible, each electronic ballot must be linked to the voter's identity and the link must be maintained until the vote can no longer be cancelled, but the content of the vote must be sealed (this may be achieved using encryption). This places special security requirements on the routines related to the handling of e-votes, to be elaborated

2.7.1 Technical challenges and possible solutions:

In the present section we take up the following tasks defined in the mandate:

- Give an overview of different systems by which a vote may be cast electronically through different channels (Internet, touch screens, SMS, digital TV, etc.) [9].
- Point out advantages and disadvantages of the different systems/channels [10].
- Assess the different systems/channels with respect to user friendliness and security of the votes [11].

- Discuss and assess the recommendation of e-voting by means of Internet technology in as well as outside the polling stations.
- Consider solutions for proper identification and authentication of a voter ready to submit an electronic ballot (smart card, ID card, etc.).
- Consider the introduction of verification solutions in the systems, and recommend possible procedures for such solutions.
- Consider the problems related to open source codes.
- Consider the use of an electronic Population Registry, and its implications for an e-voting system.

2.7.2 Conditions for technical solutions

In this section we sum up the conditions that must be met in a technical solution for e-voting:

2.7.3 Two phase election:

Elections in Norway will still be run in two phases (known as an advance voting period and a voting period on Election Day). The first phase runs over several days, or weeks or months, while the second phase is a one-day election (possibly two days). Between the two voting periods there is a break, the duration of which may be determined later.

Electronic voting in phase one only

The working committee’s studies show that introducing e-voting in controlled environments is very expensive and the gains are rather limited. The election results will be arrived at faster with less human resources, but the cost of equipment and arrangement will be higher than if our current system is used. Only if the solution is based on technical equipment owned and administered by the voters themselves, will there be a potential for considerable reductions in election costs. Moreover, a well-tested traditional voting system in the second phase should be maintained, not least as a safety measure in case problems arise with the electronic solutions in the first phase.

No changes in the voting procedures in phase 2 (on Election Day) Voters who prefer to cast their votes in the polling stations on Election Day will still be able to do so in the future, in accordance with traditional procedures. Electronic solutions, therefore, must be designed in a way that does not affect the procedures of a traditional paper ballot system.

2.7.4 Different voting channels:

The technical solutions should make it possible to introduce several voting channels in phase 1 of the elections. Possible channels are the Internet, a mobile phone (SMS) or other future channels.

2.7.5 The principle of repeated ballot-casting

A voter should be able to cast a ballot several time, but only the last ballot registered from this person is counted. In the second phase a voter may cast his or her ballot only once. A ballot cast by a voter in a controlled environment in phase 2 overrides all other ballots cast that voter in the first phase. An electronic ballot from a voter is not a valid vote inserted in the electronic ballot box until it is made clear that this voter has not cast his or her ballot in the polling station on Election Day. A voter casting a paper ballot, whether in phase 1 or in phas2, does not have the opportunity to cast a (new) ballot again, whether in the first or the second phase of the election.

2.7.6 Compromises will affect the e-voter, not the traditional voter:

If compromises with respect to the voter's privileges cannot be avoided in an electronic voting solution, they should only affect the e-voter, not the voter casting a paper ballot.

E -voting requires that the voter pass personal information to the voting system (server). In the worst case this information may be used to disclose the voter's identity. Thus the voter must trust that the system processes this information correctly, and that there are adequate is provisions for keeping the voter and the content of his or her vote apart. The situation analogous to the manual system of advance voting or distant voting in which the ballot as to (placed in an envelope) is inserted in a cover envelope identifying the voter. The voter hast to trust that his or her ballot is separated from the cover envelope in a way that secures the anonymity of the ballot.

However, the working committee is of the opinion that a somewhat higher risk that the voter identity is linked to the content of the ballot may be acceptable if this acceptance simultaneously guarantees that the voter's ballot is registered correctly.

2.7.7 The user interface design:

The EC Recommendation on e-voting emphasizes that the user interface should be of a very high quality, cf. Standards no 47 -50 of the Recommendation. This implies that in designing the user interface it is of utmost importance that the presentation is neutral with respect to the voting options. Furthermore, voting in political elections is not an everyday task, which means that the user interface must be user friendly. The WAI- guidelines [12], intended to accommodate people with disabilities, should form the basis for the design.

The technical solutions should satisfy the standards of the EC Recommendation on e-voting a number of technical requirements have been listed in Appendix III of the Recommendation this working committee assumes that future solutions developed must satisfy these standards. In the present chapter we consider only the most relevant requirements listed in the Recommendation, and relate them to the overall conditions for technical solutions.

In Norway the voters have great confidence in the legitimacy of the elections. Traditional methods based on paper ballots are in principle so simple that the citizens can understand them and observe them in a way that makes them transparent to the layman. Once the ballots cast by the voters are read and processed by a computer, all layman observation and control must be replaced by trust in the experts who have designed, programmed, tested, controlled and certified the system. A lack of transparency and no real layman control raise questions with respect to the integrity of the system and a possible undermining of people's confidence.

Introducing new technology in the voting system also introduces new threats. Although current manual systems are not completely flawless, the threats related to them are of a kind that requires a number of independent errors or infidels to have any real consequences for the election results. An electronic solution enables a person with sufficient access to the system to make small changes in the system solutions, which may affect a great number of ballots. Computerized ballot storage also avails itself to threatening manipulation (extensive manipulation threats)

2.7.8 The main elements of an e-voting system are the following:

- The voter client – The computer used by the voter in casting a ballot.
- The ballot receiving server – one or more computers receiving and transmitting the ballots cast by the voters.
- A data line or a data network between the voter client and the ballot receiving server.
- A core system of one or more computers, uploading the ballots from the ballot receiving server and doing further processing.

It is generally impossible to guarantee that an electronic system is absolutely flawless. The question is what failure rates may be tolerated in the different applications, and what initiatives may be taken to counter possible faults. Problems related to the security of the Internet are well known and have been widely discussed in the literature. A number of assessment reports and security analyses have been published on Internet-based solutions55 and specially designed voting machines used in elections56. Generally, the introduction of computer systems implies a certain risk of programming errors and technical breakdowns of central components. The use of new technology also avails itself to errors resulting from user incompetence or user inadvertency.

In Appendix B we sum up the most important security challenges related to e-voting in uncontrolled environments. Other e-voting solutions are considerably less vulnerable to fraud or error.

The greatest technical challenges associated with introducing electronic voting are:

1- Fraudulent computer software in the voting client.

2- General vulnerability of the computer networks, the Internet in particular.

3- Difficulties in obtaining redundant data for trustworthy verification of counted results.

4- Inside attacks intended for sabotage or the manipulation of voting results, in particular attacks on the ballot receiving server and the core system.

2.7.9 Identifying the challenges:

Electronic voting solutions have obvious advantages, such as wide availability, procedural simplicity and counting efficiency. At the same time they create a number of challenging problems. Based on the fundamental democratic principles, the following challenges are defined:

- Ensure that the voter is able to cast a ballot.
- Ensure that only one ballot cast by a voter is counted.
- Ensure the secrecy of the vote.
- Ensure that the vote is not changed or falsified.
- Ensure that a cast ballot is not lost.
- Ensure that no fake ballots (votes that have not been cast by an eligible voter) are inserted into the voting system.

2.8 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.

2.8.1 Why Foo Scheme

In Chapter 1 the introduction has mentioned that E-Voting schemes based on Anonymous Channel:

1- Holomorphic Encryption.
2- MIX-net.
3- 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 holomorphic 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.

2.8.2 Schemes Based On Blind Signatures

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 [13] 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.

2.8.3 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 [14] 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:

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.

2.8.4 Achieved Properties

IDi: Identification of the voter VI. 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 collect or 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.

2.8.5 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.

2.9 Related Work:

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.

2.9.1 Estonia [15]

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. 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 [16]

2.9.1.1 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.

2.9.1.2 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.

2.9.1.3 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).

2.9.1.4 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.

2.9.2 Washington D.C. Internet Voting System [17]

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.

2.9.2.1 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).

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.

2.9.2.2 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.

2.9.2.3 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

2.10 PROPOSAL SYSTEM COMPARE WITH ESTONIA

2.10.1 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.

2.10.2 Estonia

2.10.2.1 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.

2.10.2.2 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.

2.10.2.3 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.

2.10.3 Proposal System

2.10.3.1 from Security Perspective

1- The system based on Blind Signatures and it suffer from all schema troubles and provide all schema properties.

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 un blinding signature. 5- Provide no universal verifiability.

2.10.3.2 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.

2.10.3.3 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.

Chapter 3

System analysis

3.1 INTRODUCTION

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

3.2 ANALYSES

Figure 3.1: 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.

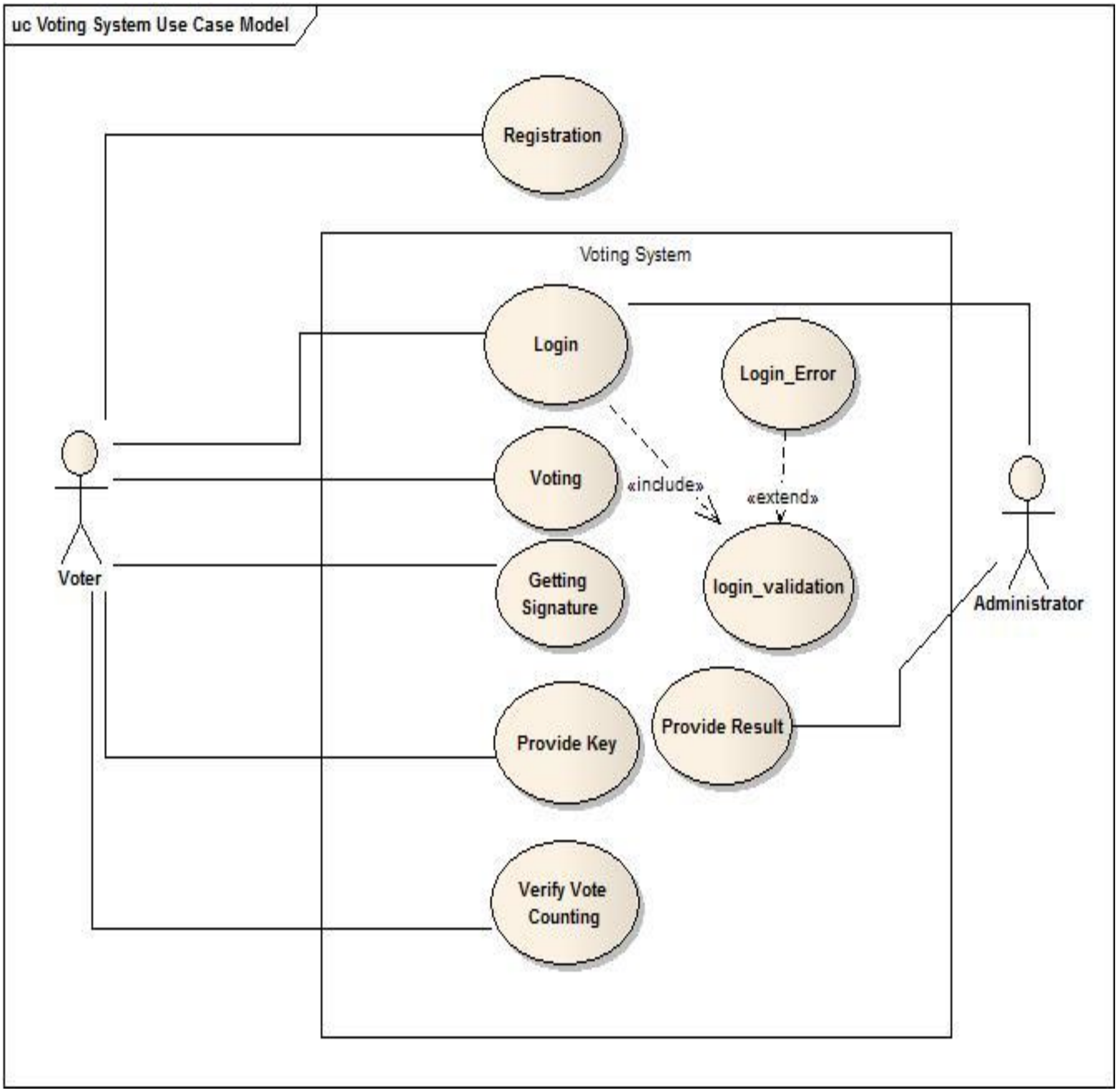


Figure 3-2: Describe the operations that can be performed by System user.

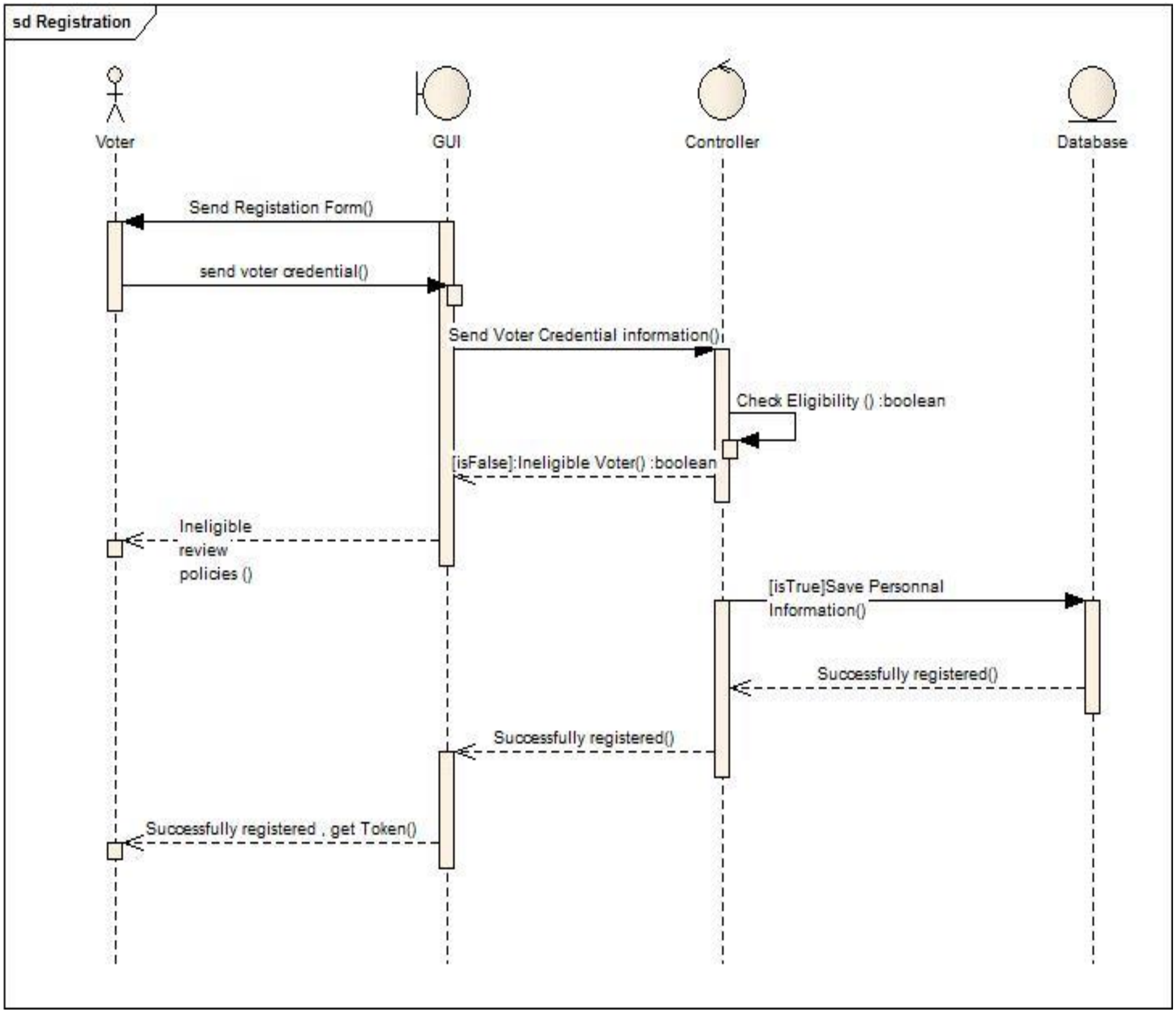

sd Registration
Voter
GUI
Controller
Database
Send Registation Form()
send voter credential()
Send Voter Credential information()
Check Eligibility () :boolean
[isFalse]:Ineligible Voter() :boolean
Ineligible review policies ()
[isTrue]Save Personnal Information()
Successfully registered()
Successfully registered()
Successfully registered , get Token()

Figure 3-3: Describe 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.

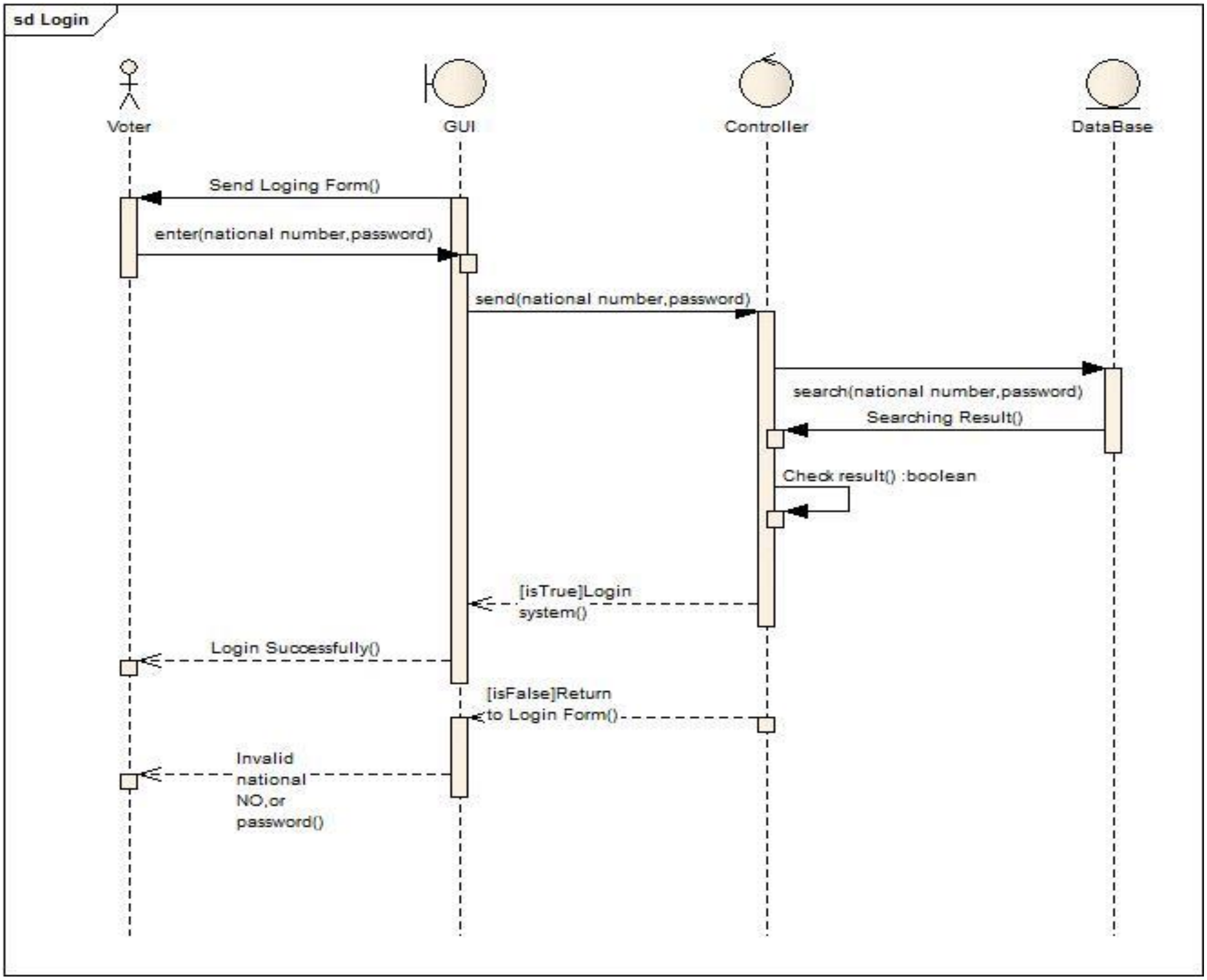

sd Login
Voter
GUI
Controller
DataBase
Send Loging Form()
enter(national number,password)
send(national number,password)
search(national number,password)
Searching Result()
Check result() :boolean
[isTrue]Login system()
Login Successfully()
[isFalse]Return to Login Form()
Invalid national NO,or password()

Figure 3-4: Describe 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.

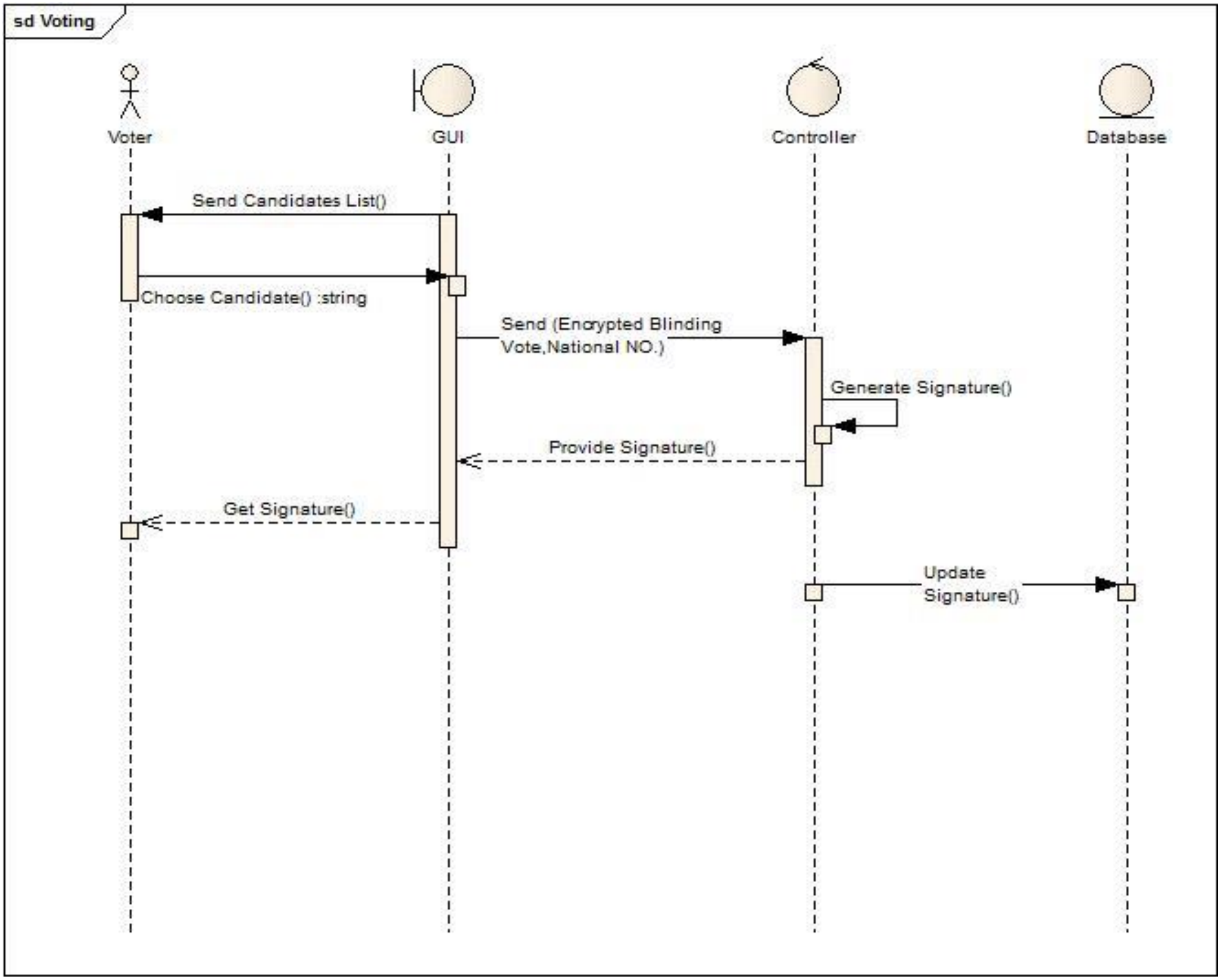


Figure 3-5: Describe the sequence voting process.

- 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.

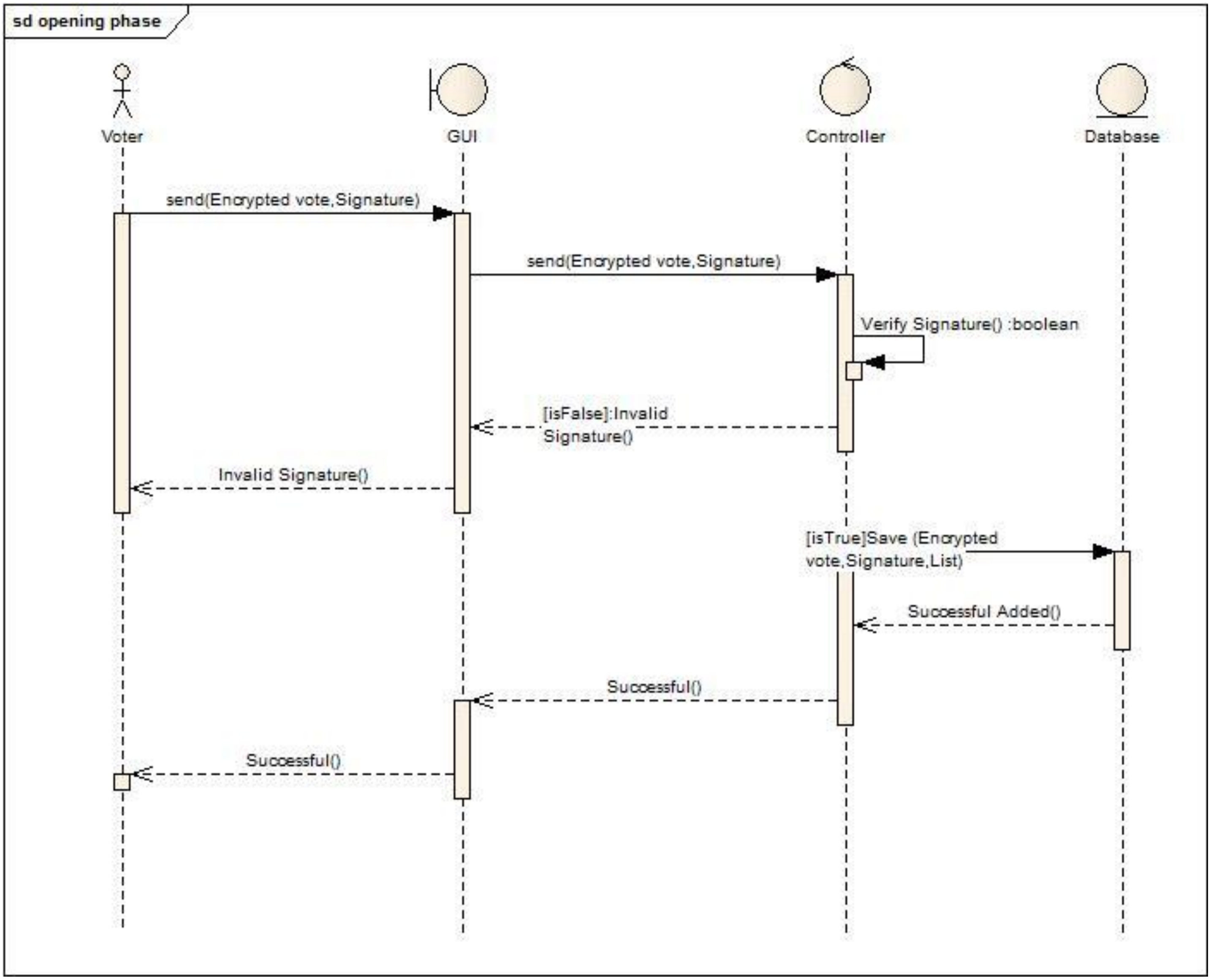

sd opening phase
Voter
GUI
Controller
Database
send(Encrypted vote,Signature)
send(Encrypted vote,Signature)
Verify Signature() :boolean
[isFalse]:Invalid Signature()
Invalid Signature()
[isTrue]Save (Encrypted vote,Signature,List)
Successful Added()
Successful()
Successful()

Figure 3-6: Describe 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.

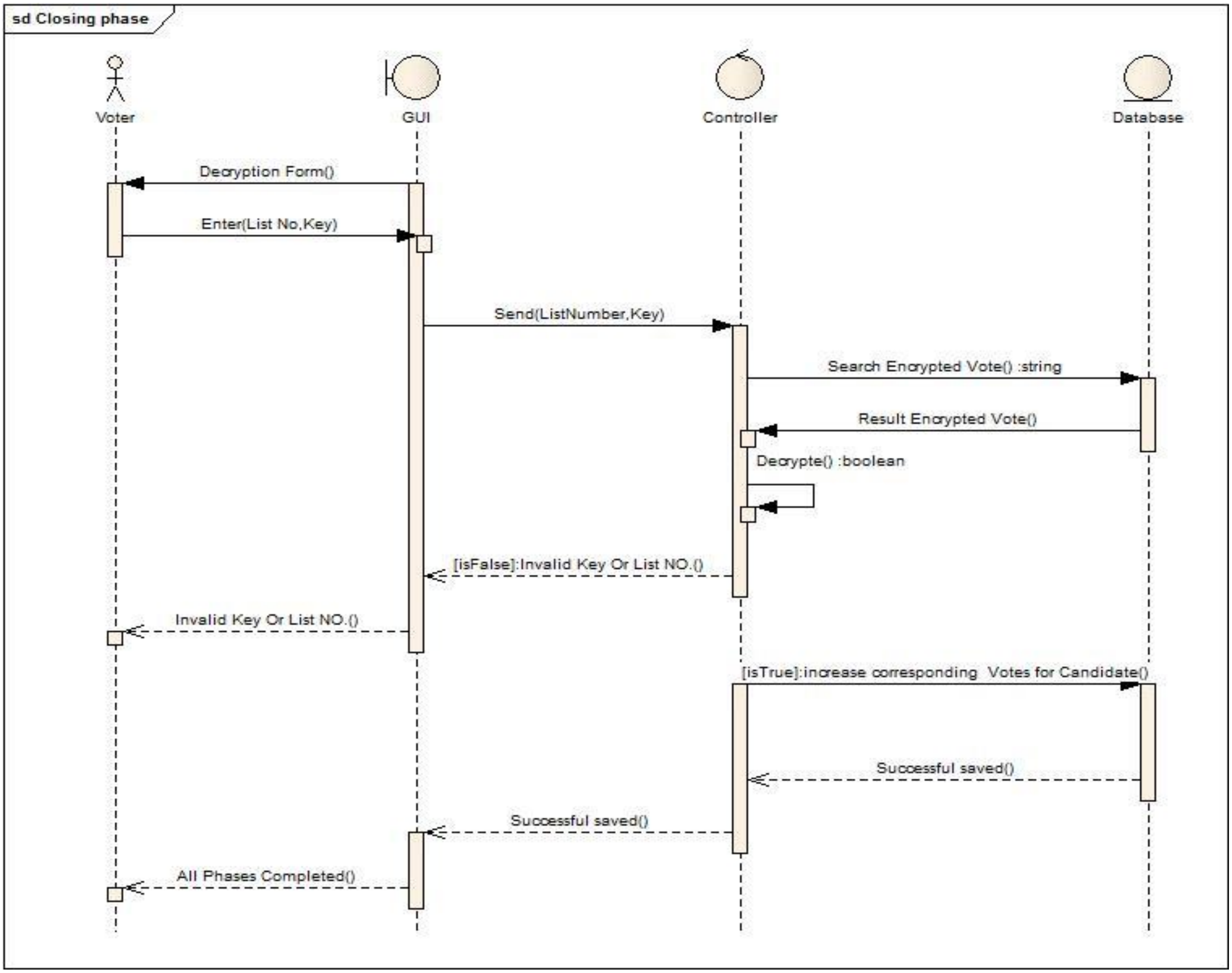


Figure 3-7: Describe the sequence of decryption process (counting stage).

- 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.

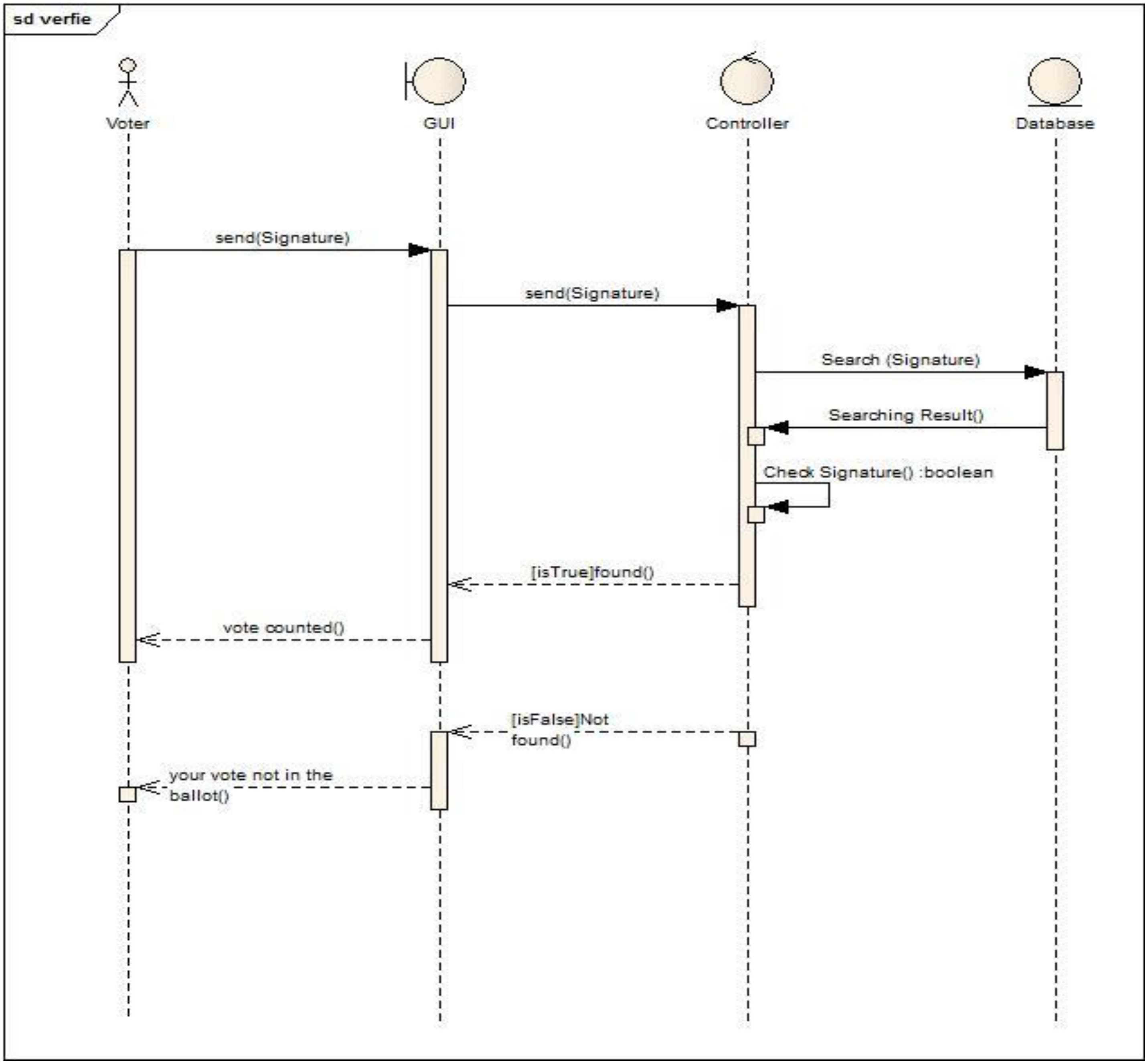


Figure 3-8: Describe the sequence of verifying process.

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

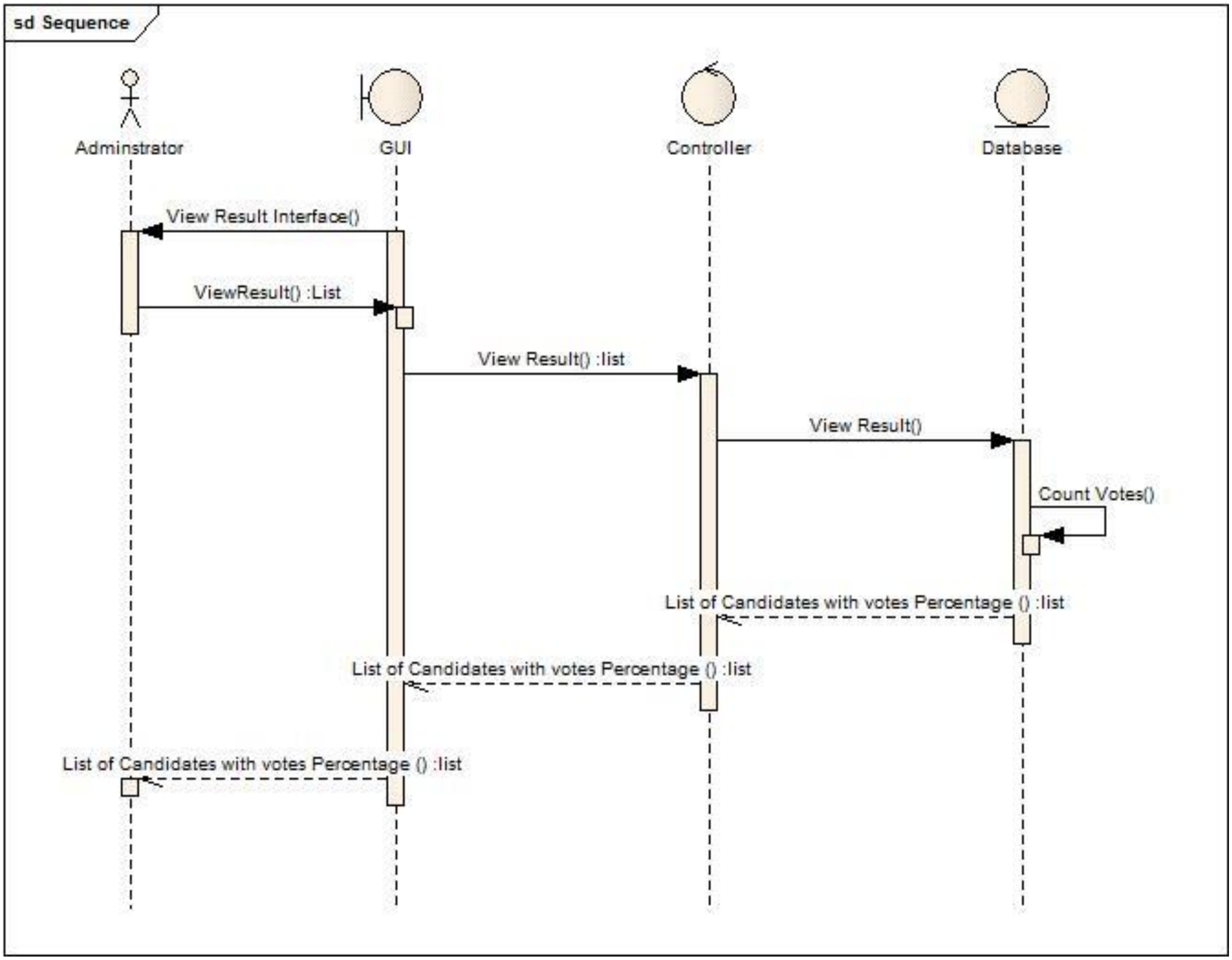

sd Sequence
Adminstrator
GUI
Controller
Database
View Result Interface()
ViewResult() :List
View Result() :list
View Result()
Count Votes()
List of Candidates with votes Percentage () :list
List of Candidates with votes Percentage () :list
List of Candidates with votes Percentage () :list

Figure 3-9: Describe 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.

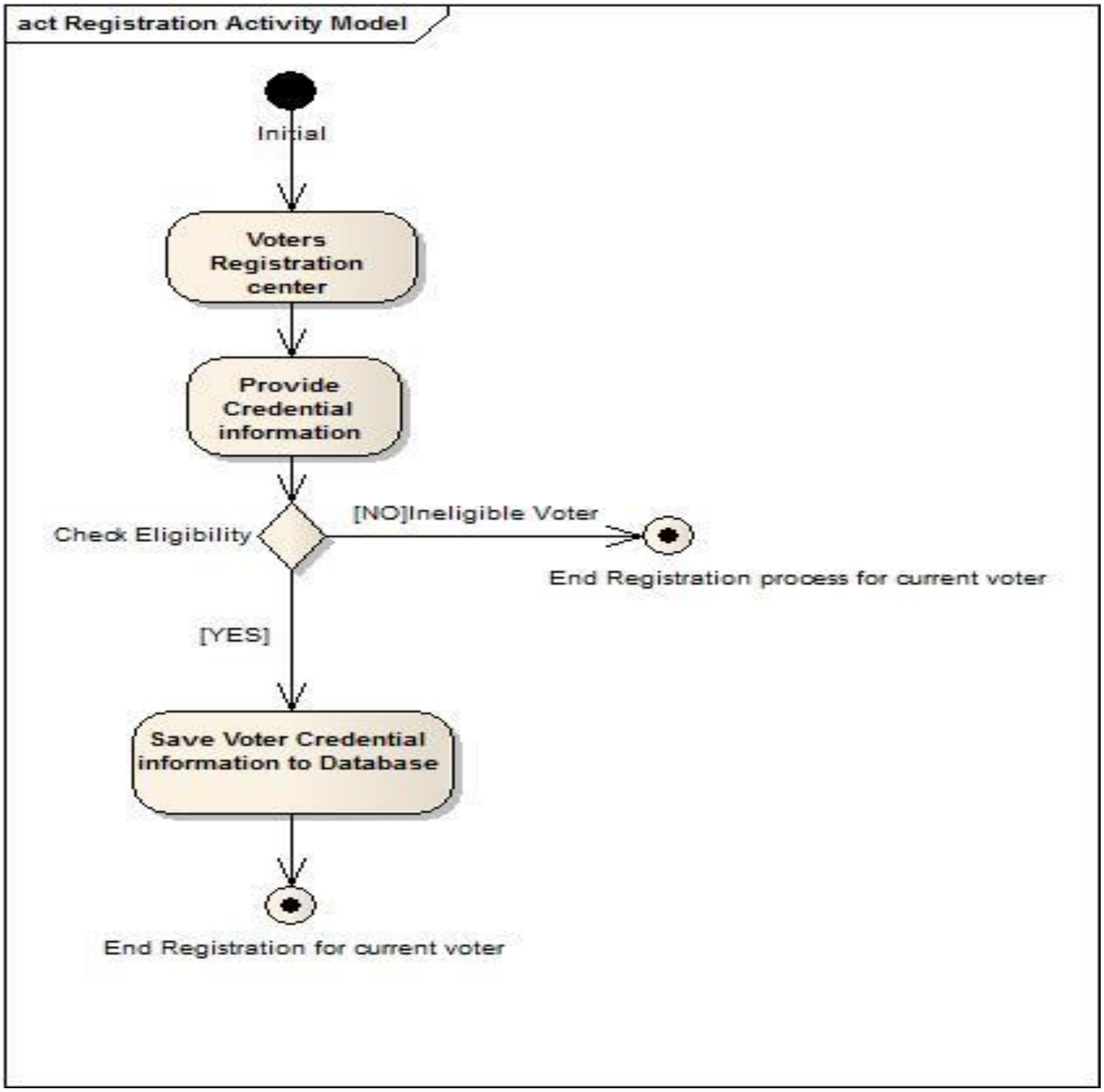

act Registration Activity Model
Initial
Voters Registration center
Provide Credential information
Check Eligibility
[NO]Ineligible Voter
End Registration process for current voter
[YES]
Save Voter Credential information to Database
End Registration for current voter

Figure 3-10: Describe group of Activity that users of system use it in registration process.

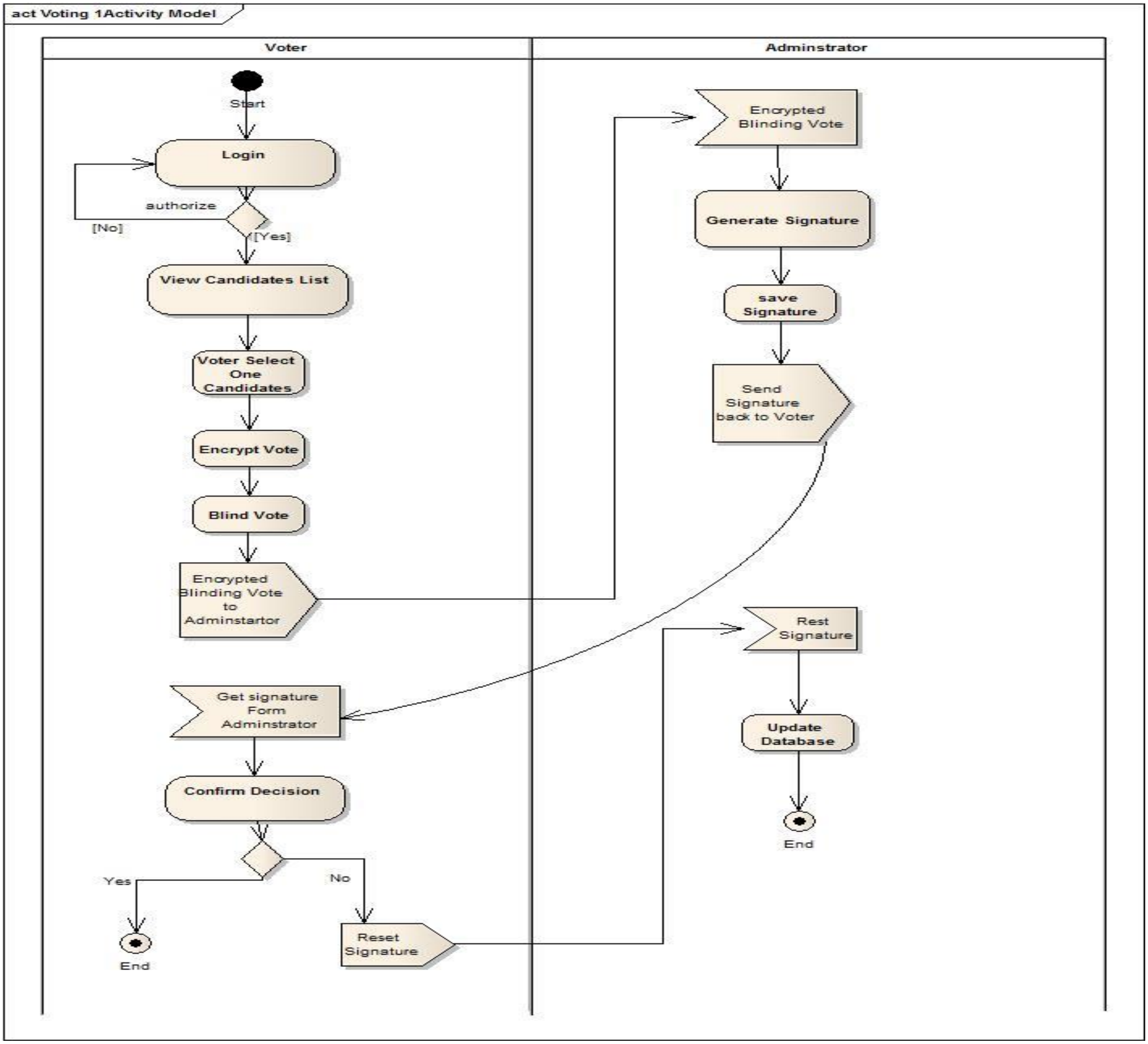


Figure 3-11: Getting signature

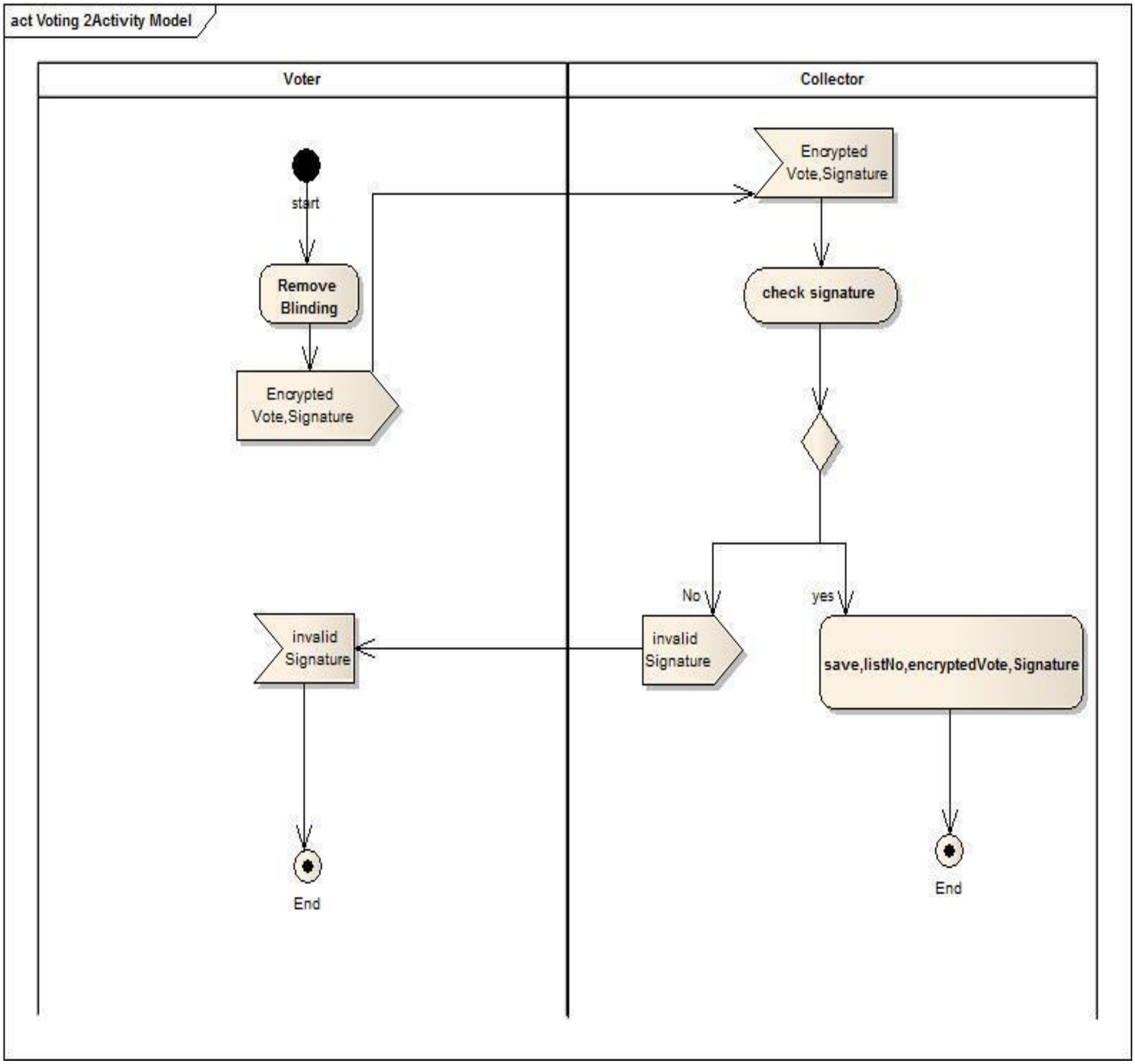


Figure 3-12: Opening phase.

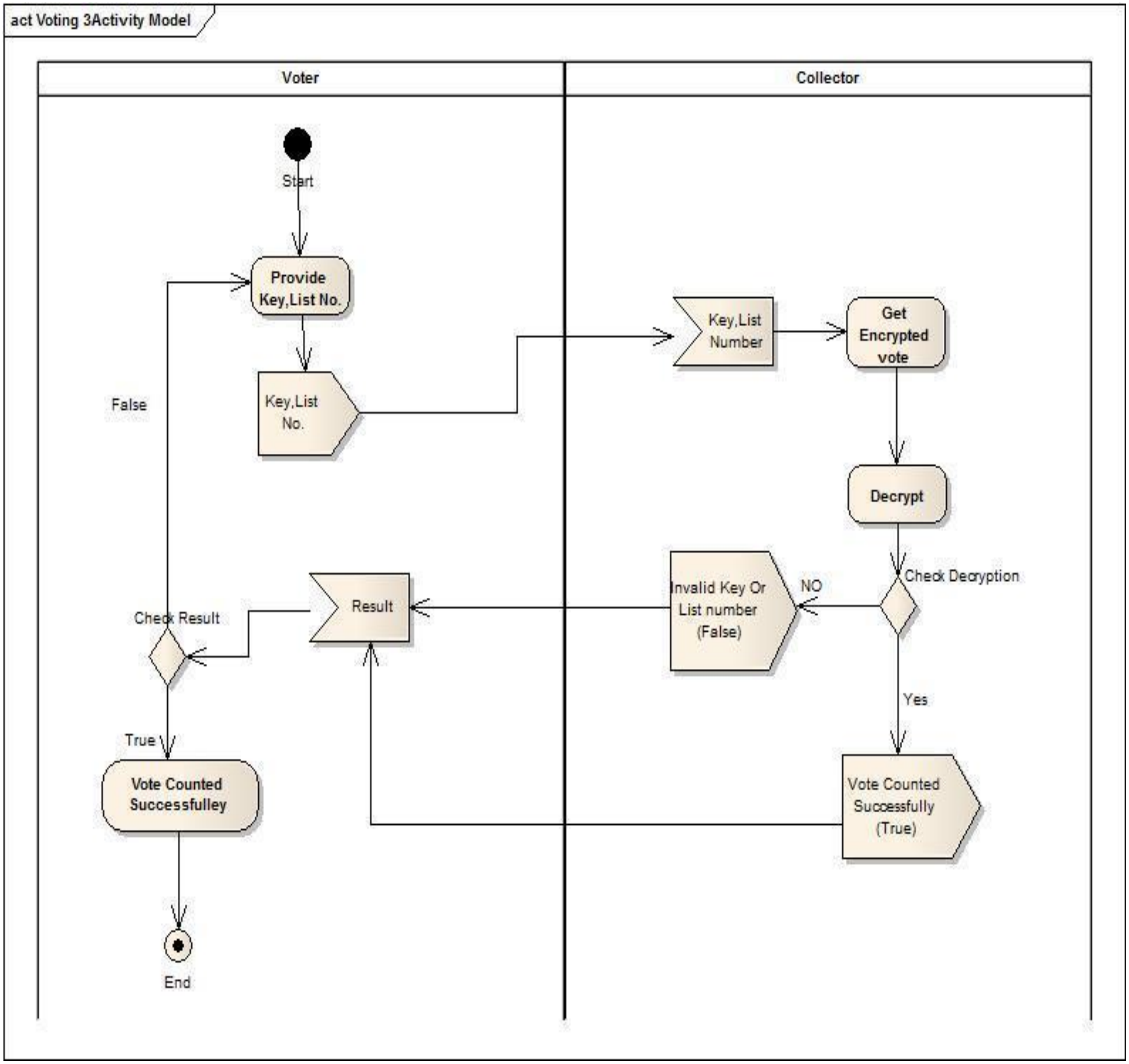


Figure 3-13: Counting phase.

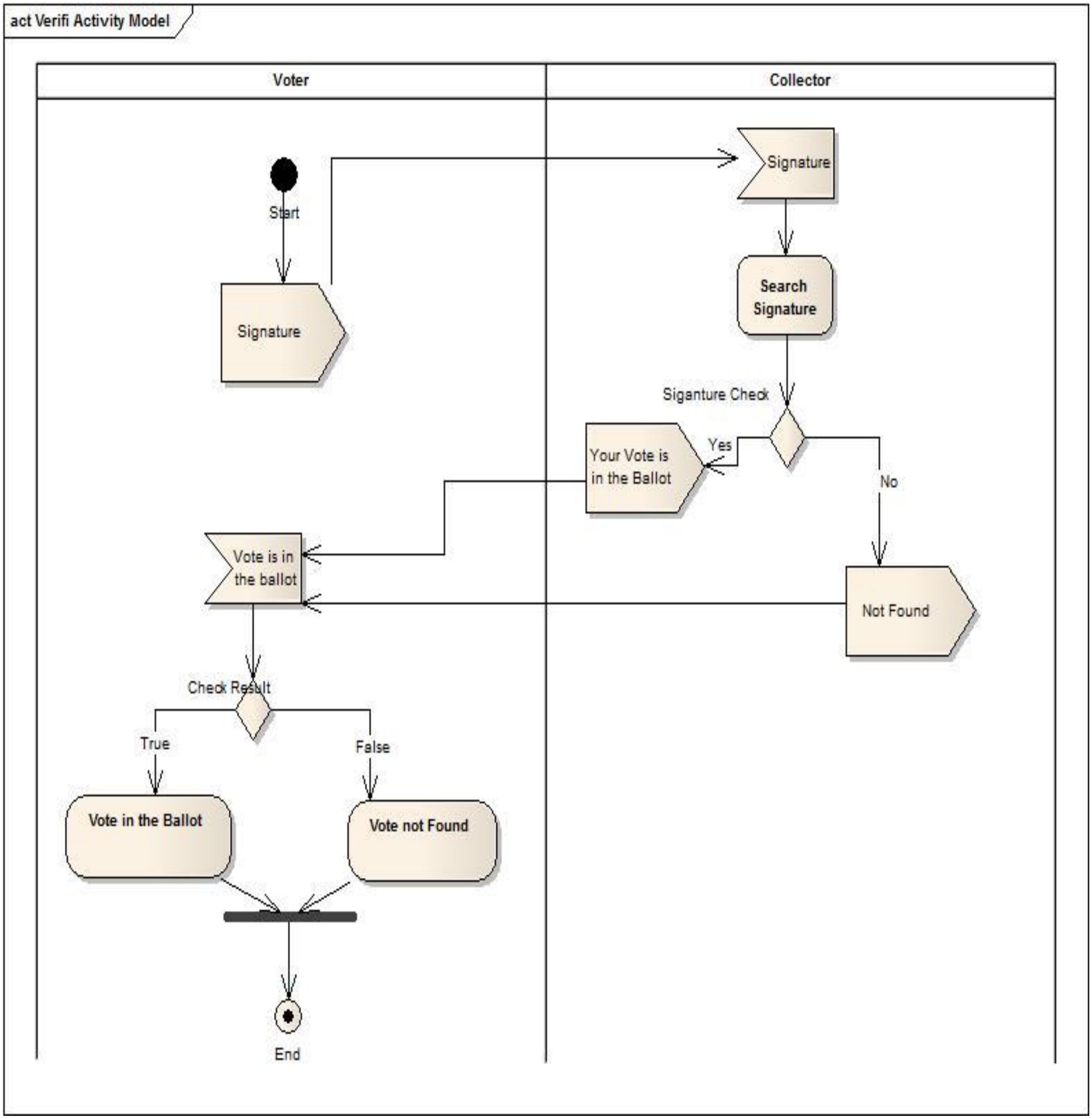


Figure 3-14: Illustrates group of Activity that provide voter to verify his vote counting.

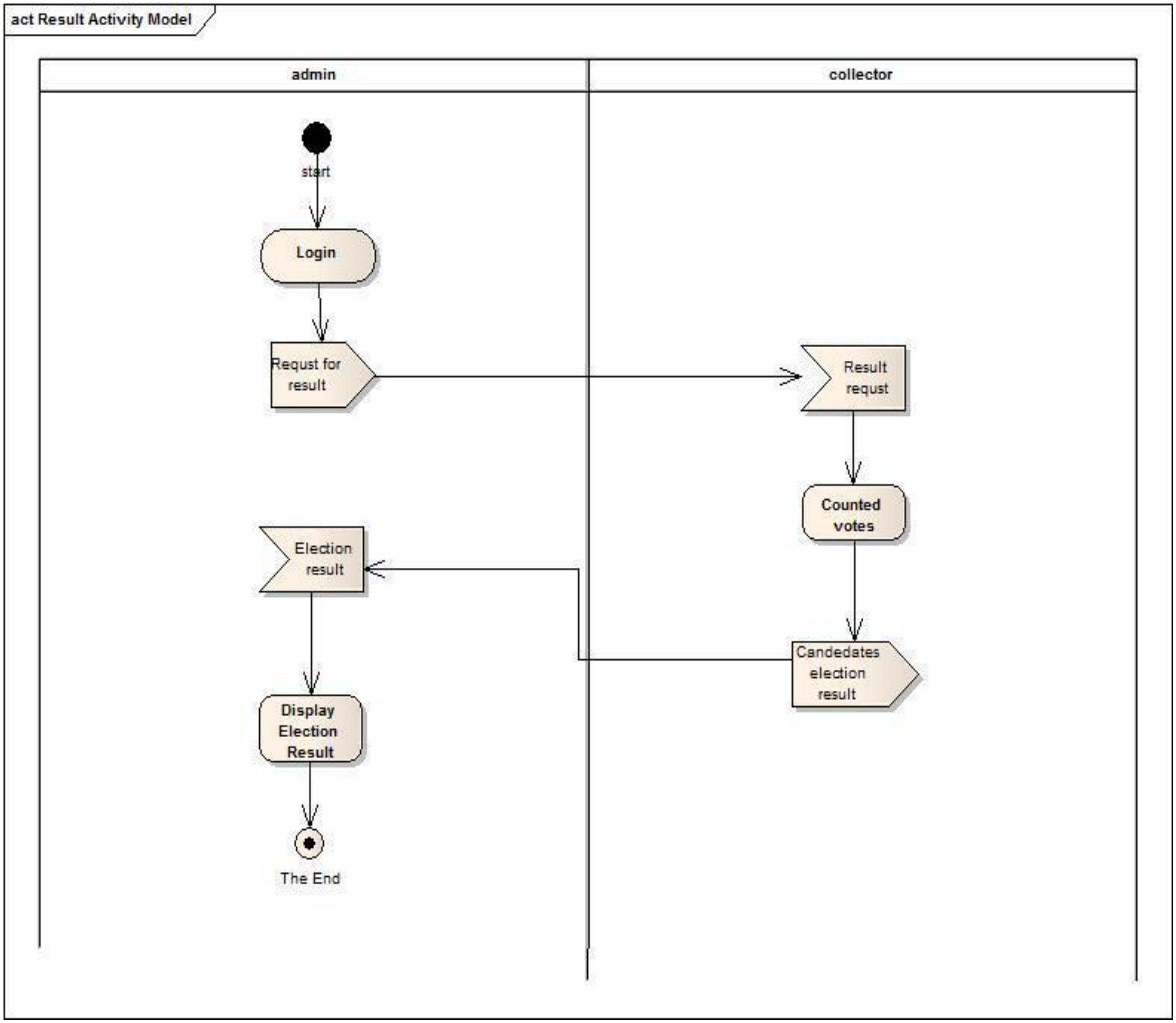


Figure 3-15: Illustrates group of Activity that support the admin to display final election result.

Chapter 4

Implementation

4.1 INTRODUCTION

In this section, the talk 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 13-6 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.

4.2 PRE- ELECTORAL PERIOD

4.2.1 Registration phase [18]

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).

4.2.2 Sudanese registration process principle [19]

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.

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.

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

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.

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).

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.

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.

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.

4.2.3 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.

ELECTORAL PERIOD [20]

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.

4.3 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.

4.4 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.

4.4.1 Registration Phase

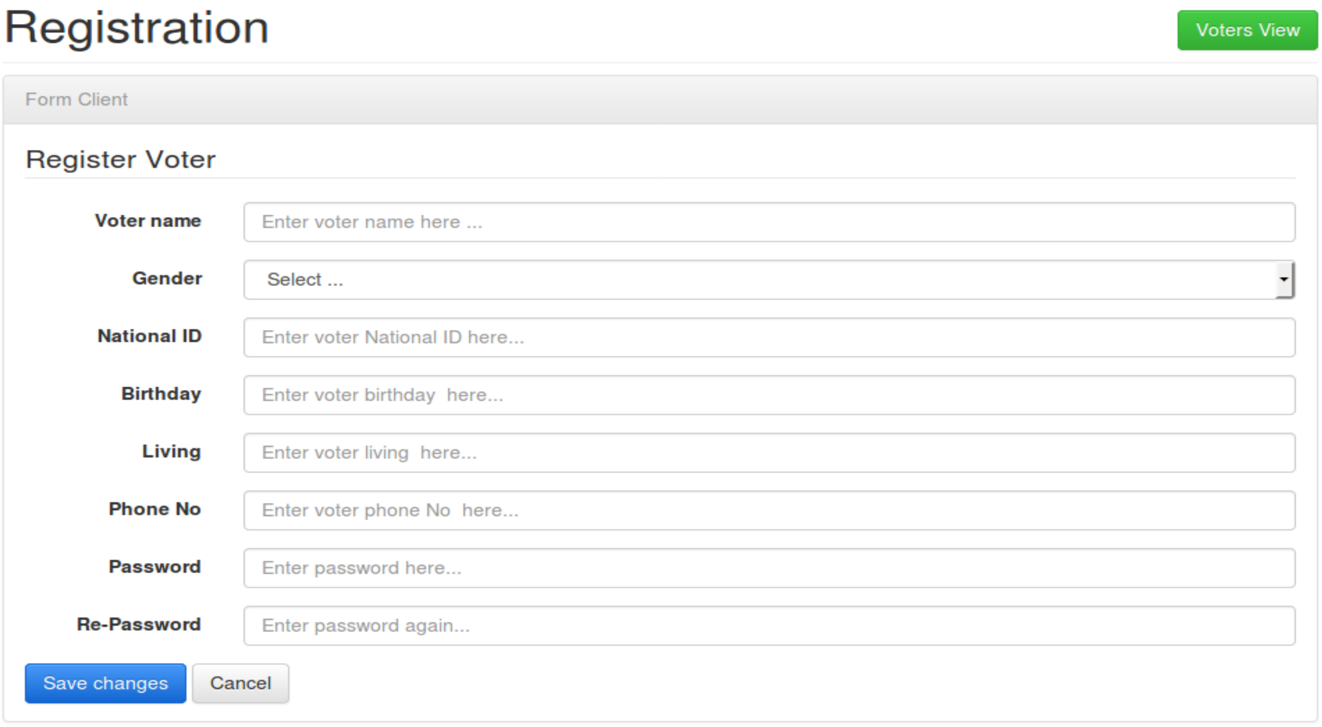
As mentioned at the start of this chapter an accurate and comprehensive voter register is a basic component of a credible electoral. The first problem is how to do an online authentication since proposal solution present a full online voting system.

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.).



Registration

Form Client

Register Voter

Voter name	Enter voter name here ...
Gender	Select ...
National ID	Enter voter National ID here...
Birthday	Enter voter birthday here...
Living	Enter voter living here...
Phone No	Enter voter phone No here...
Password	Enter password here...
Re-Password	Enter password again...

Figure 16: Registration System.

4.4.2 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.

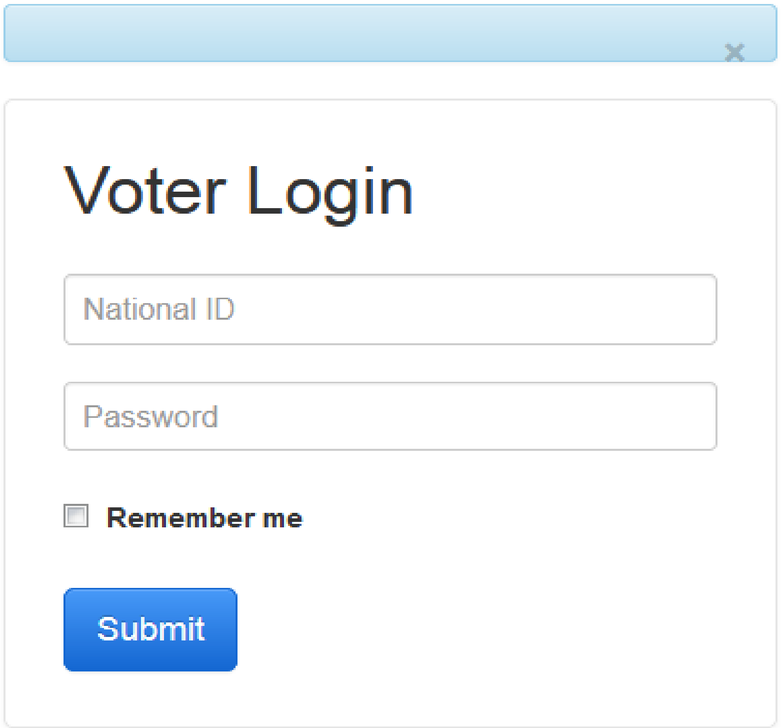


Figure 17: Authentication process.

Voting Phase

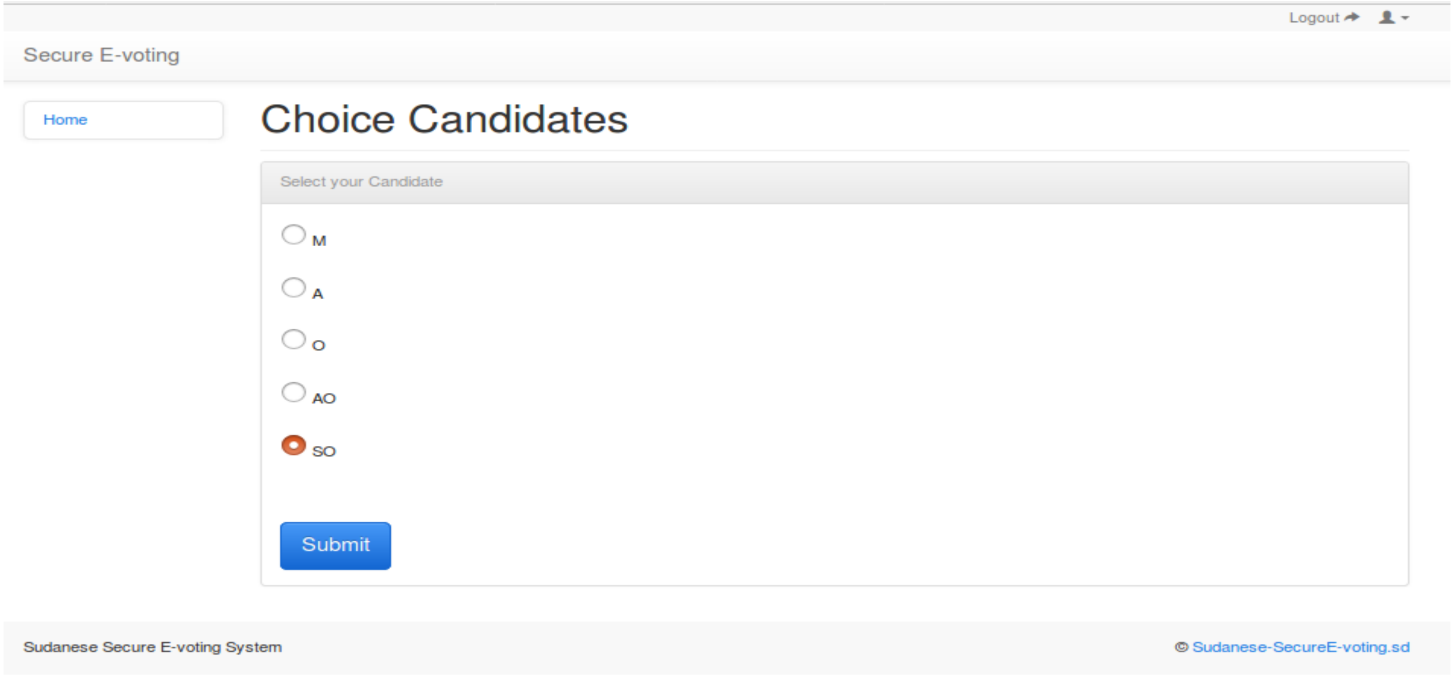
After administrator verify and validate token, provide list of candidate. In this process the following actions are carried out:

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.



Choice Candidates

Select your Candidate

○ M

○ A

○ O

○ AO

● SO

Figure 18: 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.

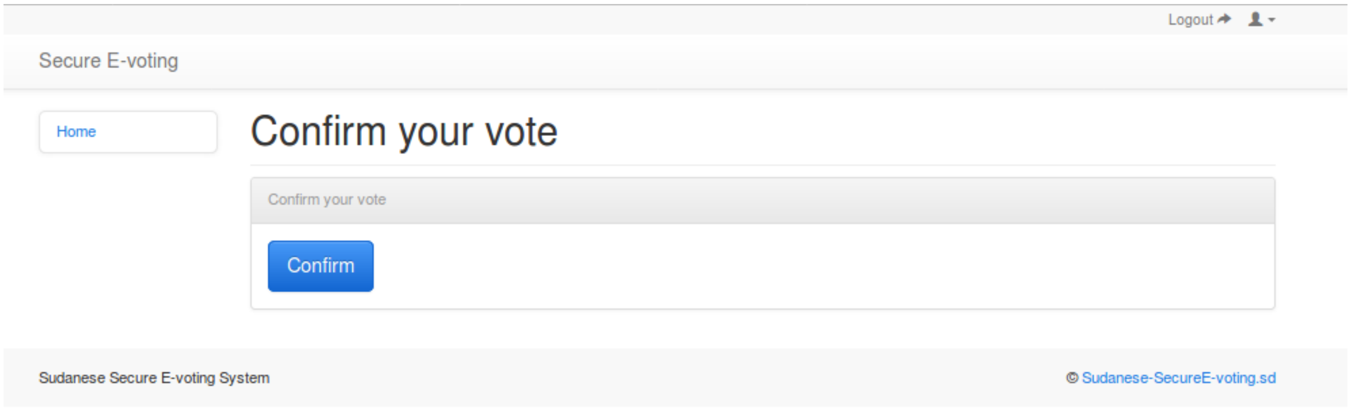
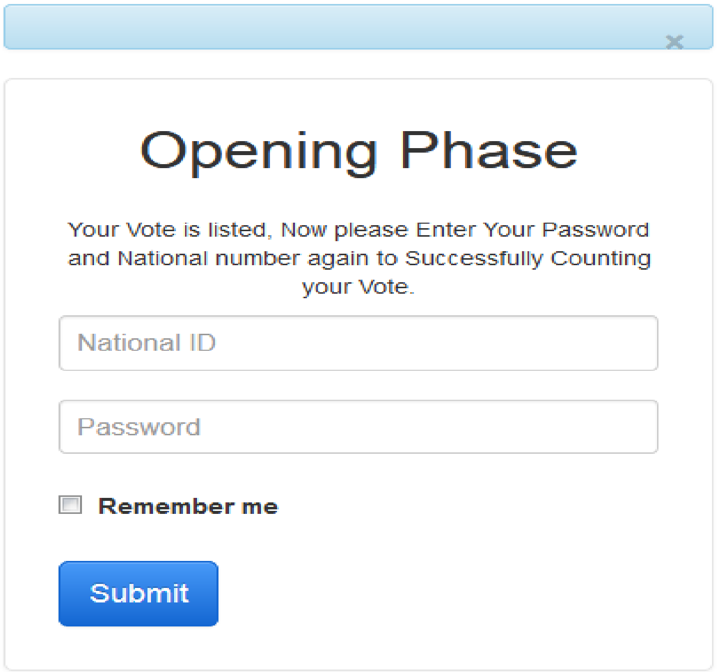


Figure 19: Verify.

Opening Phase

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

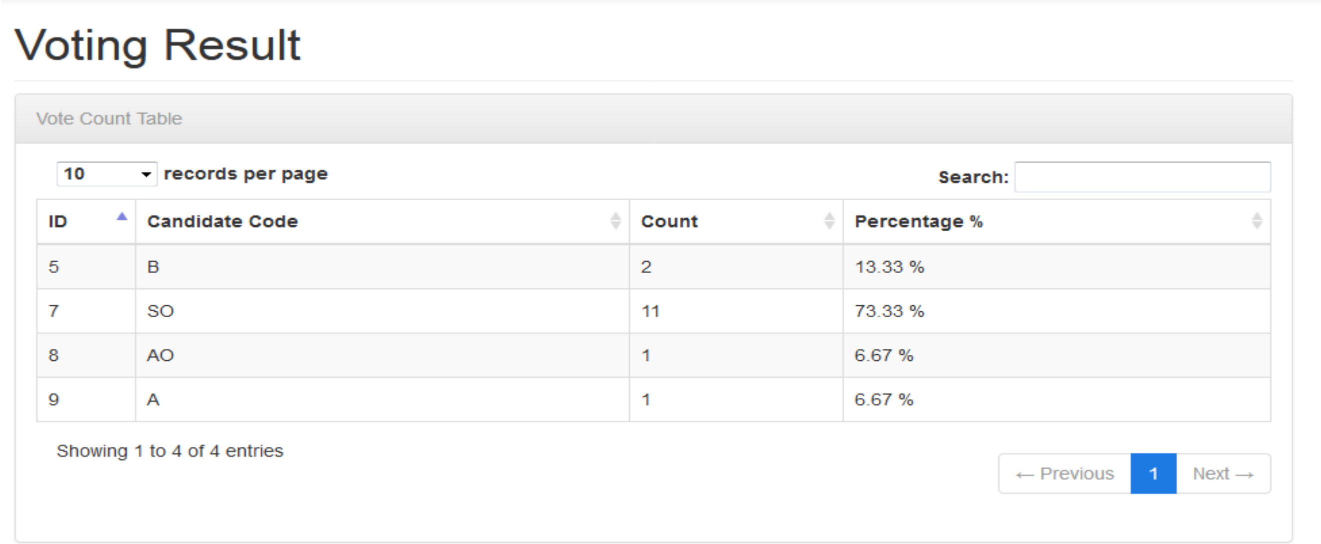


Your Vote is listed, Now please Enter Your Password and National number again to Successfully Counting your Vote.

Figure 20: Voter provide key.

Counting Phase

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



Voting Result

Vote Count Table

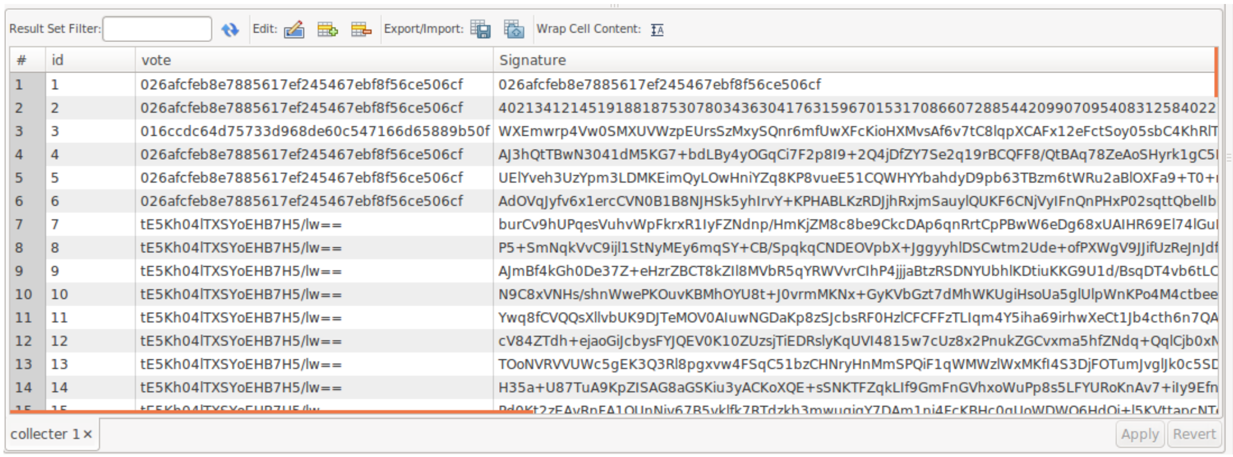
10 records per page

Search:

ID	Candidate Code	Count	Percentage %
5	B	2	13.33 %
7	SO	11	73.33 %
8	AO	1	6.67 %
9	A	1	6.67 %

Showing 1 to 4 of 4 entries

Figure 21: Voting Result.



#	id	vote	Signature
1	1	026afcfeb8e7885617ef245467ebf8f56ce506cf	026afcfeb8e7885617ef245467ebf8f56ce506cf
2	2	026afcfeb8e7885617ef245467ebf8f56ce506cf	40213412145191881875307803436304176315967015317086607288544209907095408312584022
3	3	016ccdc64d75733d968de60c547166d65889b50f	WXEmwrp4Vw0SMXUVWzpEUrsSzMxySQnr6mfUwXFcKioHXMvsAf6v7tC8lqpXCAFx12eFctSoy05sbC4KhRlT
4	4	026afcfeb8e7885617ef245467ebf8f56ce506cf	AJ3hQtTBwN3041dM5KG7+bdLBy4yOGqCi7F2p8I9+2Q4jDfZY7Se2q19rBCQFF8/QtBAq78ZeAoSHyrk1gC5I
5	5	026afcfeb8e7885617ef245467ebf8f56ce506cf	UElYveh3UzYpm3LDMKEimQyLOwHniYZq8KP8vueE51CQWHYYbahdyD9pb63TBzm6tWRu2aBlOXFa9+T0+
6	6	026afcfeb8e7885617ef245467ebf8f56ce506cf	AdOVqJyfv6x1ercCVN0B1B8NJHSk5yhIrvY+KPHABLKzRDJjhRxjmSauylQUKF6CNjVyIFnQnPHxP02sqttQbellb
7	7	tE5Kh04lTXSYoEHB7H5/lw==	burCv9hUPqesVuhvWpFkrxR1IyFZNdnp/HmKjZM8c8be9CkcDAp6qnRrtCpPBwW6eDg68xUAIHR69El74lGuI
8	8	tE5Kh04lTXSYoEHB7H5/lw==	P5+SmNqkVvC9ijl1StNyMEy6mqSY+CB/SpqkqCNDEOVpbX+JggyyhlDSCwtm2Ude+ofPXWgV9JJifUzReJnJdf
9	9	tE5Kh04lTXSYoEHB7H5/lw==	AJmBf4kGh0De37Z+eHzrZBCT8kZIl8MVbR5qYRWVvrClhP4jjjaBtzRSDNYUbhlKDtiuKKG9U1d/BsqDT4vb6tLC
10	10	tE5Kh04lTXSYoEHB7H5/lw==	N9C8xVNHs/shnWwePKOuvKBMhOYU8t+J0vrmMKNx+GyKVbGzt7dMhWKUgiHsoUa5glUlpWnKPo4M4ctbee
11	11	tE5Kh04lTXSYoEHB7H5/lw==	Ywq8fCVQQsXllvbUK9DJTeMOV0AIuwNGDaKp8zSJcbsRF0HzlCFCFFzTLIqm4Y5iha69irhwXeCt1Jb4cth6n7QA
12	12	tE5Kh04lTXSYoEHB7H5/lw==	cV84ZTdh+ejaoGiJcbysFYJQEV0K10ZUzsjTiEDRslyKqUVI4815w7cUz8x2PnukZGCvxma5hfZNdq+QqlCjb0xN
13	13	tE5Kh04lTXSYoEHB7H5/lw==	TOoNVRVVUWc5gEK3Q3Rl8pgxvw4FSqC51bzCHNryHnMmSPQiF1qWMWzlWxMKfl4S3DjFOTumJvglJk0c5SD
14	14	tE5Kh04lTXSYoEHB7H5/lw==	H35a+U87TuA9KpZISAG8aGSKiu3yACKoXQE+sSNKTFZqkLIf9GmFnGVhxoWuPp8s5LFYURoKnAv7+iIy9Efn
15	15	tE5Kh04lTXSYoEHB7H5/lw	Pd0Kt2zEAvBnFA1OUnNiv67B5vklfk7BTdzkh3mwuqiqY7DAm1nj4FcKBHc0qUoWDWO6HdOi+l5KVttancNT

Figure 22: Voting Database.

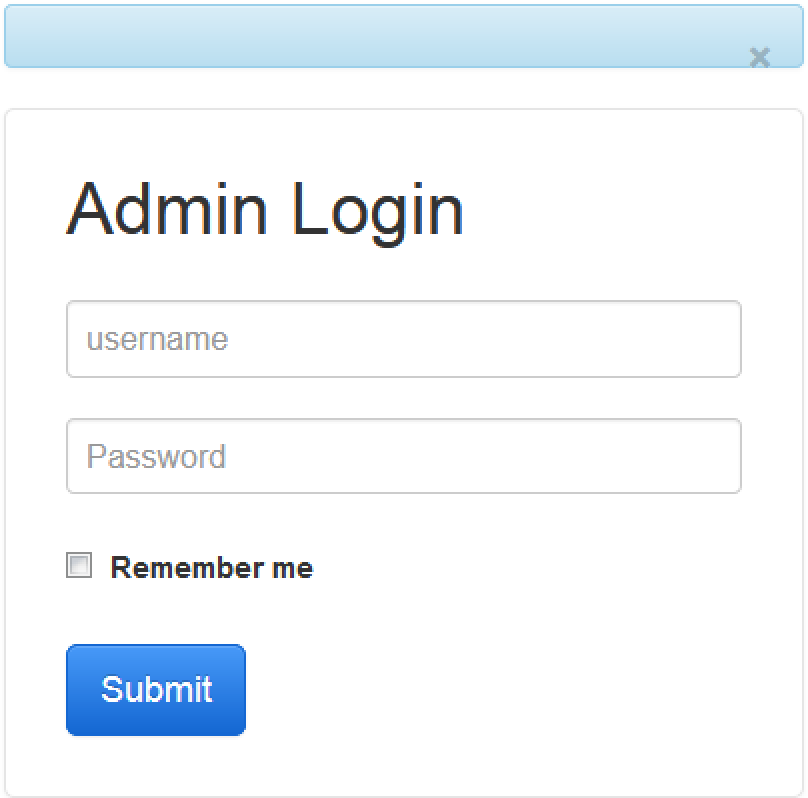
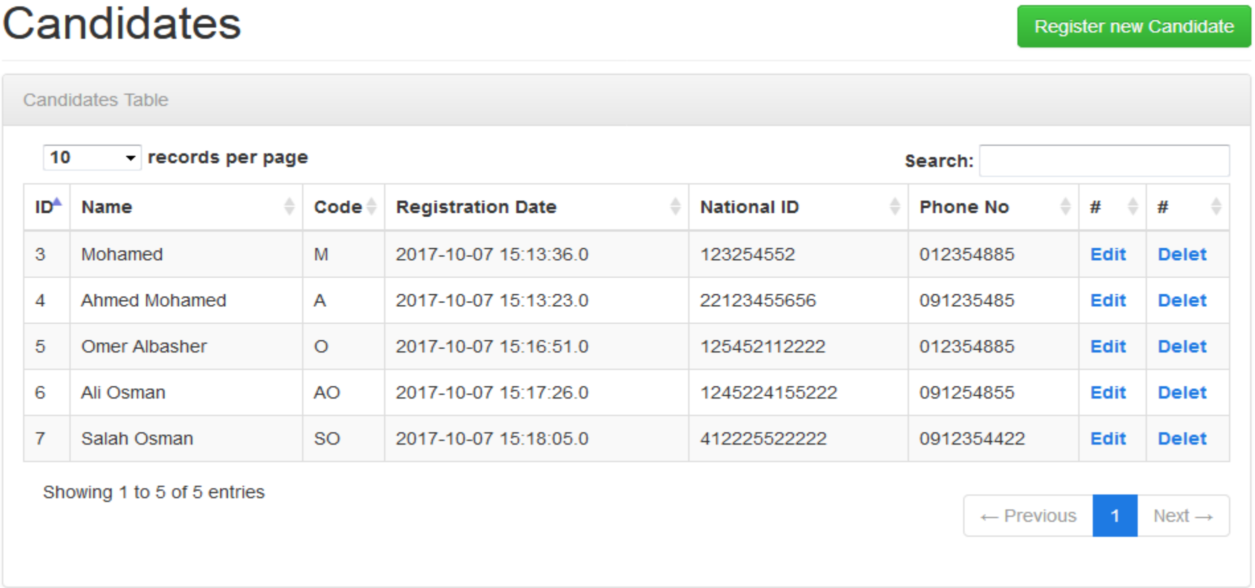


Figure 23: Admin login.



ID	Name	Code	Registration Date	National ID	Phone No	#	#
3	Mohamed	M	2017-10-07 15:13:36.0	123254552	012354885	Edit	Delet
4	Ahmed Mohamed	A	2017-10-07 15:13:23.0	22123455656	091235485	Edit	Delet
5	Omer Albasher	O	2017-10-07 15:16:51.0	125452112222	012354885	Edit	Delet
6	Ali Osman	AO	2017-10-07 15:17:26.0	1245224155222	091254855	Edit	Delet
7	Salah Osman	SO	2017-10-07 15:18:05.0	412225522222	0912354422	Edit	Delet

Showing 1 to 5 of 5 entries

Figure 24: Candidates list.

4.6 Tool and technologies used in the study

4.6.1 MVC Invalid source specified.:

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.

4.6.2 JAVA

Java is a general-purpose computer programming language that is concurrent, class-based, object-oriented, and specifically designed to have as few implementation dependencies as possible. It is intended to let application developers "write once, run anywhere" (WORA), meaning that compiled Java code can run on all platforms that support Java without the need for recompilation. Java applications are typically compiled to byte code that can run on any Java virtual machine (JVM) regardless of computer architecture. As of 2016, Java is one of the most popular programming languages in use, particularly for client-server web applications, with a reported 9 million developers. Java was originally developed by James Gosling at Sun Microsystems (which has since been acquired by Oracle Corporation) and released in 1995 as a core component of Sun Microsystems' Java platform. The language derives much of its syntax from C and C++, but it has fewer low-level facilities than either of them.

4.6.3 JAVA SCRIPT:

Is a high level, dynamic, UN typed, 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.

4.6.4 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.

4.6.5 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.

4.6.6 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

4.7 CRYPTOGRAPHIC PRIMITIVES

4.7.1 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.

4.7.2 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. It also has a verification key which the recipient can use to verify the legitimacy of the signature

4.7.3 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.

4.7.4 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.

4.7.5 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.

4.7.6 Wireshark:

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

4.8 RESULT AND DISCUSSIONS

4.8.1 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.

4.8.2 DISCUSSIONS:

In this section we will talk about the challenges we are faced before on e-voting and how we are solved it.

- **Possibility of stolen voter packages or identification cards:**

We are using complex password to prevent the brute force attack, and stored as hash password to be encrypted.

- **Misuse of elector's ID card and personal information voting by others without the knowledge of the elector.**

We are assume we have physical registration center, to verify and register the voter and give him secret password, only he can use it.

- **Possible pressure on electors to vote a certain way if in the presence of others.**

The system has the ability to adjust the vote of voters

- **Hacks or viruses attacking the system and altering election results.**

Voter’s votes in the database are encrypted and do not contain voter data or candidate’s data, only the collector he can verify the votes and count it.

- **Inaccuracies on the voters' list, resulting in one elector receiving a card intended for another elector.**

The elector list is designed very simply to make it easier for the user.

Chapter 5

Conclusion & future work

5.1 CONCLUSION

This 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 FOO 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.

Also 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 (Holomorphic 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.

5.2 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.

References

[1] C. LAMBRINOUDAKIS1, Electronic Voting Systems: Security Implications of the Administrative Workflow.

[2] R. F. Bauer, The American Voting Experience:Report and Recommendations of the Presidential Commission on Election Administration, January 2014.

[3] D. Jefferson, "If I can shop and bank online, why can't I vote online?," David Jefferson..

[4] F. Schneier, "http://www.wired.com/news/columns/0,72124-0.htm.," [Online]. Available: http://www.wired.com/news/columns/0,72124-0.htm..

[5] A. &. V. D. Franco, Small vote manipulations can swing elections. cations of the ACM, 2004..

[6] Safevote, Voting System Requirements, November 2000..

[7] Efficiency Comparison of Various Approaches in E-Voting Protocols, Oksana Kulyk, Melanie Volkamer, February 2016.

[8] Analysis of Security Requirements for Cryptographic Voting Protocols, Institute of Applied Mathematics, METU, Ankara, Turkey: Orhan Cetinkaya, 2007.

[9] J. Kitcat, "Electronic voting: I want to understand the issues," [Online]. Available: http://www.jasonkitcat.com/writings/e-voting/electronic-voting-i-want-to-learn/.

[10] Europe, Council, E-voting handbook, France : Council of Europe Publishing, November 2010 .

[11] A. Riera, Comments on the Report e-Voting Security Study, Communications- Electronics Security Group , 28 August 2002.

[12] Ben Goldsmith, Holly Ruthrauff, Building theSystem for E-voting or E-counting, 2007.

[13] TCommite, E-Voting system. 1 ed. Tallin: The National Election Commite, Accessed 2 September 2015.

[14] Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta, A practical secret voting scheme for large scale elections.Advaced in Cryptology - AUSCRYPT'92, 1992.

[15] Sector, Electronic Government," ITU Telecommunication Development Sector, Geneva 20, Switzerland., 2008.

[16] D. A. Gritzalis, "Principles and requirements for a secure e-voting system"..

[17] I. Z. S. Kimbi1, "A Secure Model for Remote Electronic Voting: A Case of Tanzania"..

[18] Y. Jung-Ying, Design and Implementation of , Taiwan: National Kaohsiung [Accessed 4 August 2015], 2008.

[19] Jung-Ying, Design and Implementation of , Taiwan: National Kaohsiung [Accessed 4 August 2015], 2008.

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

[21] Drew Springall, Security Analysis of the Estonian Internet Voting System, United States: University of Michigan, Ann Arbor [Accessed 30 August 2015]., 2014.

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

[23] Scott Wolchok, Attacking the Washington, D.C., United States.: University of Michigan [Accessed 19 September 2015]., 2010.

[24] http://www.schneier.com/crypto-gram-0012.html#..

[25] AllJoyn4 is a library which allows peer-to-peer communication between several devices..