Republic of Iraq
Ministry of Higher Education and Scientific Research
University of Anbar
College of Computer Science and Information Technology
Department of Computer Science

Enhanced I-Voting System based on Helios and Public Key Digital Certificates

A Thesis

Submitted to the Department of Computer Science College of Computer Science and Information Technology, University of Anbar as Partial Fulfilment of the Requirement for Master Degree of Science in Computer Science.

By:

Noor Hamad Abid

Supervised By:

Prof. Dr. Sufyan T. Faraj Al-Janabi

1441 A.H *2020 A.D*

اسم الطالـــــب: نور حمد عبد

الكليــــــــــة : كلية علوم الحاسوب وتكنولوجيا المعلومات - قسم علوم الحاسبات

عنوان الرسالة: نظام التصويت المحسّن على أساس هيليوس وشهادات المفتاح العمومي الرقمية

Supervisor's Certification

*I certify that I read this thesis entitled "***Enhanced I-Voting System based on Helios and Public Key Digital Certificates***" that was done under my supervision at the Department of Computer Science of the University of Anbar, by the student "***Noor Hamad Abid***" and that in my opinion it meets the standard of a thesis for the degree of Master of Science in Computer Science.*

Signature :

Name : Prof. Dr. Sufyan T. Faraj Al-Janabi

Date : / /2020

Certification of the Examination Committee

We the examination committee certify that we have read this thesis entitled " ***Enhanced I-Voting System based on Helios and Public Key Digital Certificates*** *" and have examined the student "* ***Noor Hamad Abid*** *", in its contents and what is related to it, and that in our option it is adequate to fulfill the requirements for the degree of* ***Master of Computer Science****.*

Signature:
Name: ***Ass. Prof. Dr. Salah Sleibi Mustafa*** ***(Chairman)***
Date: / / 2020

Signature:
*Name**:** **Ass. Prof. Dr. Alaa Kadhim Farhan*** ***(member)***
Date: / / 2020

Signature:
Name: ***Ass. Prof. Dr. Ahmed Noori Rashid*** ***(member)***
Date: / / 2019

Signature:
Name: ***Prof. Dr. Sufyan T. Faraj Al-Janabi*** ***(Supervisor)***
Date: / / 2020

Approved by the Dean of the College of Computer Science and Information Technology, University of Anbar.

Signature:
Name: ***Ass. Prof. Dr. Salah Awad Salman***
Title: ***Dean of the College***
Date: / / 2020

Student Name: Noor Hamad Abid

Thesis Title: Enhanced I-Voting System based on Helios and Public Key Digital Certificates

Abstract

Voting is the process by which representatives of the country (or an organization) are chosen. Everyone has the right to elect candidates who deem fit to lead the country. It must be ensured that the elections are fair and that votes are not manipulated, deleted or changed, or even that voters are forced to vote for candidates they don't want. Some voters do not go to the polls to vote for personal or public reasons. One solution to this problem is Internet voting (I-voting) where it can be voted from anywhere and anytime.

Internet voting has many advantages and certainly, there are disadvantages. Many I-voting systems have been proposed, but their use is low and uncommon in the world. This is due to the lack of confidence on the Internet among voters because it is possible that the system is being attacked from anywhere in the world and also not everyone in the world uses the Internet. The Helios Voting System, an open source system, is one of the most popular voting systems.

This thesis presents a proposed I-voting system based on Helios and a public key certificate. The reason for using Helios is that it is open-source, widespread use and easily accessible. Improvements to the Helios system have been proposed. A certification authority has been added which creates voter certificates containing public and private keys which are used later in the voting process, where it is used in encryption and digital signature. Signing the vote also added by either Rivest Shamir Adleman (RSA) or Digital Signature Algorithm (DSA) algorithm. Each voter has given one real account and other fake accounts to be used in case the voter is coerced. Finally, the Helios interface has been improved and the Arabic language has been added to the system.

The system has been tested and the timing needed to sign and encrypt the vote has been calculated and compared with Helios. It was found that adding the certification authority increases safety and scalability, and also the time taken for the proposed system compared to the original system is very close despite the addition of the digital signature. Adding multiple accounts makes the voter more free to choose the account she wants and use it in coercive situations. The new interfaces have been also tested, and a questionnaire of 60 people has been conducted. The results have indicated that the satisfaction level of voters is higher for the proposed system compared to the original Helios interfaces.

Keywords: Internet Voting, Certificate Authority, Helios, Multi-Accounts, Public Key Certificates, Interface.

Acknowledgments

First of all, I would like to express my thanks and gratitude to ***ALLAH the Almighty****, who granted me all graces.*

*I would like to express my appreciation and gratitude to my supervisor Prof "***Dr. Sufyan Al-Janabi***" for his guidance, encouragement, advice and support during this work.*

My special thanks go to the people who supported me and encouraged me, especially my friends ***"Farah and Amal"****.*

*Special thanks to "***assist. Prof. Dr. Salah Awad***", Dean of the College of Computer Science and Information Technology for his valuable cooperation.*

And special thanks to the ***staff*** *of the College of Computer Science and Information Technology.*

Noor Hamad

Dedication

This thesis is dedicated to:

My parents

My brothers

My sisters

And my friends.

Noor Hamad

Contents

List of Figures

List of Algorithms

List of Tables

List of Abbreviations

BPS	Ballot Preparation System
CA	Certification Authority
CP	Certificate Policy
CR	Certificate Repositories
CRL	Certificate Revocation Lists
DB	Data Base
DRE	Direct Recording Electronic
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
E-voting	Electronic voting
FIPS	Federal Information Processing
ID	Identification
I-voting	Internet voting
ms	millisecond
MTV	Model-Template-View
NIST	National Institute of Standards and Technology
NOTE	Name and vOte separaTed Electronic voting
OS	Operating System
PDF	Portable Document Format

PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
RA	Login Authority
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SPKC	Simple Public Key Certificate
URL	Uniform Resource Locator
V3	Version 3
VCC	Vote Counting Committee
VOIP	Voice Over Internet Protocol
XSS	Cross-Site Scripting
ZKP	Zero-Knowledge Proof

Chapter One: Introduction

Chapter one

Introduction

1.1 General Background

Elections are an act of democracy that transcends divisions among people. Thus, elections encourage individual freedom according to law, where people can express themselves according to their choice. This gives an opportunity for people to freely express their opinions on various issues, not just choose a person representing them. Elections are very important and must be fair and not manipulated so as not to choose a corrupt person [1].

There are several ways to vote, most notably paper voting, which used paper to vote. In this way, voters vote by depositing their ballot papers in sealed boxes and distributed to constituencies throughout a country. The ballot boxes are opened after the election period ends, and in the presence of the authorized officials, the votes are counted manually [2].

Although there are many benefits to paper-based voting such as it can be used by all people, even those who do not have experience in technology, there is less possibility to add papers containing false or fake votes, and more importantly, people trust in this kind of voting. However, paper voting has many disadvantages, like it consumes a lot of paper resulting in damage to the environment, voters may find a way to vote more than once, there may be a mistake in the counting process, besides it takes a long time to count the votes and sometimes the election results are manipulated in favor of a candidate [3, 4].

The development of technology and its entry into almost everything influenced the voting process and the emergence of so-called electronic voting. Electronic voting was developed to eliminate the shortcomings and drawbacks of traditional voting. Electronic voting is a collection of opinions of citizens, which are widely disseminated, with the help of electronic means, including casting, transmitting, tallying and reviewing votes. Citizens of many countries have demanded the introduction and adoption of electronic voting, especially in developing countries because they believe that traditional voting is often marred by widespread fraud [5, 6].

Electronic voting has many advantages including the speed and accuracy of counting and giving results in hours or less. Also, the cost is low, and the use of cryptographic methods to store votes in an unknown location. On the other side, electronic voting can be vulnerable to penetration. Indeed, not everyone has experience in technology and can comfortably use this type of voting. Confidence and trust is another challenging issue in this respect. If the company responsible for the voting system is corrupt and the security policies are not correctly enforced, this means giving the possibility of controlling the entire voting process such as adding or deleting votes or even modifying them [7, 8].

Internet voting (I-Voting), which is a type of electronic voting used in elections at the national level in only a few countries. It is a voting mechanism that is increasingly being explored as a means to allow access to the election process for voters who may otherwise find it difficult to go to their polling location on Election Day. Internet voting, however, presents a number of technological challenges focused on security, privacy, and secrecy issues, as well as challenges for stakeholder involvement in and observation of the process. All of these must be comprehensively addressed for election authorities to consider moving forward with Internet voting [9].

The first use of Internet voting for a binding political election took place in the US in 2000, with more countries subsequently beginning to conduct trials of and/or use Internet voting. A total of 14 countries have now used remote Internet voting for binding political elections or referenda. Within the group of Internet voting system users, four core countries have been using Internet voting over the course of several elections/referenda: Canada, Estonia, France and Switzerland. Estonia is the only country to offer Internet voting to the entire electorate. The remaining ten countries have either just adopted it, are currently piloting Internet voting, have piloted it and not pursued its further use, or have discontinued its use [10].

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

The Helios system is a widely used voting system that tries to meet these criteria as it is used in many small-scale elections.

1.2 Literature Review

Although the Helios voting system is used in many elections held online, it needs some improvements. In literature, researchers analyzed the Helios system and made some improvements and suggestions that make the Helios voting system better to use. Each of these researches has its advantages and limitations. In this section, the most relevant papers are reviewed.

In **2011, Fatih Karayumak *et al.*** analyzed the verifiability and ballot casting procedures of the Helios voting system by using a cognitive walkthrough approach. They demonstrate that Helios voting system needs to improve the verifiability and usability before using it in large-scale elections. New interfaces have been proposed for Helios and other voting systems based on their findings. In this study, the emphasis was placed on the client side and the first part of individual verification only [11].

In **2011, Fatih Karayumak *et al.*** tested the proposed enhancement of Helios interface for individual verifiability and vote casting in the previous work and applied it to 34 voters in mock primaries. Before and after the elections voters were given instructions as well as filling out questionnaires. A helmet has been used to track eye movements and data has been collected on time and mouse movement. They argued that the interface is easy to use, while some voters found it difficult to understand the motives behind individual verification. The ease of use of the voting system after improvements has reached an acceptable level compared to the original version of Helios [12].

In **2014, Véronique Cortier *et al.*** provided a verifiability definition in the computational model to count for a virulent bulletin board that may be filling ballots. Then, they introduced a new scheme that makes weak verifiability in systems (which means the verifiability of honest Login authority and sincere bulletin board) into strong verifiability (which means system verifiability under weaker trust assumptions, namely, that the bulletin board and the Login authority aren't simultaneously dishonest). For simplicity, this scheme was presented to a single trustee and for a single vote (yes/no). The schema can be extended to multi-trustee and multi-candidate elections with threshold decryption. The Login authority can simply convey private credentials to voters and distribute the corresponding public credentials. The application of these constructions results in a system similar to Helios having strong verifiability and ballot privacy. The Helios-C system has been implemented and tested and has remained a conservative on Helios simplicity [13].

In **2015, Oksana Kulyk *et al.*** introduced a new way to achieve the participation privacy and private eligibility verifiability by filling the real votes with empty votes that can't be distinguished from non-empty votes. With this, the presence of empty votes obscures those who have already voted. In this scheme, the voter cannot prove that she/he voted for a specific candidate, so this scheme provides the receipt-freeness. But this scheme is still vulnerable to randomization and forced abstention attacks. In this scheme, voters do not want to take part in the aspects of participation privacy and the receipt-freeness can ignore them and vote. However, the possibility of their participation is still sufficient to provide them with privacy. Some problems that may be faced are the usability and understanding: such as the confusion of voters when they see many votes in their row or remember all the votes that have been cast to be capable to update and thus lead to mistrust in the system [14].

In **2016, Daniel Chung *et al.*** discovered the risk of distributed denial-of-service attacks on individual election servers. Malicious attacks are not simple and can be distributed from remote locations. A single attack on election servers could cause complete disruption to an indefinite time, a big problem because election time is limited. Their solution was to replicate Helios into a network of multiple servers. The problem of maintaining the state through the various servers was handled in a potentially flawed network, by increasing Helios with Paxos protocol (a fault tolerant protocol designed to ensure progress and safety in an incomplete environment). The biggest problem with Helios replication is the cost of latency associated with implementing a secure protocol over an insecure network. High latency can negatively affect the usability of the voting system. The delay that occurs can lead to the distraction or surrender of the user and not complete the vote, especially without understanding the reason for the delay [15].

In **2016, Oksana Kulyk *et al.*** expanded the Helios system toward proxy voting, allowing voters to delegate a trusted proxy to vote in their place. They provided new credentials that called delegation credentials. This scheme secures the process of delegation by ensuring that the selection of the proxy by the voter and vote process is private, and the proxy cannot vote unless allowed by the voter. In addition, all delegate votes from voters that have not been overwritten by a higher priority authorized vote or direct vote by the voter, are properly included. It also prevents the proxy from proving the number of votes obtained, and at any time the voter can cancel the delegation and vote directly. The proposed system maintains the special safety requirements for proxy voting as well as safety requirements for the main Helios system [16].

In **2016, Michael Backes *et al.*** performed an automatic security analysis of JavaScript of the Helios voting system. They analyzed the actual JavaScript implementation despite being thoroughly analyzed by the security society. Large-scale JavaScript security analysis can cause significant technical challenges. These challenges can be overcome by creating a series of transformations in the program, which makes JavaScript of Helios available to current analysis techniques. They then analyzed the transformed client by using a histogram, reducing 7 million nodes representing the flow of information to implementation of the client into a few harmful flows comprising less than 40 nodes. This analysis resulted in the discovery of two security holes that affect the Helios version, a minor flaw that results in leakage the plaintext ballot and a large security vulnerability in XSS that has been escalated into arbitrary execution of the script. These attacks can be overcome by a simple modification to Helios. The transformations of their program result in a low surface attack and a version of the system with fewer external reliance [17].

In **2016, Nicholas Chang-Fong *et al.*** conducted a security analysis on the Helios system and carried out exploits and discovered a range of weaknesses attacking integrity, availability and confidentiality that affect the voting process. Some of these weaknesses are allowing a malicious voter to make a distorted vote to prevent the counting of final votes, allowing an attacker to vote on behalf of the voter, and allowing corrupt election administrator to give random results and accept evidence of their validity. The problems related to privacy, including the generation of random number bias, which affects the encryption of votes, were examined. These issues have been reported, and they worked with Helios designers to fix them [18].

In **2018, Elizabeth A. Quaglia *et al.*** provided work to wipe out trust assumptions placed on external authentication service operators. Helios-C system which based on Helios and invented by Cortier et al. have made progress in this direction by signing the ballots. They discovered that with an opponent controlling the communication channel or bulletin board, the confidentiality of the ballot was not satisfied and thus the verifiability was not satisfied either in the Helios-C system. They proved that the correct construction of both the signature and the ballots of the Helios system is sufficient for non-malleability. This prompted them to design construction and led to accompanying security evidence that it produces systems which satisfy the verifiability and secrecy of the ballot [19].

In **2018, Ben Smyth** studied game-based definitions of universal and individual verification by Clarkson, Smyth and Frink. It has been demonstrated that building the voting systems from El Gamal along with the generation of correct key is sufficient for individual verification. It is also sufficient for universal verification. Thus, proof of universal verification is simplified, as well as eliminating the costs of individual verification proof of voting systems based on a class of encryption. In addition, he analyzed the implementation of individual and universal verification of Helios Mixent. It has been shown that because of the security gaps in the Helios voting system, the aspect of universal verification soundness is unsatisfactory. Reform of these problems was proposed and proved that this reform is sufficient for universal and individual verification [20].

In **2019, Maxime Meyera *et al.*** showed that the attacker in the Helios system could cause a vote other than the last vote of the voter. The attacker can intercept the authorization code associated with the vote that the attacker wants to cast, then the intercepted token is released after the voter casts his final vote. The released code causes the bulletin board to archive the last voter's vote and accepts the attacker's vote. Thus, the Helios system does not satisfy non-reusability. They showed that the attacker could choose the contents of such votes. The attacker can exploit the voter's educational needs and vote as the attacker wants. Thus, attackers can unduly influence voters' choices. The voters can detect this malice, but there is no evidence that these malicious practices have occurred and therefore voters have little recourse [21].

1.3 Problem Statement

I-voting systems in general still need many improvements in various aspects in order to be nationally and internationally widely accepted and deployed. Helios as one of the most interesting I-voting platforms is not excluded from this. Despite the previous suggestions to improve Helios in the literature, however, there are aspects that have not been resolved or that need more work on them, such as:

1. The Helios system can only hold elections in a low-risk, small-scale environment, but in large-scale elections, the attacks would increase and thus threaten the security of the system [22].
2. Helios does little to save voters from coercion. The coercer can dictate his orders to the voter throughout the election process and verify that the voter has complied with his orders [23].
3. The terms used are incomprehensible and misleading to non-expert voters, and the audit process is confusing, as explained in [24] that 38% of voters did not complete the process successfully, we can say that usability is below average.

1.4 Research Objectives

The main objective of the research is to use Helios as the basic I-voting engine and enhance it in order to build an I-voting system:

1. The proposed system should be more secure and scalable by adding a digital signature to vote via the RSA and DSA algorithms. Also, adding a certification authority that creates public and private keys for the encryption and digital signature process.
2. The proposed system must be less vulnerable to coercion, by adding four accounts to each voter who uses it in the event of subject to coercion.

3. The proposed system need to be easier to use by deleting unnecessary commands and adding an explanation of some steps in the Helios system. Also make it used by a larger segment by adding the Arabic language to the interface.

1.5 Thesis Outline

In addition to this chapter, the rest of the thesis is organized as follows:

Chapter Two: Represents a theoretical background on all concepts used in the proposed system. Also, some of Internet voting schemes.

Chapter Three: Shows the design and implementation stages of the proposed system.

Chapter Four: Presents the results of performed experiments of the proposed System.

Chapter Five: Summarizes the final conclusions and recommendations for future works.

Chapter Two: Theoretical Background

Chapter Two

Theoretical Background

2.1 Introduction

Internet voting has been on its way to maturity over the past years. There have been many concerns and discussions about the possibility of holding secure elections electronically, especially crucial elections such as government elections. People were worried that if something went wrong or something out of control, the consequences would be dire. However, the election today offers more and more electronic means to participate. Although these means have restrictions such as the use of special booths or special devices but remain a major step towards real I-voting [25].

In this chapter, an introduction to I-voting is provided, as well as basic mods and some characteristics and requirements for I-voting are presented. Then, some of the proposed I-voting schemes are reviewed. Then the strengths and weaknesses of I-voting are mentioned. This chapter also includes a detailed explanation of the steps of the Helios system and its advantages and disadvantages, as Helios is the basis of the proposed system. Finally, the public key infrastructure, public key certificates and digital signatures are briefly explained.

2.2 Internet Voting

Internet voting (I-voting) is one method of electronic voting that can be deployed under two circumstances: uncontrolled environment and controlled environment. An uncontrolled environment means the possibility of using any public computers, workplace computers or personal computers in the voting process. While a controlled environment means the use of voting machines like computers that controlled and monitored by the election authority, as shown in Figure 2.1 [26, 27].

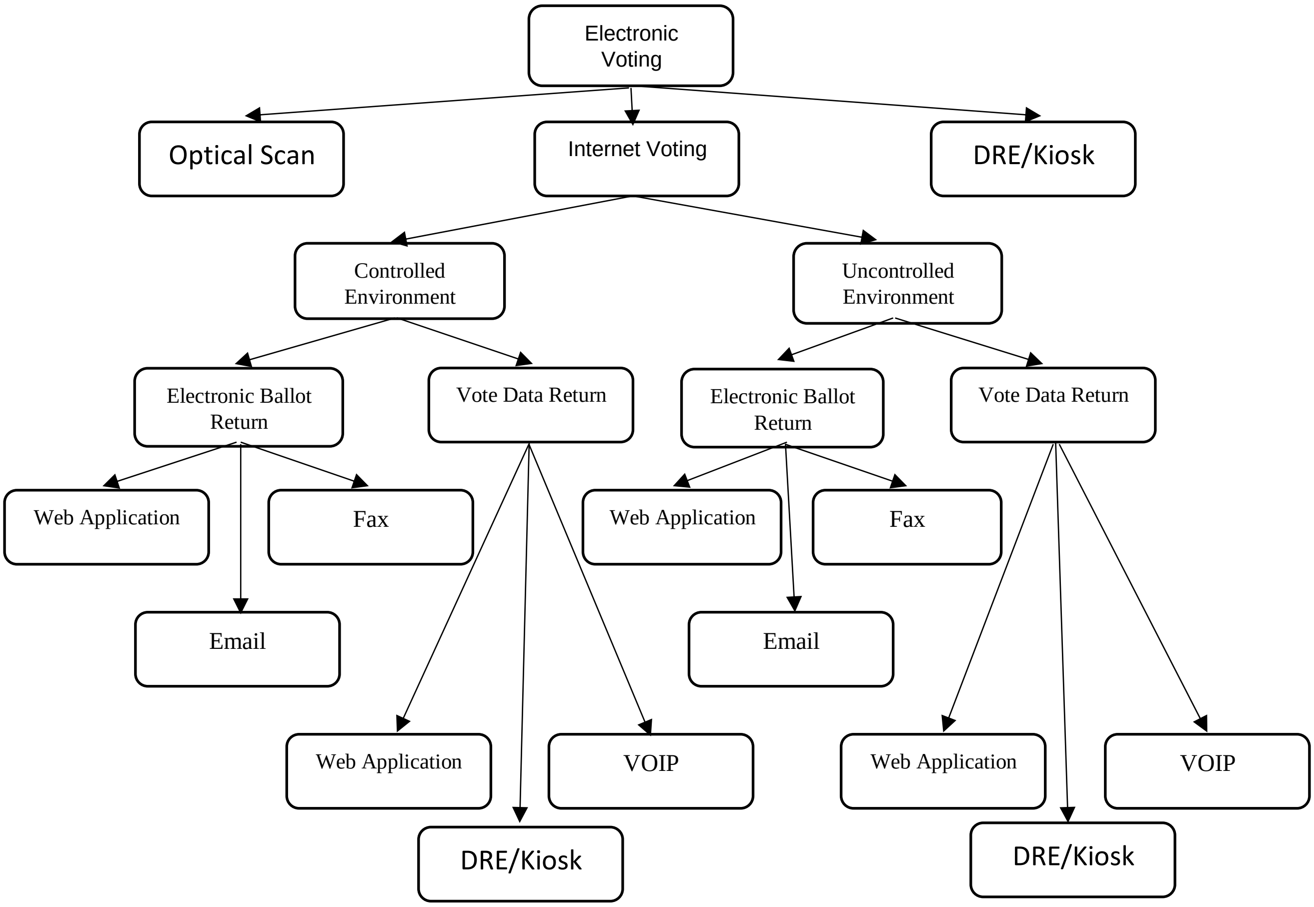


Figure 2.1: Electronic voting categories [27].

I-voting means that elections are held from anywhere, at any time and on any device. This procedure provides many facilities to ensure the participation of the largest segment of people in the elections, such as the participation of people with special needs or if the polling stations are far from voters and many problems. Many I-voting schemes appeared, but few voting systems were successful [28].

Despite the many benefits of the I-voting, it is not widespread in the world, and there are few countries that use it like Estonia and Switzerland. Building an I-voting system is not easy. The security level must be high, transparent, easy to use and, most importantly, voters must trust it and use it instead of the paper ballot. At present, the paper voting process cannot be cancelled and replaced by an I-voting due to the digital divide, but it needs more time to ensure its effectiveness and voters confidence in this system. Therefore, it is used in some countries as a supplement to a paper ballot [22, 29].

2.3 I-Voting Basic Mode, Characteristics, and Requirements

The basic participants in the elections are the voters and the authorities. Thus, it is possible to consider the following terms [30]:

- *Votes:* Voting is the process of answering questions in elections and selecting candidates. The structure of votes depends on the type of election.
- *Voters:* Voters do not want to annoy themselves with a complex election process so it should be easy and simple. Voters can abstain if they want. Also, all information about voting must be confidential and no one can access it.
- *Authorities:* The authorities are people run the election process and are keen to protect it from attacks and they are also voters that sometimes entitled to vote.

Typically, the main phases of I-voting consists of [31]:

- *Initialization phase:* In the first phase of the elections, the system is established, the secret and public keys are set up, the persons eligible to vote are declared, and the questions and answers are formulated. All this is done by the authorities.
- *Voting phase:* In the second stage, eligible voters will have access to a system to vote, and the votes will be sent to the relevant authorities for the next stage.
- *Counting phase:* In the last stage, the authorities reach the votes using secret and general keys, and then these votes are counted and the final result is published where the voters can make sure that their votes have been counted.

The main characteristics of I-voting are [32]:

- Providing an easy-to-use environment that for Internet-based systems is reachable through a traditional WWW browser.
- Counting the final vote tally after the end of the election automatically.
- Supporting all the required services for conducting and organizing the process of opinion expressing. Relying on the process of election these

services may be Login of the voter, authentication of the voter, casting the vote, calculation of the vote tally and verification the result of the election.

- Assisting the voter by supporting collaborative techniques, and all relevant behavioral and social aspects must be taken into account.
- Supporting the active participation in the elections, including representatives of parties, voters, candidates, election organizers, and administrators (monitoring voting centers, managing eligible voters and voting areas, ballot generation and management, remote voting areas, etc.)

However, there are many opportunities for corruption during performing these tasks. Election organizers may permit the Login of unqualified voters or allow voters to vote more than once. Achieving privacy and security is not easy if the system is not properly built and easily hacked. This could corrupt the voting process and violates the privacy of the voter. A secure and efficient voting protocol for the voting system should be implemented to prevent fraud and violation of voter privacy. In this respect, it can be shown that I-voting needs the following requirements [33-35]:

- *Accuracy:* Votes must be recorded in the system and only valid votes are counted.
- *Eligibility:* Only eligible voters have the right to vote.
- *Reliability:* Even if the system encounters a failure it must be able to continue working.
- *Coercion-Resistance:* The voter must not be forced to choose a candidate he/she doesn't want. There must be no proof of how voters voted.
- *Privacy:* The voter's vote must not be known by anyone and remains hidden.
- *Flexibility:* The system must accept different formats used.
- *Receipt-Freeness:* The voter must not be given anything that proves his/her vote to a particular person because it can be used by the coercer against him.
- *Completeness:* Calculating all valid votes correctly.

- *Auditability:* Election records must be reliable.
- *Integrity:* After the election, there must be no deletion, replacement or removal of votes.
- *Uniqueness (Unreusability):* Each voter is entitled to vote once.
- *Verifiability:* After the election is over, there must be a possibility to verify the election and that the votes have been counted correctly.
- *Anonymity:* No one should know who voted in the elections.
- *Secrecy:* No one can know how voters voted in elections.
- *Fairness:* Only the final result is announced and there are no partial results.

2.4 Primary Cryptographic Techniques

Some of the primary cryptography techniques typically used in I-voting systems are: ElGamal, homomorphic encryption, mixnets, and blind signature. The relevant I-voting schemes are described in the following subsections.

2.4.1 ElGamal Cryptographic System

ElGamal is a public key scheme based on discrete logarithms and associated with Diffie-Hellman technology, announced by Tahir ElGamal in 1984. ElGamal cryptographic system is used in some formats in a number of standards, including the S/MIME e-mail standard and the Digital Signature Standard (DSS) [36].

It uses the same domain parameters of Diffie-Hellman Key Exchange **(p, q, g)** and private/public key pair **(b, B = g^b mod p)** for a recipient **B**. The plaintext message to be encrypted needs to be encoded as an integer ***m*** in the range **[1, p – 2]** [37].

Algorithm 2.1: ElGamal Encryption

```
INPUT: Domain parameters (p, q, g); recipient's public key B; encoded message m in range $0 < m < p - 1$.

OUTPUT: Ciphertext (c1, c2).

1. Choose a random k in the range $1 < k < p-1$.
2. Compute $c1 = g^k \bmod p$
3. Compute $c2 = mB^k \bmod p$
4. Return ciphertext (c1, c2).
```

The ciphertext is the pair **(c1, c2),** which are both about ***p*** bits long. Neal Koblitz [38] describes **c2** as the message ***m*** "wearing a mask" and **c1** as a "clue" which can be used to remove the mask, but only by someone who knows the secret key ***b***.

Algorithm 2.2: ElGamal Decryption

```
INPUT: Domain parameters (p, q, g); recipient's private key b; ciphertext (c1, c2).

OUTPUT: Message representative, m.

1. Compute $m = c_1^{p-b-1}$ c2 mod p
2. Return m.
```

$c_1^{p-b-1} = (c_1^b)^{-1}$, since, for any $\mathbf{c} \in \mathbb{Z}_p^*$, $c^{p-b-1} = c^{-b} \cdot c^{p-1} = (c^b)^{-1} \cdot 1$, as $c^{p-1} = 1$.

2.4.2 Homomorphic Encryption based Schemes

There are many I-voting schemes hiding the contents of the ballot instead of hiding the identity of the voter. These cards are traceable and linked to the identity of the voter so that the possibility of verification can be achieved. But sometimes voter privacy can violate when calculating election results and the ballot is decrypted. The ballot is encrypted with a homomorphic encryption function to avoid this. A cryptographic function E is called (⊗, ⊕)-homomorphic if the following equation holds for any two plaintext T_1, T_2 [39]:

$$\mathrm{E}\ (T_1) \otimes \mathrm{E}\ (T_2) = \mathrm{E}\ (T_1 \oplus T_2) \qquad (1)$$

Usually, but not necessarily, the operator's ⊗ and ⊕ represent modular multiplication and addition, respectively. Encrypted ballots are multiplied together and the result is a result of the encrypted election. I.e. the result can be calculated without decrypting the ballot. But the addition restricts the votes by yes or no (1 for yes and 0 for no), while it is necessary to prove that the encrypted ballot paper actually includes such a ballot and not an arbitrarily large value [32]

The encrypted result can be distributed to several authorities so that it can only be decrypted when there are coalitions of a certain size because, if the system is under corrupt authority it will fail. One of the advantages of homomorphic encryption based schemes is that votes cannot be counted before they are cast. Indeed, counting steps are unpretentious. On the negative side, there is a worry about the use of a zero-knowledge proof in the I-voting schemes. Furthermore, these schemes are vulnerable to attacks like RSA blinding attack.

2.4.3 Mixnet based Schemes

Mixnets are based on public key cryptography, thus providing the non-tracking and hide identity. Mixnet is a multi-party communication protocol that takes input messages and arranges them randomly. None of these parties knows anything about the mixing algorithm, but only know that it has been mixed.

Mixnet uses anonymous channels to communicate where the sender's information is hidden, and no one even the recipient can find out or back to the sender's address. This is done through nodes that take the message and return it in random order. The sender sends the message and passes it through the node. This node switches the order of the contents of the message and sends it to the second node, etc. When the message reaches the last node, it sends it to the recipient. If one node works correctly, it is possible to make sure that the sender's identity is hidden [40]. There are two main categories of Mixnet [41]:

- *Decryption Mixnet:* The contract in this category contains a pair of public and private keys. The keys are distributed by the public key infrastructure. Let pub_i be the public key and $priv_i$ the private key for the *i*-th node, and r_i be a random padding. The encryption protocol works as follows if a voter sends a message *m* through five nodes:

  $$m_{enc}= E_{pub1}(r_1,\ E_{pub2}(r_2,\ E_{pub3}(r_3,\ E_{pub4}(r_4,\ E_{pub5}(r_5, m))))) \qquad (2)$$

  The message will be encrypted in layers, and in the correct order, the encrypted message will be passed, the message is decrypted through the nodes and the last node delivers the message. When using private keys, the protocol works the same way.

- *Re-encryption Mixnet:* It is also made up of several nodes and mixes messages and passes them. In this category, the message is re-encrypt in each node and sent to the next node instead of decrypting it when it is received from the previous node. For this, it can be guaranteed hide identity if only one node has its work properly. ElGamal is one example of a re-encryption Mixnet deployment.

The advantages of these schemes are that they do not require that the phases to be sequential and the use of mixing makes votes not tied to voters. There disadvantages are that their accommodation of large messages is inefficient and the input needs multiple encryptions.

2.4.4 Blind Signature based Schemes

Blind signature [42] is a type of digital signature and is used in many I-voting schemes, where the message is signed without disclosing its contents and thus achieve privacy. It will not be known to whom the voter voted because the authorities blindly signed the voter's vote.

Presently, blind key signature schemes exist with many public key protocols. One of these is the use of traditional RSA with the blind RSA Scheme. Let (N, e) be the public key of authority and (N, d) be his private key where d is the inverse of e mod $\phi(N)$. The voter need to select a random number r such that gcd (r, N) = 1, and sends the following to the authority [43]:

$$\mathrm{v}' = \mathrm{v} \cdot \mathrm{r}^{\mathrm{e}}\ mod\ N \qquad (3)$$

The random number r is used to hide the ballot v from the authority. Next, the authority signs the blinded ballot after verification and sends back S'.

$$S' = (v')^{d} = v^{d} \cdot (\mathrm{r}^{\mathrm{e}})^{d} = v^{d} \cdot \mathrm{r}\ mod\ N \qquad (4)$$

Then, the voter now can unblind it to get the true signature S since she/he knows r.

$$S = S' \cdot \mathrm{r}^{-1} = v^{d} \cdot \mathrm{r} \cdot \mathrm{r}^{-1} = v^{d}\ mod\ N \qquad (5)$$

To achieve more privacy anonymous channels can be used. The voter will submit a vote to Mixnet after signing it. Then, at the end of the ballot, Mixnet will process the encrypted votes. Votes are decrypted by the authorities and the voting results are then published [44]. Blind signature based schemes are simple and can be efficiently implemented. However, universal verifiability is difficult to carry out and the signer controls only the features associated with the public key.

2.5 I-Voting Schemes

In this section, some important I-voting schemes are reviewed with a summary of their analysis.

- VoteBox: VoteBox [45] is a system that provides auditability and robustness in the case of faulty initialization, manipulation or failure because it uses frequent logs and a distributed broadcast network. Vote decryption keys can be distributed to mutable unreliable parties. In order for the voter to ensure that his or her vote has been received as intended, the system uses an immediate challenge to vote. The system provides receipt-freeness. Privacy and coercion-resistance are also achieved because it is assumed that there is a voting booth.

- *Civitas:* Civitas [46] uses a digital signature to preserve the integrity, as well as uses a publicly viewable record service like a bulletin board. Through many cases of zero-knowledge proof (ZKP), protocol compliance is enforced. The voter creates false credentials by using his private key and running an algorithm and these cards are used to resist coercion. All votes adopted on false credentials are excluded. In this scheme, the resistance of coercion is achieved through false credentials, as well as verifiable through the bulletin boards. Figure 2.2 shows the Civitas architecture.

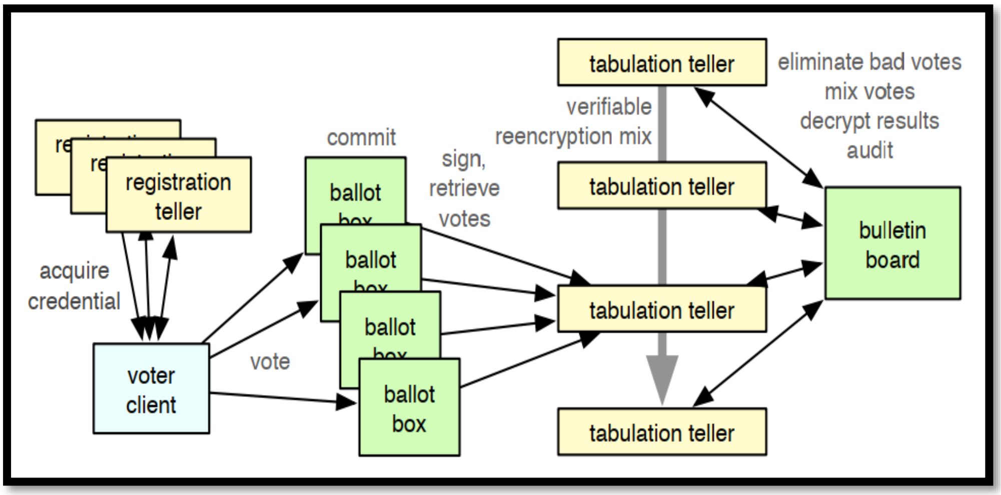


Figure 2.2: Civitas Architecture [49].

- *Prêt á Voter:* Prêt á Voter [47] uses a random candidate list to encode the voter's voice. Confidentiality is guaranteed by randomization. The voter ensures that his vote has been received after voting at the voting booth by giving him a receipt. By using encrypted receipt, voters can re-vote. Secret cryptographic keys are shared over multiple tellers. Voters check their votes after it has been posted on the bulletin board. All voter receipts are taken by tellers and decrypted, and then calculated after application of the mix network. This scheme offers the possibility of resisting coercion and privacy because it assumes the existence of the voting booth and also provides the receipt-freeness and end-to-end verifiability.

- *Multi-Authority E-voting System:* This scheme overcomes conspiracy and ensures privacy because elections are controlled by multiple parties [48]. It uses homomorphic encryption. Using the ElGamal Digital Signature Algorithm (DSA), the voter's ballot is signed and encrypted with the additive ElGamal scheme. Completeness and fairness are ensured. Voters are allowed to vote only once, but opponents can use these votes in their favor, and voters do not have a means of defense against coercion. This schema uses ZKP. The architecture of this system is shown in Figure 2.3.

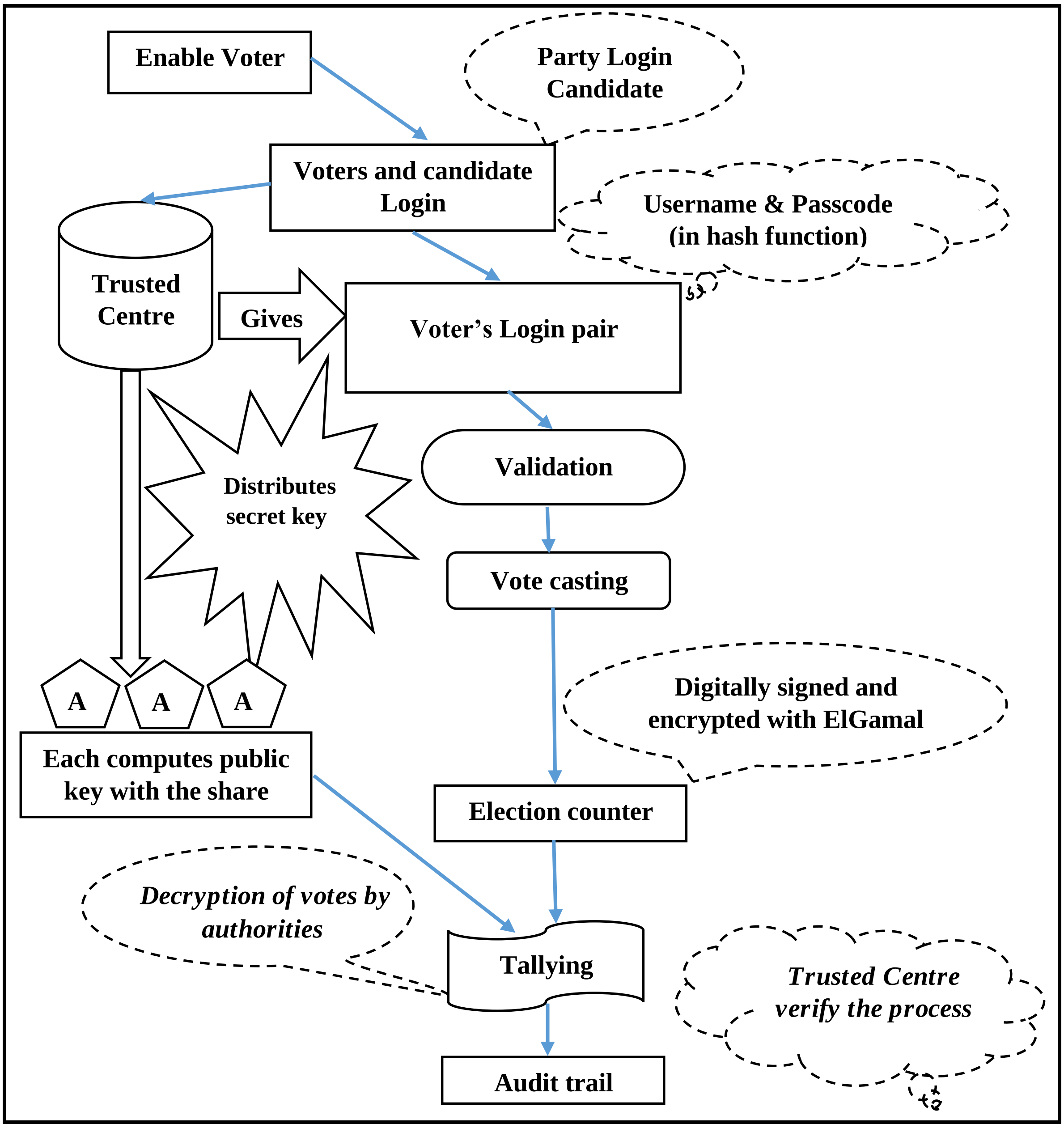

Enable Voter
Party Login Candidate
Voters and candidate Login
Username & Passcode (in hash function)
Trusted Centre
Gives
Voter's Login pair
Distributes secret key
Validation
Vote casting
A
A
A
Digitally signed and encrypted with ElGamal
Each computes public key with the share
Election counter
Decryption of votes by authorities
Tallying
Trusted Centre verify the process
Audit trail

Figure 2.3: Multi-Authority E-voting System architecture [48].

- *Secure Internet Voting Using DSA Public Keys:* By mixing the DSA public keys, this scheme hides the identity of the voter [49]. Credentials of votes consist of a simple DSA public keys. As a result of mixing, a list of anonymous keys that the voter can use to verify his signature is created, but these keys cannot be assigned to individual voters. Receipt-freeness and universal verifiability are provided in this scheme, but resistance to coercion is dubitable.

- *E-NOTE:* E-NOTE is a scheme that prevents the collusion of the authorities and also Leaks privacy through the use of two levels of security measures. E-NOTE is an improved version of NOTE (Name and vOte separaTed E-voting scheme) [50], in this scheme privacy concern can be wiped out while calculating votes by separating votes from names on the ballot. To eliminate fraud all voting transactions are Logined. Login is done by the authorities and a certificate is given to voters. Voters receive a ballot through this certificate. There is no correlation between the voter's certificate and his identity, so this scheme guarantees confidentiality. The electronic ballot made up of three sections. The votes are sent to vote counting committee (VCC) but can only decrypt one section of the voting data. Voters can be protected from enemies, also the privacy is achieved because evaluation is done without matching the vote with the voter. To achieve confidentiality each voter is given a watchdog by the election commission. Receipt-freeness is not carried out because the voter gets a receipt to track and review his vote. Also, coercion resistance is not achieved [51].

- *UVote:* The voters Login in advance and can vote more than once but give priority to voting from the polling station or the last vote. When voters vote from polling stations, this prevents coercion. Because the voter can vote again, this prevents the sale of votes. The voter creates the main account by his e-mail or his phone number to Login and also can create other accounts later. To resist coercion, the voter uses his or her main account. The account is verified by sending messages and alerts to the main account and can't be deleted. Each voter receives a unique identification number to access the election site and also receives a public and private key for encryption and decryption. In this scheme, universal and individual verification is achieved, also fairness is achieved because partial results are not announced. The voter is given a receipt and thus receipt-freeness is not achieved [52].

- *Cobra:* Cobra is a scheme where voters must Login by constructing and presenting encrypted credential. These credentials are added to the encrypted Bloom filter [53, 54] homomorphically. A voter chooses a password to Login from among several candidate passwords. The votes are encrypted and by using the password, the voter re-produce the credential. When the voter is subjected to coercion, a false password can be given to the imposter, so this scheme is coercion resistant. Anonymous channels are used to send votes. Authorities count the votes. Homomorphically, the credentials are added and decrypted, and the results are announced. Final results can be verified [55].

- *Zeus:* Zeus is a web-based system, where voters Login their private and public keys by visiting the website. The recorded key is compared with the hash value by the browser. This scheme is similar to Helios and uses the same encryption techniques. The mixing process is carried out by external authorities and the Zeus system. When the mixing process is completed, trustees are notified for decryption. Encryptions are collected by Zeus and the results are announced. External algorithms can be used to advertise results. In this scheme, universal verification is achieved because the results are published on the bulletin board. Because the voter gives an encrypted receipt, it does not achieve receipt-freeness [56].

Table 2.1 gives a comprehensive view of the requirements satisfied by the schemes mentioned above, together with their corresponding cryptographic technique.

Table 2.1: Comparison of voting schemes based on the requirements

Schemes/ Systems	Individual Verifiability	Universal Verifiability	Fairness	Coercion-resistance	Robustness	Receipt freeness	Cryptographic primitives
UVote	Y	NK	NK	Y	NK	N	Mixnets
Zeus	Y	Y	Y	N	Y	N	Mixnets, ZKP
Cobra	N	N	Y	Y	Y	Y	HE, EBF
DSA Public Keys	Y	Y	Y	Y	Y	NK	HE, Mixnets, ZPK
Civitas	Y	NK	Y	Y	Y	Y	Mixnets
Multi-Authority	NK	Y	Y	Y	Y	Y	HE, ElGamal DSA
E-NOTE	Y	Y	Y	NK	Y	N	RSA
VoteBox	Y	Y	NK	Y	Y	Y	HE, HC
Prêt á Voter	Y	Y	Y	Y	Y	Y	Mixnets

Y: Yes; N: No; NK: Not Known; HE: Homomorphic Encryption; EBF: Encrypted Bloom Filter; ZKP: Zero Knowledge Proof; HC: Hash Chaining;

2.6 Strengths and Weaknesses of I-Voting

On one hand, I-voting has many advantages. These include a potential for competent authorities, better accessibility, transparent results, and strong credentials. These can be described as follows:

- *Qualification of Authorities:* Usually, I-voting requires a small number of employees. I-voting system is monitored by specialized and competent people. It also requires fewer resources than traditional voting, which requires more resources, more voting staff, and security personnel to protect the voting process [57].
- *Accessibility:* I-voting is done from anywhere and from any device, so it provides voters with comfort and also increases voter turnout because, in the traditional vote, voters must go to polling stations that may be far

from them and difficult to reach, especially by people with special needs or the elderly [58].

- *Transparent Results:* I-voting allows voters to verify the election results after the results are announced and to ensure that their votes are counted correctly, using encryption techniques, thus making the elections transparent and visible to the voters, without revealing the identity of voters. On the contrary, in the traditional elections, voters have to accept the final result without verifying it or knowing how votes have been counted [59].
- *Strength of Credentials:* In I-voting, secure authentication systems are used, so only qualified people are entitled to vote for one time only, and this reduces the sale of votes. In traditional elections, credentials used for the purpose of voting are not sufficiently secure and can be easily falsified and used by impostors [60].

On the other hand, there are many weaknesses in the I-voting system, the existence of data on the Internet itself puts it at risk. It can be attacked from anywhere and at any time. Many believe that an online voting system is unsafe and cannot be useful, but if the system is built properly, weaknesses can be overcome. The attacks on an I-voting system can generally be categorized into two types:

- *Client-side attacks:* Client-side attacks include counterfeit sites used for election or harmful technical support. Voters can be intimidated and forced to vote for a particular person, their credentials may be stolen, and unscrupulous voters sometimes sell their votes for money. A large group of people do not care about the elections. People can be taught how to use websites to counter malicious web attacks, as well as using methods to prevent coercers from forcing voters to vote for them, but selling votes is extremely dangerous and difficult to prevent [61].
- *Server-side attacks:* The attack on the server is more dangerous since one problem can lead to a complete system crash. If the attacker breaks the voting system, he/she can manipulate the election and its results. This can be avoided by providing strong system protection as well as sound management. In fact, there is nothing to guarantee the security of I-voting, but it can be more efficient than traditional voting since the latter

is not safe either because ballot boxes are placed in places that are not safe enough and can easily be accessed, stolen or burned [23].

2.7 Helios Voting System

Helios [62] is an I-voting system released in 2008 by Ben Adida. The initial version of Helios was a simple verifiable voting scheme by Benaloh [63]. Which was inspired by a protocol by Sako and Kilian [64]. In this release, the characteristics of the open-audit were guaranteed, and Helios was a single trustee of the voting confidentiality. Helios generates a pair of keys for the encryption process; the public key is used to encrypt votes; the Helios server mixes all the votes in order to separate the voters' identity from their voting; the votes are then decrypted using the private key. This release can be summarized as sacrificing privacy in return for strong verification guarantees.

In the next version of Helios [65], the first end-to-end verification was conducted in legally binding elections of several thousand voters in 2009. The main modification in this version is the abandonment of the mixing approach and the use of homomorphic approach that is more efficient, simpler and inspired by the Schoenmakers, Gennaro and Cramer protocol [66]. In this approach, all encrypted votes are collected and then decrypted. The second major modification of this version is the use of distributed encryption, thus enhancing voting privacy so that no device or entity at any time be in touch with sufficient keying material to decrypt individual votes. This resulted in the removal of the need to manipulate the decryption key by Helios, thus reducing the consequences of server compromise. Other features have been added, such as the use of aliases rather than voter IDs on the bulletin board [60].

Since 2009, many enhancements have been added to the Helios system, such as improved auditing features, enhanced interfaces, new authentication methods and increased compatibility by taking advantage of browser design developments. Despite the changes that occurred in the Helios system, but had remained indifferent to the problem of protection from coercion. Therefore, the Helios system is not an appropriate option for high-risk elections, where coercion becomes an effective option for harmful actors [67].

2.7.1 Voting Procedure

In this subsection, the steps and method of voting followed in the Helios system are listed as below.(See Figure 2.4) [11, 58, 68]:

1. An e-mail is sent to the voter containing the voter-ID, the assigned password, an election fingerprint, and, the URL of the election page.
2. The voter connects to the election web page through the browser. A ballot preparation system (BPS) operates as a service on the browser. The BPS permits the voter to select their choice among the valid votes set.
3. Then, the BPS encrypts the answers together with some arbitrary data.
4. The voter can now select between audits the ballot or submit.
    - If she/he selects audit: key and the ciphertext are given to the voter, who can now verify if this agrees with the vote she/he wanted to cast. If everything is ok, the BPS proceeds and re-encrypts the options with new arbitrary data, again allowing the voter to select audit or submit.
    - If she/he selects submit, all but ciphertext are enduringly removed.
5. Authentication is requested from the voter, if she/he passes, the encrypted vote is recorded as the vote of the voter.
6. On the bulletin board, voter's encrypted vote is displayed. All cast votes are also shown. Every vote is either associated with the identification number or the voter's name. Anyone who has voted can see her/his encrypted voice on the bulletin board. The voter can check whether her/his vote exists or if it was indeed her/his vote.
7. After the election ends, administrators of election work together to calculate the total number of encrypted votes. This is done through the

use of homomorphic encryption and secure multi-party computation.

8. The election results are announced. By using the bulletin board, anyone can verify that her/his vote has been taken into account and that adding votes has been done correctly.

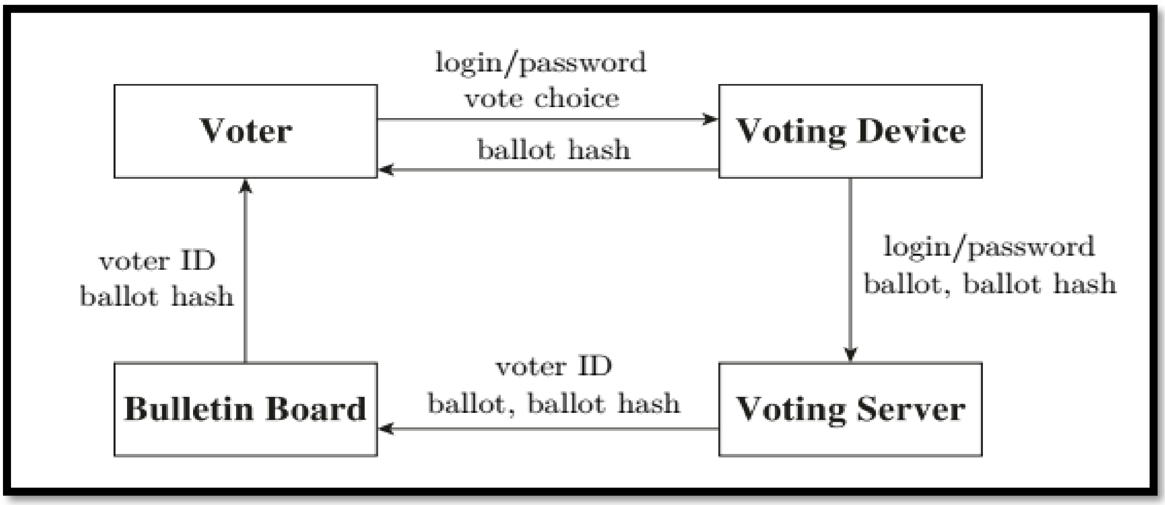


Figure 2.4: Helios voting protocol [45].

2.7.2 Strengths and Weaknesses of Helios

The Helios voting system has many strengths that made it one of the best and most popular electronic voting programs, some of which can be mentioned as follows:

1. The Helios system is fully open source and allows end-to-end verification [11].
2. Using Helios does not require the existence of a physical mail address, any custom hardware, or the installation of any specific program [67].
3. Trusting in the server is not required because of the nature of the Helios system, even if system administrators are completely malicious, the voting process still fully verifiable [58].
4. Encryption is done using JavaScript, so the user can even disconnect the computer from the Internet after downloading all credentials, making its options, encrypting the vote, and reconnecting the Internet to the vote. Therefore, the attacks which need access to the Internet, are useless [35].
5. All encrypted votes are shown on the bulletin board. Even during

counting, the votes remain encrypted, so the Helios system achieves the ballot secrecy [69].

6. The bulletin board permits only one vote to link with an identity [70].

Despite the strengths of the Helios system, it also has many weaknesses, including:

1. Helios does little to save voters from coercion. The coercer can dictate his orders to the voter throughout the election process and verify that the voter has complied with his orders [67].
2. Helios does not do much to counteract the threat of a web browser or client-side operating system compromise. A virus can change a user's secret password and cover all checks made on the same computer to hide its paths [65].
3. Helios can be accessed over the Internet, making it susceptible to attacks such as denial of service attacks [35].
4. Anyone can know who has voted whether the real name or the nickname and that's because the bulletin board is public [71].
5. In the future, if the encryption algorithms used in Helios broken, the attacker will be able to decrypt all votes [18].
6. Helios only aims to achieve the privacy of the ballot and clearly, ignores the concepts of confidentiality in favor of efficiency [72].
7. The system can cast votes for non-existing voters or voters that have not cast their ballots because the system cannot fully amend or remove the votes, and voters who have not voted will have to make sure that no vote has been Logined by their names [58].

2.8 Public Key Infrastructure

Public Key Infrastructure (PKI) is a set of encryption technologies, services, and software through which organizations can maintain the security of their business transactions and their connections on the Internet. PKI provides a secure connection to users that are widely distributed and that do not know each other through the use of a common certificate commonly known as a chain of trust. Reliability, non-repudiation, and integrity of data and confidentiality are services provided by PKI to enterprises through the use of digital certificates, which are considered a digital passport containing the user name and some other data according to regulatory policies [73]. The digital signature created by public key cryptography [74, 75] can be verified by the digital certificate.

The PKI consists of the certification authority (CA), the primary part that creates certificates for users and also manages and exports public keys for data encryption as well as secure credentials. The PKI components vary according to the system used, but often consist of the following [76]:

- End Entities: It is the user or anything that needs a digital certificate to identify for any reason such as computers. The end entity uses the certificate provided by the CA in the possible PKI applications.
- Certification Authority (CA): It is an authority that establishes certificates for the end entity after the RA has reviewed their application for certification. It is a trusted authority that creates and manages public keys used to encrypt messages. The CA distributes the certificates to the end entity as well as cancels the certificate if it expires or the end entity request to cancel it or any other reason.
- Login Authorities (RA): It is the authority that performs the administrative tasks in PKI and it is optional component. RA verifies the request of the end entity of the certificate and decides if it is eligible to issue a certificate to it or not.
- Certificate Policy (CP): It is a set of guidelines and rules established by the CA to define the mechanism of work as well as determine who is entitled to obtain a digital certificate and where this certificate can be applied and determines the purpose of the PKI and the security services it supports.
- Certificate Repositories (CR): It is a system that stores digital certificates and it is an optional component in PKI. The entities that deal with are signed by the CA so it does not have to be trusted. It also stores Certificate Revocation Lists (CRL).

2.8.1 Public Key Certificates

A public key certificate is a digital certificate signed by the CA issued to the final entity. It is used to prove ownership of the public key of the final entity. There are many types of digital certificates approved such as Pretty Good Privacy (PGP) Certificates, X.509 Public Key Certificates, and Simple Public Key Certificates (SPKC). But here we relied on Version 3 of X.509 public key certificates because of its wide use in the PKI systems. As shown in Figure 2.5, the certificate consists of the following components [41]:

- Version: It distinguishes among consecutive versions of the certificate format.
- Serial number: A unique number used within the CA systems to identify the certificate.
- Signature algorithm identifier: It is defines the algorithm that used to sign the certificate with the related parameters.
- Issuer name: It is used to identify the entity that checked the information and signed the certificate.
- Period of validity: It consists of two fields not before and not after, used to determine the validity date of the certificate.
- Subject name: It is the name of the certificate holder who has the private key corresponding to the public key in this certificate.
- Subject's public-key information: The public key of the certificate holder as well as an algorithm identifier to which this key will be used.
- Issuer unique identifier: A unique number that is used to identify the issuing CA of the certificate in case the X.500 name has been reused for various entities, which is an optional field.
- Subject unique identifier: A unique number that is used to identify the issuing subject in case the X.500 name has been reused for various

entities, which is an optional field.

- Extensions: A collection of extensions that were included in version 3.
- Signature: It is the signature of the issuing CA for the certificate. It contains a hash code for other fields that are encrypted by using the CA private key.

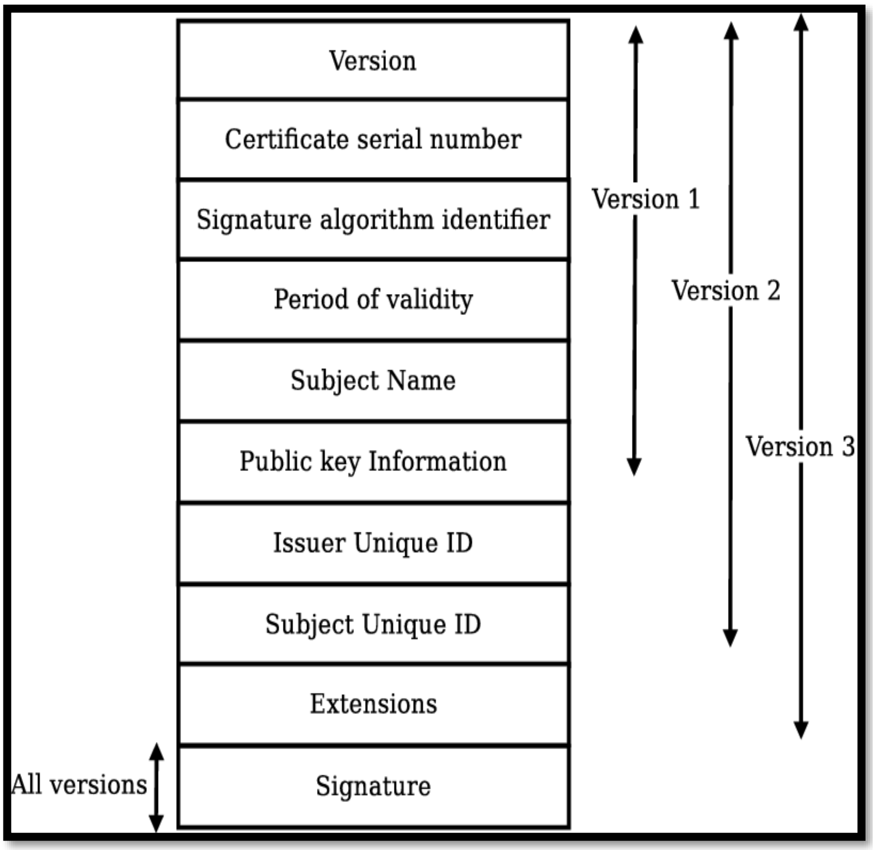


Figure 2.5: X.509 Certificate V3 [77].

2.8.2 Digital Signature

The digital signature is the most important cryptographic process in the PKI systems. The digital signature provides protection if the parties exchange the digital documents between them. The recipient then can ensure that this document has not been manipulated or altered, and makes sure that the document was actually sent by the sender. This is done by creating a data element attached to the document that is uniquely linked to the sender and when the document is received by the recipient, some steps can be taken to ensure that the signature matches the sender [78].

If the digital signatures are not used, the attacker can simply intercept the document sent by the sender and change it to another document and send it to the recipient without being detected, as shown in Figure 2.6.

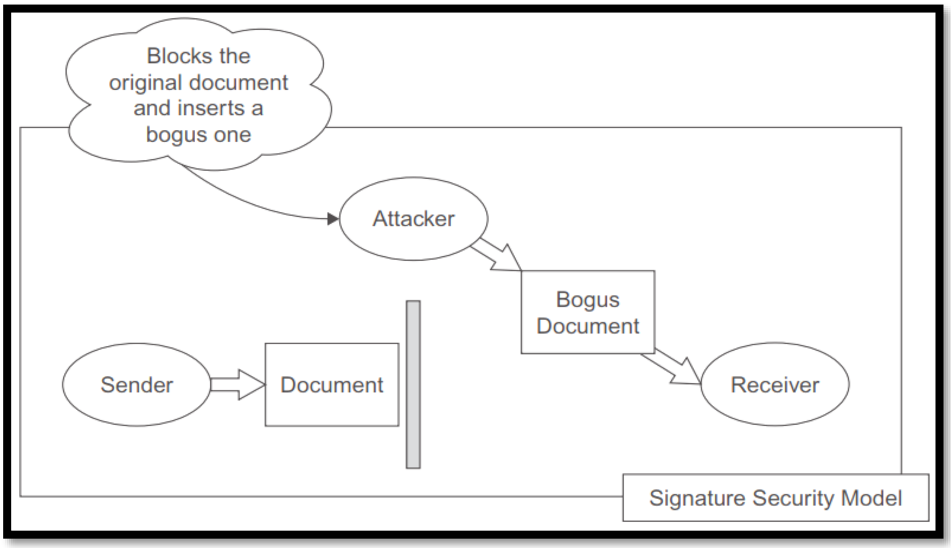


Figure 2.6: Block diagram of altering an unsigned document [78].

However, if the signature is attached to the document and changed by the attacker with another document, the recipient can know that the document is false and not sent by the sender, as shown in Figure 2.7. Secure digital signatures can be created by using suitable cryptographic algorithms.

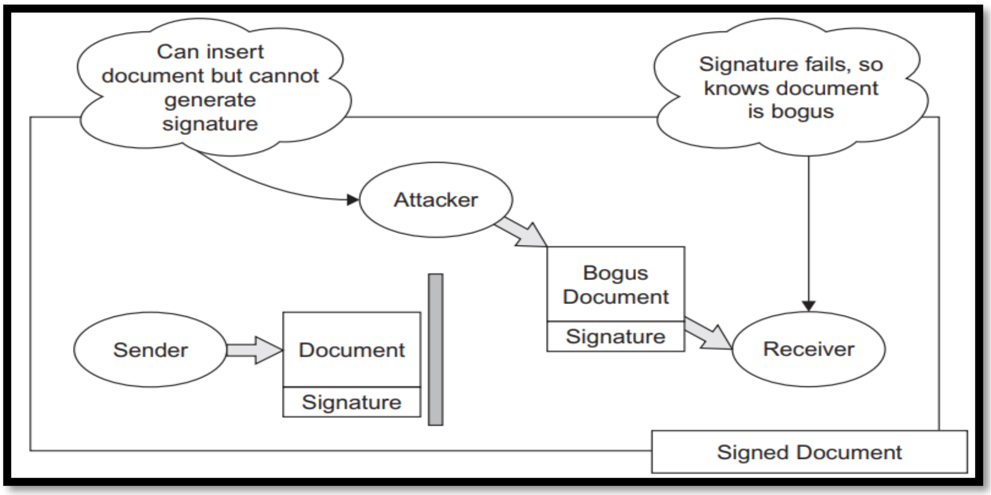

Can insert document but cannot generate signature
Signature fails, so knows document is bogus
Attacker
Bogus Document
Signature
Sender
Document
Signature
Receiver
Signed Document

Figure 2.7: Block diagram showing prevention of an alteration attack via digital signature [78].

A. RSA Signature Scheme

The RSA signature system is based on RSA encryption that developed by Rivest, Shamir and Adleman in 1978 at the Massachusetts Institute of Technology. The strength of security in RSA is that it is difficult to analyse large numbers. RSA signature is one of the most widely used digital signature systems in practice [36].

Algorithm 2.3: Generate an RSA key pair.

INPUT: Required modulus bit length, ***k***.

OUTPUT: An RSA key pair **((N, e), d)** where **N** is the modulus, the product of two primes **(N = pq)** not exceeding ***k*** bits in length; ***e*** is the public exponent, a number less than and coprime to **(p − 1) (q − 1)**; and **d** is the private exponent such that ***e*d ≡ 1 mod (p − 1) (q − 1).**

```
Select a value of $e$
repeat
    $p \leftarrow$ genprime $(k/2)$
until $(p \bmod e) \neq 1$
repeat
    $q \leftarrow$ genprime $(k - k/2)$
until $(q \bmod e) \neq 1$
$N \leftarrow pq$
$L \leftarrow (p - 1)(q - 1)$
$d \leftarrow$ modinv $(e, L)$
return $(N, e, d)$
```

The function genprime (b) returns a prime of exactly **b** bits, with the ***b***th bit set to 1. Note that the operation ***k/2*** is *integer* division giving the integer quotient with no fraction.

Encryption

Sender **A** does the following:-

1. Obtains the recipient B's public key **(n, *e*).**
2. Represents the plaintext message as a positive integer **m** with $\mathbf{1 < m < n}$.
3. Computes the ciphertext $\mathbf{c = m^e \bmod n}$.
4. Sends the ciphertext **c** to **B**.

Decryption

Recipient **B** does the following:-

1. Uses his private key **(n, d)** to compute $\mathbf{m = c^d \bmod n}$.
2. Extracts the plaintext from the message representative **m.**

Digital signing

Sender **A** does the following:-

1. Creates a *message digest* of the information to be sent.
2. Represents this digest as an integer **m** between 1 and $\mathbf{n - 1}$.
3. Uses her *private* key **(n, d)** to compute the signature $\mathbf{s = m^d \bmod n}$.
4. Sends this signature **s** to the recipient, **B**.

Signature verification

Recipient **B** does the following:-

1. Uses sender **A**'s public key **(n, e)** to compute integer $\mathbf{v = s^e \bmod n}$.
2. Extracts the message digest **H** from this integer.
3. Independently computes the message digest $\mathbf{H'}$ of the information that has been signed.
4. If both message digests are identical, i.e. $\mathbf{H = H'}$, the signature is valid.

In RSA signature, public and private key roles are exchanged against RSA encryption. The sender applies the private key in the RSA signature on the message, while the public key is applied in RSA encryption. On the other hand, the receiver implements the public key on the message in the RSA signature for verification and applies the private key in the RSA encryption [79].

B. DSA Standard

The National Institute of Standards and Technology (NIST) has proposed the Digital Signature Algorithm (DSA) which is Federal Information Processing Standard (FIPS 186). DSA takes advantage of the Secure Hash Algorithm (SHA). One of its main advantages and excel on the ElGamal signature scheme is that the length of the signature is 320 bits, which can expose the ElGamal to the threat of penetration but cannot be applied to DSA [36].

It uses the same Diffie-Hellman domain parameters **(p, q, g)** and private/public key pair **(a, $A = g^a \bmod p$)** for a signing party **A**.

Algorithm 2.4: DSA Signature Generation

```
INPUT: Domain parameters (p, q, g); signer's private key a; message-to-be-signed, M; a secure hash function Hash() with output of length |q|.
OUTPUT: Signature (r, s).
  1. Choose a random $k$ in the range $[1, q - 1]$.
  2. Compute $X = g^k \bmod p$ and $r = X \bmod q$. If $r = 0$ then go to step 1.
  3. Compute $k^{-1} \bmod q$.
  4. Compute $h = \mathrm{Hash}(M)$ interpreted as an integer in the range $0 \le h < q$.
  5. Compute $s = k^{-1}(h + ar) \bmod q$. If $s=0$ then go to step 1.
  6. Return (r, s).
```

Algorithm 2.5: DSA Signature Verification

```
INPUT: Domain parameters (p, q, g); signer's public key A; signed-message, M; a secure hash function Hash() with output of length |q|; signature (r, s) to be verified.
OUTPUT: "Accept" or "Reject".
  1. Verify that r and s are in the range $[1, q-1]$. If not then return "Reject" and stop.
  2. Compute $w = s^{-1} \bmod q$.
  3. Compute $h = \mathrm{Hash}(M)$ interpreted as an integer in the range $0 \le h < q$.
  4. Compute $u_1 = hw \bmod q$ and $u_2 = rw \bmod q$.
  5. Compute $X = g^{u_1} A^{u_2} \bmod p$ and $v = X \bmod q$.
  6. If $v = r$ then return "Accept" otherwise return "Reject".
```

Chapter Three: The Proposed I-Voting System

Chapter Three

The Proposed I-Voting System

3.1 Introduction

In this chapter, the proposed Helios-based I-voting system is presented. It represents several improvements to the original Helios system. The proposed system will be explained in general with an architecture covering all the steps of the system. Then, there is an explanation of the design and implementation of the proposed system.

Three main improvements have been added. Firstly, on the security and scalability side, a certification authority has been added that creates certificates for voters that contain public and private keys used in the encryption and digital signature process. A digital signature has also been added to the vote, where the voter can sign her/his vote using either RSA or DSA. Secondly, there is an improvement that aims to reduce coercion. Each voter has four accounts she/he can use them to vote. One real account and three fake accounts used by the voter in case of coercion. Finally, improvements to the interface where the Arabic language has been added so that Arabs can use the system more easily. Also, some interfaces have been enhanced where unimportant commands were removed and a concept explanation was added for some steps.

3.2 System Architecture

The proposed system includes improvements to the Helios voting system in three main areas: Security and scalability, anti-coercion, and usability. The suggestion of these improvements came after studying the Helios system and showing its weaknesses that make it less used by voters. These improvements make Helios safer and more widely used.

Figure 3.1 is a block diagram that illustrates the architecture of the proposed system. In the figure, the voting steps can be observed in the original Helios system as well as the proposed improvements to the system, which all represent the proposed system.

The voting steps in the original Helios system are:

1. Login to the system.

2. Click on "Vote in this Election" link and go to the "Voting Booth" page.
3. Read instructions on how to vote and then answer election questions.
4. Press the "Proceed" button and go to the next page.
5. Review voting, and also there are three options.
   a) Click on the "edit responses" button and return to the "Voting Booth" page.
   b) Press the "Submit" button and go to the "Submit Box" page.
      - If you press the "Cancel" button you will be taken to the Helios homepage.
      - If you press the "Cast this ballot" button, you will be taken to the confirmation page and then to the Helios homepage.
   c) Click "Verify Encryption" button and go to the "Helios verifier" page.
      - If you click on the "Ballot Verifier" link, you will be taken to a verification page, the voting will be verified and then back to the Helios homepage.
      - If the "back to voting" button is clicked, you will be returned to the "Voting Booth".

The steps added to the Helios system are:

1. Login to the system by:
   a) Google b) Facebook c) Yahoo d)LinkedIn
2. Press the "Arabic" button and convert the language to Arabic.
3. Click the "Certification Authority" button and go to the Certification Authority page.
   a) Press the "Create Certificate" button and then the voter certificate is automatically generated.
   b) Click on the "Download Certificate" button and the voter certificate will be downloaded to the voter device.
   c) Click on the "Download Public Key" button and then the Helios Public Key is downloaded to the voter device
   d) Click on the button "Verify Helios" and then go to a page to verify the validity of Helios certificate.
4. Sign Vote (RSA or DSA) using keys in certificate.
5. Encrypt Vote using keys in certificate

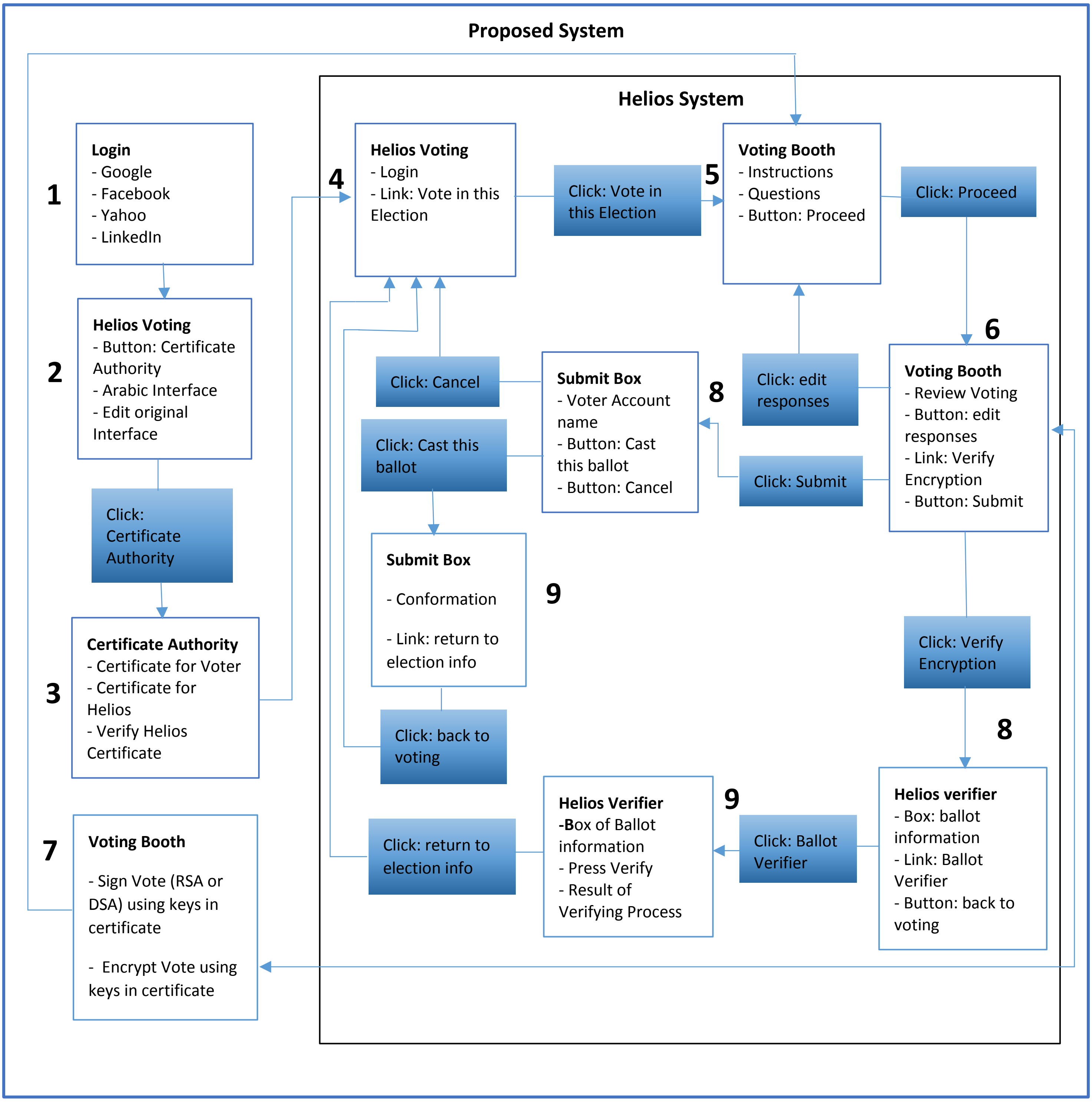


Figure 3.1: Architecture of the proposed system.

Algorithm 3.1 present steps of the proposed system

Algorithm 3.1: Steps of the proposed system

```
INPUT: Voter’s login

OUTPUT: Final result

    1. Voter login to the system
    2. If (real account)
        a) Generate certificate
           $P_K$ = Public key
           $Pr_K$ = Private key
        b) Vote for a candidate
           V = Vote
        c) Encrypt = ($P_K$ , V)
           Sign = ($Pr_K$ , V)
        d) Choose either Audit or Submit
        e) If (Audit)
           Verify (V)
           Return to step c
        f) If (Submit)
           $DB_{main} = DB_{main} + V$
           Return ($DB_{main}$)
    3. If (fake account)
        a) Repeat steps from (a to e)
        b) If (Submit)
           $DB_{Sec} = DB_{Sec} + V$
           Return ($DB_{Sec}$)
    4. FinalResult = $DB_{main}$
    5. Return (FinalaResult)
```

3.3 Design Aspects of the Proposed System

In this section, aspects of the proposed system design will be explained which include security and scalability, anti-coercion and interface. There are two sides of proposed system: the server-side and the client-side. On the client side the voting process is conducted and the voting is encrypted. Voters can vote even if they are not connected to the Internet, thereby reducing the chances of attack. After the vote, voters can reconnect to the Internet and send the vote to the server. On the server-side, decryption, counting, and announcing results are performed. The proposed system is designed to include both server and client sides.

3.3.1 Security and Scalability

At first, concerning the security and scalability aspects of I-voting, Helios is integrated with a certification authority to create and certify encryption keys. The public keys are created and linked to the voter. These keys are used in digital signature and vote encryption. The addition of the certification authority to produce necessary keys for the digital signature and encryption will significantly increase system security by enabling sophisticated security services for system and data protection. Indeed, the scalability of the I-voting system can be increased to consider relatively more distributed environment compared to previous typical deployments of Helios.

The CA issues a public key certificate (one-time use key) to a device in the network that can authenticate itself to the CA server. The voter generates the keys and uses them automatically. Certificates are used once a new session is negotiated for voting, so pre-shared keys are not created or stored, enhancing security and reducing administration. This automated feature of secure key distribution also highly contribute to increasing the scalability of the system by facilitating its deployment in more distributed and large scale environments. In this respect, public key certificates can be the safest and most practical forms of electronic data identification and protection in distributed environments. Figure 3.2 illustrates the general description of integrating the certification authority in the proposed system.

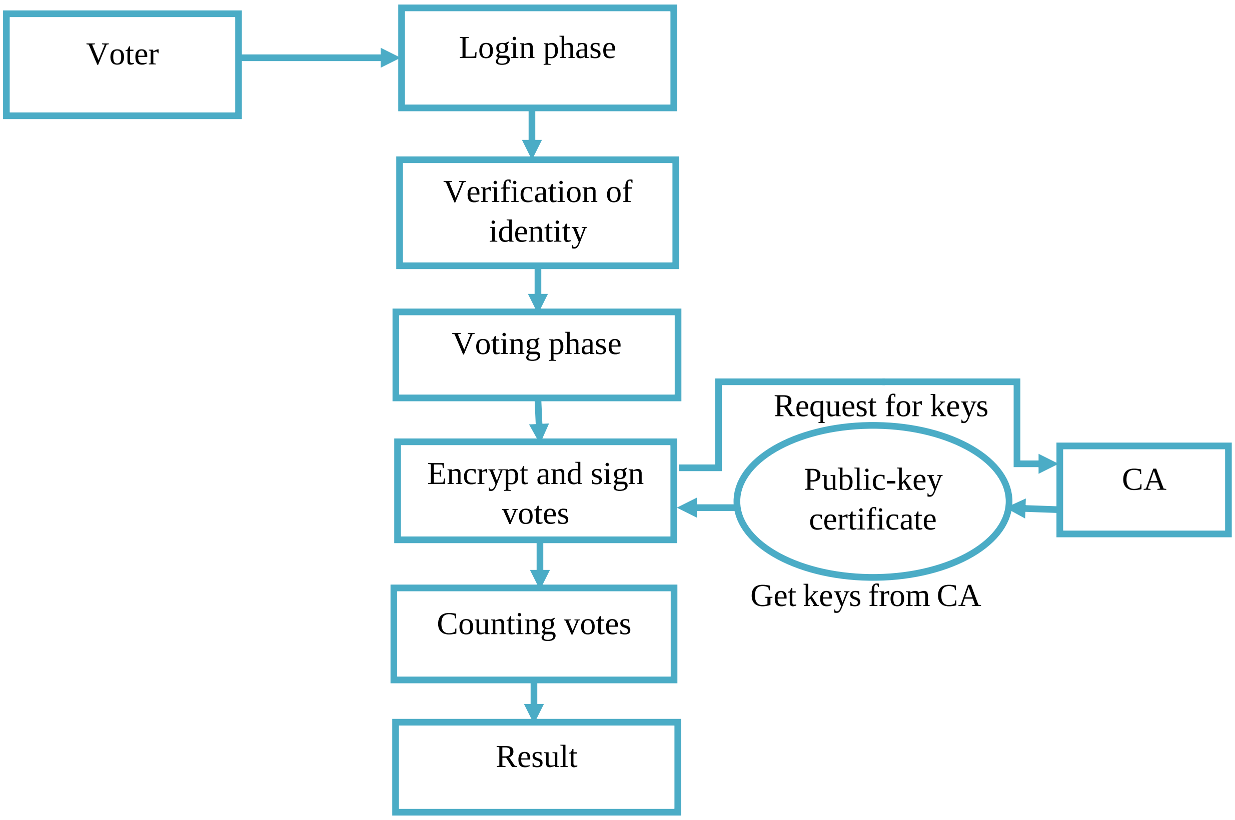


Figure 3.2: A block diagram showing the integration of certificate authority in the proposed system.

The aim of this improvement is to design a more secure and scalable Internet voting system. Emphasis has been placed on aspects of safety because it is the most important of our time. If the voting system is not secure, any attack will cause it to collapse. Because the voting process is sensitive and even a small change will greatly affect the outcome. Adding certification authority to the voting system increases security because it is a trusted entity that creates public and private keys. Public and private keys are used for encryption and digital signature, so the process of creating them by a trusted entity is necessary. This addition also increases the voters' confidence in the system and thus increases the turnout and its use by them.

3.3.2 Anti-coercion

Concerning anti-coercion property, the proposed system enables the voter to create multiple accounts during the Login stage. These multiple accounts are created for each voter where the voter has a real account (based on her choice) used in the elections and other (one or more) fake accounts used by the voter when he subjected to coercion by the attacker. In later phases, when the voter enters the system, if she/he Logins with her real account, she/he able to vote in the elections and the vote placed on the main database and thus calculated. In case the voter is subjected to coercion, she/he can use one of her fake accounts to vote as the coercer wants. In this case, the vote (unnoticeably) placed in the secondary database, and thus her vote will not count within the final result.

The coercer cannot distinguish which account is real or fake because the voter can any time choose which account to be real and the rest are fake ones. Using any fake account cause the vote to not be counted among the final votes. When voting through the fake account, these votes stored in a different database than those that done by the real account. Thus, when counting, only votes that are in the main database are counted. Voters can vote using their real account at any time and thus reduce the risk of coercion suffered by Helios. This is illustrated in Figure 3.3.

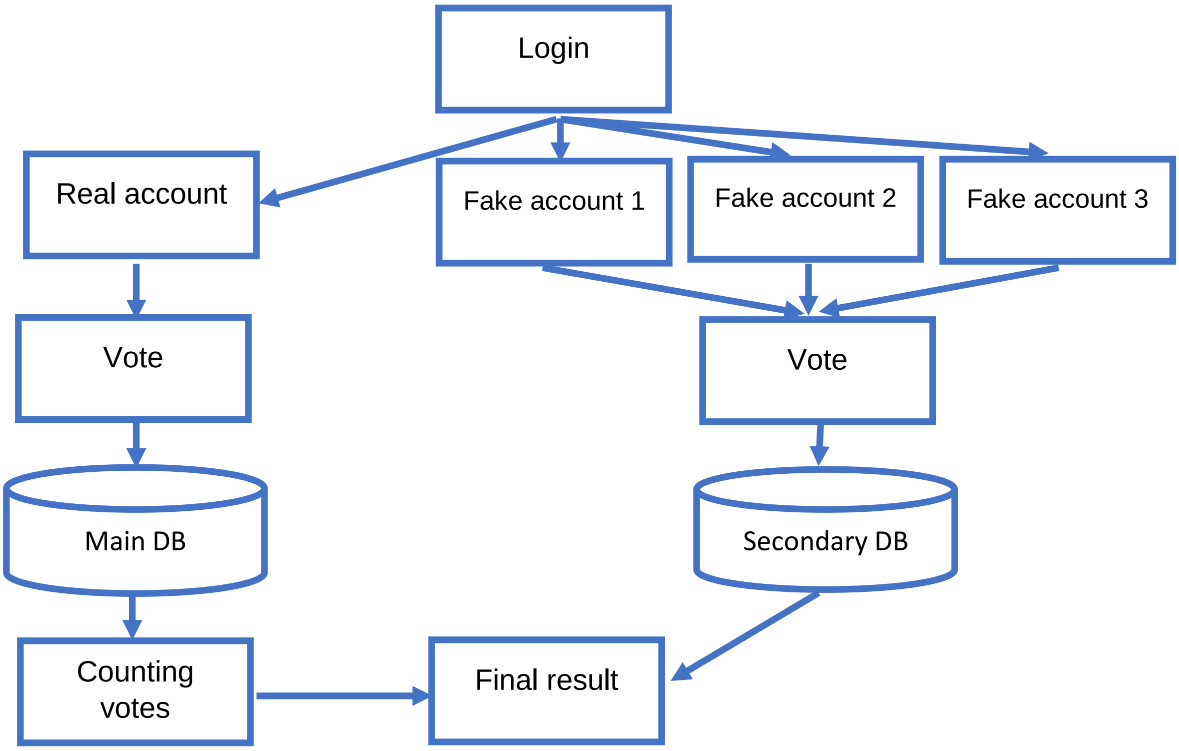


Figure 3.3: Block diagram shows adding multi-accounts to propose system.

The main goal of adding more than one account per voter is to alleviate coercion. Eliminating coercion or at least alleviating it is essential in any Internet voting system. It is also no less dangerous than cyberattacks because it causes voters to choose or vote for a candidate they don't want. Giving each voter more than one fake account increases the chance that the coercer will not know which real account the voter has. The secondary goal is to increase and diversify voter Login methods. Not all voters have accounts in Google or Yahoo, so a variety of Login methods will improve participation rates in Internet voting.

3.3.3 Interface

Concerning the usability issue, The Helios interface is improved as the interface is difficult to understand by people who do not have a broad knowledge of technology. There are many options that they do not understand the reason of their existence or what they should choose. Every step in the voting needs to be explained more and why the voter is doing it. So in the proposed system, this issue needs to be carefully tackled in order to increase usability and comfort.

The addition of Arabic to the interface makes the system more used by people that do not know English. That's where many voters cannot read English words or feel uncomfortable when dealing with commands in that language. Also, work to improve the interface and reduce unnecessary commands and add clarifications for each step makes the system better. The reason for this is that when some voters do not understand how to vote, they will surrender and log out of the system, thus reducing turnout.

3.4 System Requirements

The proposed system was implemented using Django, which is a Python-based open-source and free web framework, which follows model-template-view (MTV) architectonic pattern. Django's primary goal is to facilitate the creation of complex, database-driven websites. The framework emphasizes "pluggability" and reusability of components, low coupling, rapid development, less code, and the principle of "don't repeat yourself".

Also some other requirements are needed to implement the proposed system:

- A computer that is connected to the Internet for the purpose of completing the Login process through various accounts.
- Prompt command to run the server.
- Ubuntu operating system which is an open-source and free Linux distribution based on Debian (The reason for using Ubuntu OS is that Helios only works on this OS).

3.5 Implementation of Voting Process

The Certification Authority (CA) is a trusted entity issuing digital certificates and private-public key pairs. A digital certificate is an essential part of a secure connection. Without certification authorities, you will have a large and uncertain set of certificates, many of them are likely to be applicable, but some can also be used maliciously because there is no way to verify ownership. For the average person, this means someone can fundamentally misrepresent a key and then steal encrypted data.

Therefore, as a result, the CAs are in place to assist with authentication. Authentication simply means that you own a certain certificate, therefore, the key to that certificate. The CAs are trusted for some reason, they heavily have invested in their own infrastructure and have powerful operations in place that are capable of verifying identity and digital certification correctly.

Encryption is the process of changing the information in a way that makes it unreadable by anyone other than those with special knowledge (referred to as “key”) that allow them to change information to their original readable form. It is important because it allows secure protection of data that no other person is intended to access. Used by governments to secure confidential information, used by companies to protect corporate secrets, and used by many individuals to protect personal information to protect against things such as identity theft.

A digital signature is a digital code authenticated by a public key that is listed and enclosed with an electronic document sent to verify the content and the identity of the sender. It is the technique of legal approval for the validity or merits of a message or documents. A digital signature is equally valid and legal for a certified or handwritten signature. The advantages of digital signature are time-saving, cost-effective, fast signing of multiple PDF files, digitally signed documents secure and safe, easy to use, reliable and legally compatible.

In the proposed system, there is a certification authority that creates certificates for voters and issues public and private keys to them. This helps to prove their ownership of these keys and they are authorized to vote in the elections. The CA also creates a certificate for Helios. The keys are used in the encryption process as well as the digital signature. Algorithm 3.2 shows the voting process in proposed system.

Algorithm 3.2: The voting process

```
INPUT: Voter’s login
OUTPUT: Final result

1. Voter login to the system
2. Generate certificate
       $P_K$ = Public key
       $Pr_K$ = Private key
3. Vote for a candidate
       V = Vote
4. Encrypt = ($P_K$ , V)
   Sign = ($Pr_K$ , V)
5. FinalResult = FinalResult + V
6. Return (FinalaResult)
```

3.6 Implement Multi-Accounts Feature

At first, the voter logs into the system using the available Login methods. The voter is then asked if she wants to make this account her real account. If the voter chooses "yes", her vote will be counted among the final votes. If a voter chooses "no", her vote will not be counted. It is possible to know that these accounts belong to one person by taking the IP of the voter. Voters can change their real account at any time. Algorithm 3.3 shows voting using multi-accounts.

```
Algorithm 3.3: Voting using multi-accounts

INPUT: Voter’s login
OUTPUT: Final result

1. Voter login to the system
2. If (real account)
   a) Vote for a candidate
      V = Vote
   b) $DB_{main} = DB_{main} + V$
      Return ($DB_{main}$)
3. If (fake account)
   a) Vote for a candidate
      V = Vote
   b) $DB_{Sec} = DB_{Sec} + V$
      Return ($DB_{Sec}$)
4. FinalResult = $DB_{main}$
5. Return (FinalaResult)
```

3.7 Enhancement the Interface

Django uses the MTV pattern to design software. It is a collection of three elements Model Template and View. The model helps in dealing with the database. It's the data access layer that handles data. The template is a presentation layer that completely manages the UI portion. The view is used to implement business logic and interact with the model to carry data and render the template.

The user asks for a resource to Django, Django acts as a controller and verifies the resource available in the URL. If a URL is set, the view that interacts with the model and template is called, where a template is rendered. Django responds to the user and sends the template as a response.

Figure 3.7 represents the general framework of Helios and illustrates its software parts in Django. To improve the Helios interface, work was done on the part of the template. Templates that appear to users that contain commands and words have been modified. Some of these unnecessary commands and words have been removed and explanatory objects have been added. As for adding Arabic to the system, the commands in Python were used to translate the interface. Also, the main button that appears on all pages to change the language from English to Arabic and vice versa has been added.

Chapter Four: Results and Discussion

Chapter Four

Results and Discussion

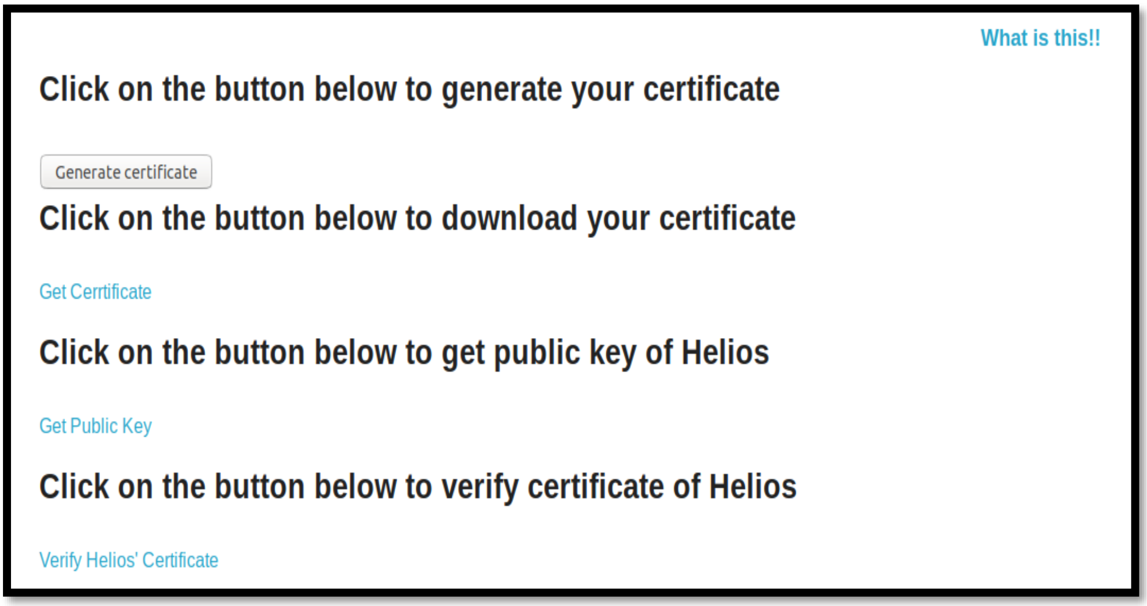
4.1. Introduction

In this chapter, the results of the proposed I-voting system are presented and discussed. The interfaces of the certification authority page and the voting page are initially explained. Indeed, the performance of the proposed system is measured and the security of the system is estimated. Next, the aspect of multiple accounts is tested. Finally, the interfaces of the proposed system are presented along with and the questionnaire conducted on the ease of use of the proposed system and its comparison with Helios. In summary, the results cover three aspects: security and performance analysis, multi-account feature and improved interfaces.

4.2 Security and Performance Analysis

Security is the most important characteristic of voting systems. Lack of strong security means that the system will not be usable. In this section, the security and performance analysis of the proposed I-voting system is conducted. Initially, the interfaces that are shown to the voter and that are specific to security are displayed.

Figure 4.1 represents the interface of the certification authority that appears to the voter. The voter can create her/his certificate as well as the possibility to download her/his certificate and Helios certificate and also check the Helios certificate. When the "Generate Certificate" button is pressed, the system automatically generates a voter certificate that contains the voter's keys. These keys are used during the voting process. The "Get Certificate" and "Get Public Key" buttons allow the voter to download his certificate and Helios public key and save it to her/his device in a safe place. Finally, the button "Verify Helios", which when pressed the voter redirects to a special page containing the certificate of Helios where it can verify its validity. Voters may have difficulty understanding these orders or how to deal with them, so there is a special page explaining their usefulness and how to use them. Figure 4.2 illustrates this page, which appears to the voter when the "What's This!!" button is pressed.



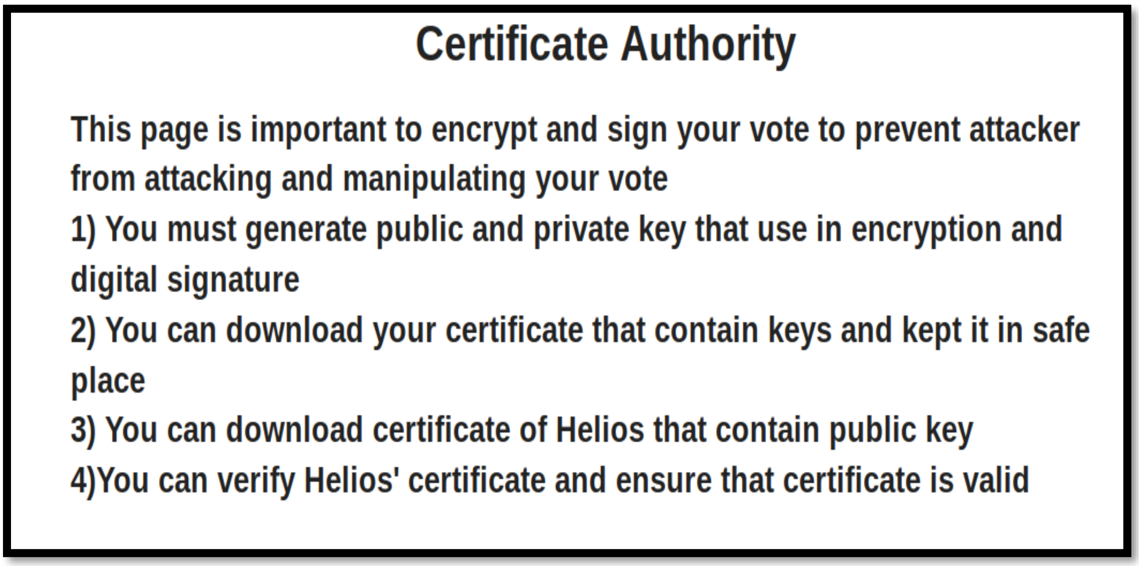
Click on the button below to generate your certificate

Click on the button below to download your certificate

Click on the button below to get public key of Helios

Click on the button below to verify certificate of Helios

Figure 4.1: Certification Authority page.

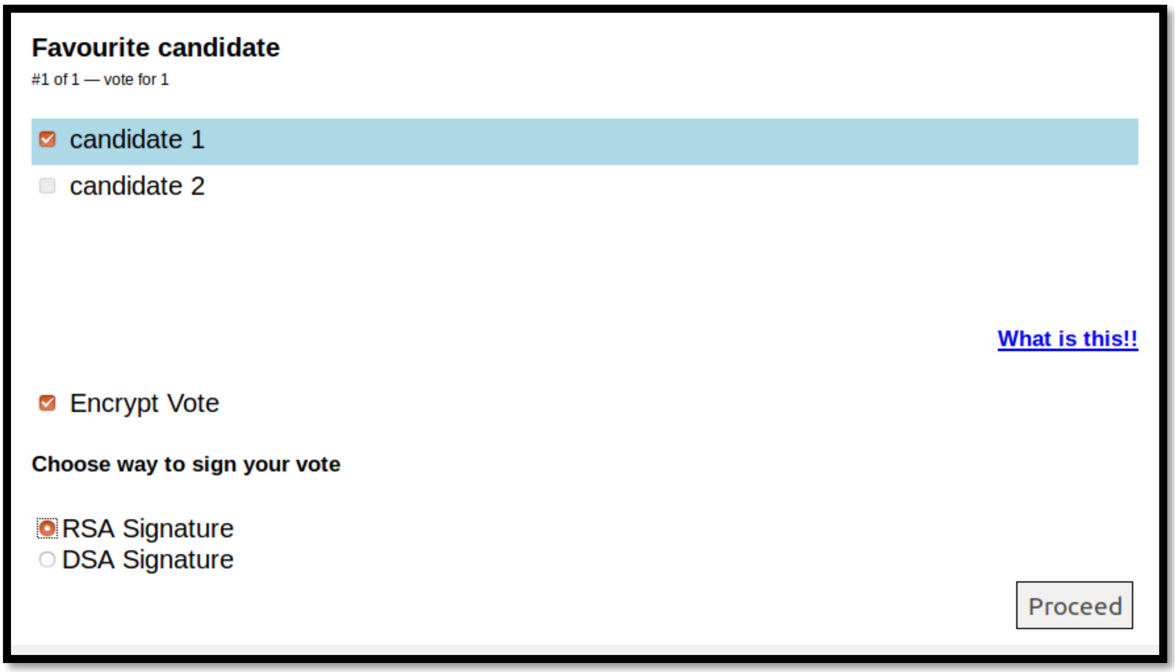


Certificate Authority

This page is important to encrypt and sign your vote to prevent attacker from attacking and manipulating your vote
1) You must generate public and private key that use in encryption and digital signature
2) You can download your certificate that contain keys and kept it in safe place
3) You can download certificate of Helios that contain public key
4)You can verify Helios' certificate and ensure that certificate is valid

Figure 4.2: The “What is this!!” Page.

Upon completion of the certificate creation process, the voter goes to the voting page. After she/he votes and selects the candidate she/he wants, the voter will then choose if she/he wants to encrypt her/his vote and sign it (using either RSA or DSA). If selected, the system will automatically use the voter keys in the certificate for voting and signing. Figure 4.3 represents the voting page. If the voter has difficulty understanding this, she/he can click on the "What is this!!" button, which takes her/his to a page explaining the importance of encryption and signing for voting, as shown in Figure 4.4.



Favourite candidate

#1 of 1 — vote for 1

☑ candidate 1

☐ candidate 2

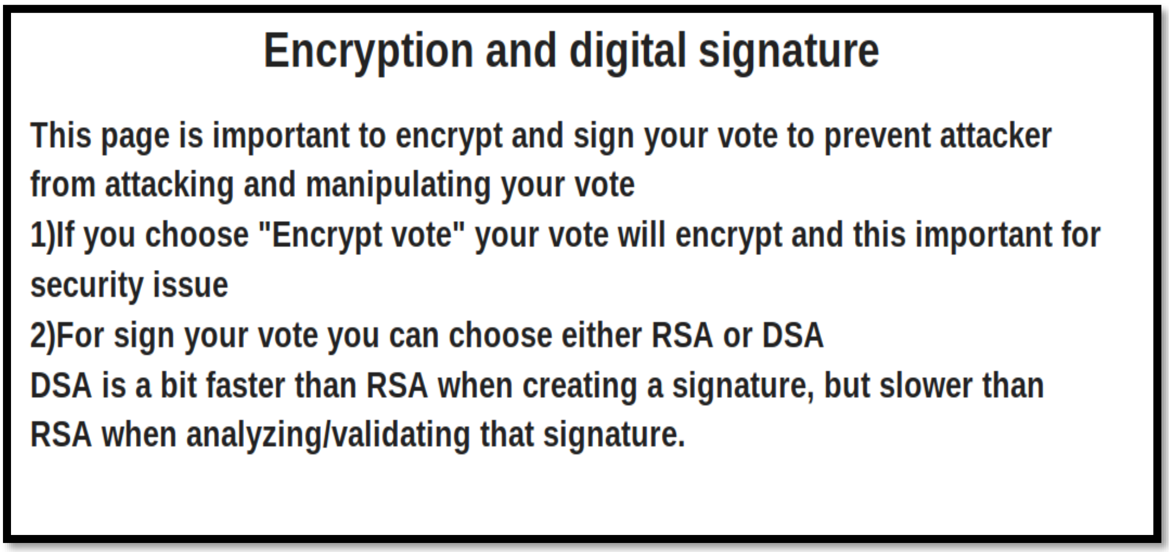
☑ Encrypt Vote

Choose way to sign your vote

● RSA Signature

○ DSA Signature

Figure 4.3: Voting Page.



Encryption and digital signature

This page is important to encrypt and sign your vote to prevent attacker from attacking and manipulating your vote

1)If you choose "Encrypt vote" your vote will encrypt and this important for security issue

2)For sign your vote you can choose either RSA or DSA

DSA is a bit faster than RSA when creating a signature, but slower than RSA when analyzing/validating that signature.

Figure 4.4: The Second “What is this!!” Page.

For testing, a Lenovo computer was used with an Intel Celeron processor and 4GB RAM. The time taken by the system to sign the vote has been calculated. Figure 4.5 shows the results where RSA with different key sizes and DSA are used for signature. The sizes of the RSA keys tested are 512, 1024, 2048 and 4096. The DSA key size is 2048. Note that all results show that the time required to sign a vote is less than one second, which for our case can be considered to be a very short time. Time increases as the volume of the key used increases. When the size of the key used in the DSA algorithm is equal to the key in the RSA, the speed of performance is almost equal or with a very small difference.

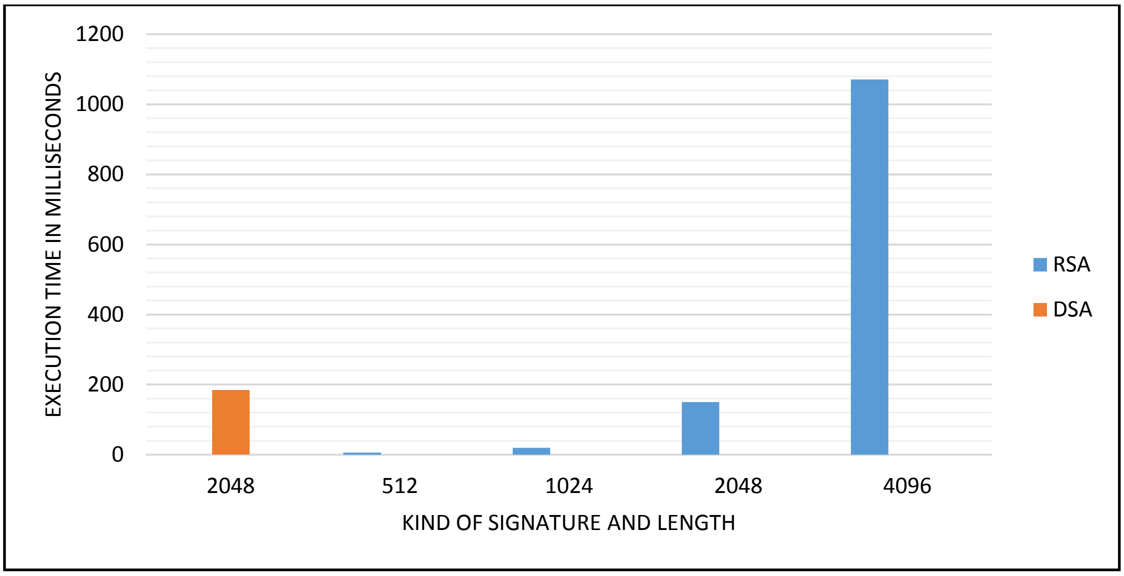


Figure 4.5: Results of the speed of digital signature performance.

Breaking the digital signature algorithm (RSA and/or DSA) depends on analysing the keys used for their initial elements. What makes the RSA and DSA algorithms safe is that no polynomial algorithm for dividing large integers on a classical computer has been found so far. Computing power is measured in MIPS years: a computer with a million instructions per second working for one year. Figure 4.6 represents the results of the estimated time to break the DSA and RSA algorithms.

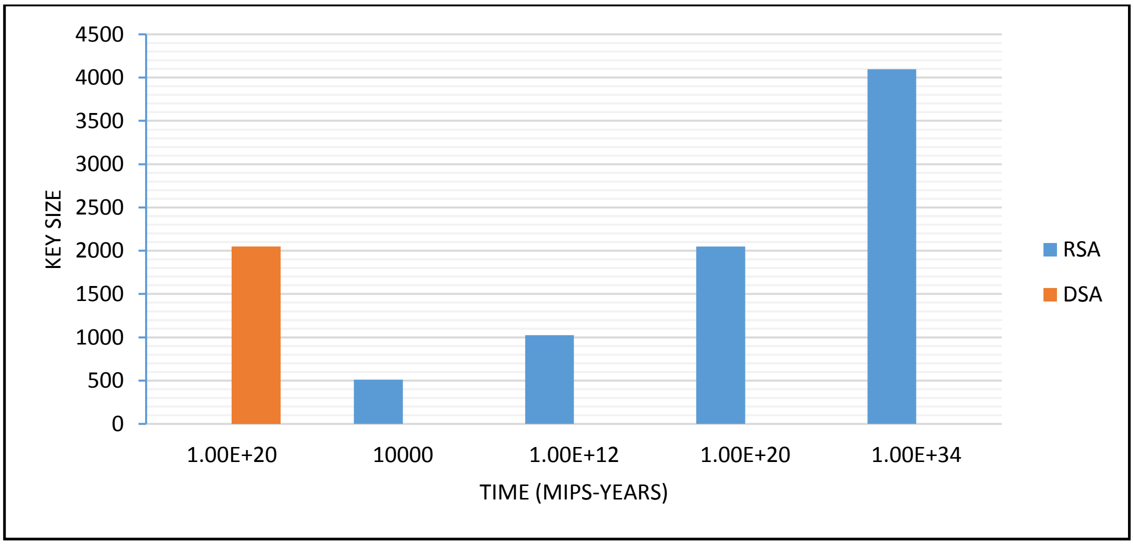


Figure 4.6: Estimated time to break digital signature.

The Helios system encrypts voting only, while the proposed system uses encryption and digital signature. The time it takes for Helios to encrypt and the time it takes for the proposed system to encrypt and sign are calculated. Figure 4.7 represents these results, and it is noted that the difference is very simple and the user will not notice during the voting. The increase in the time required by the proposed system compared to Helios is prudently justified by the increase in security resultant from the added digital signatures.

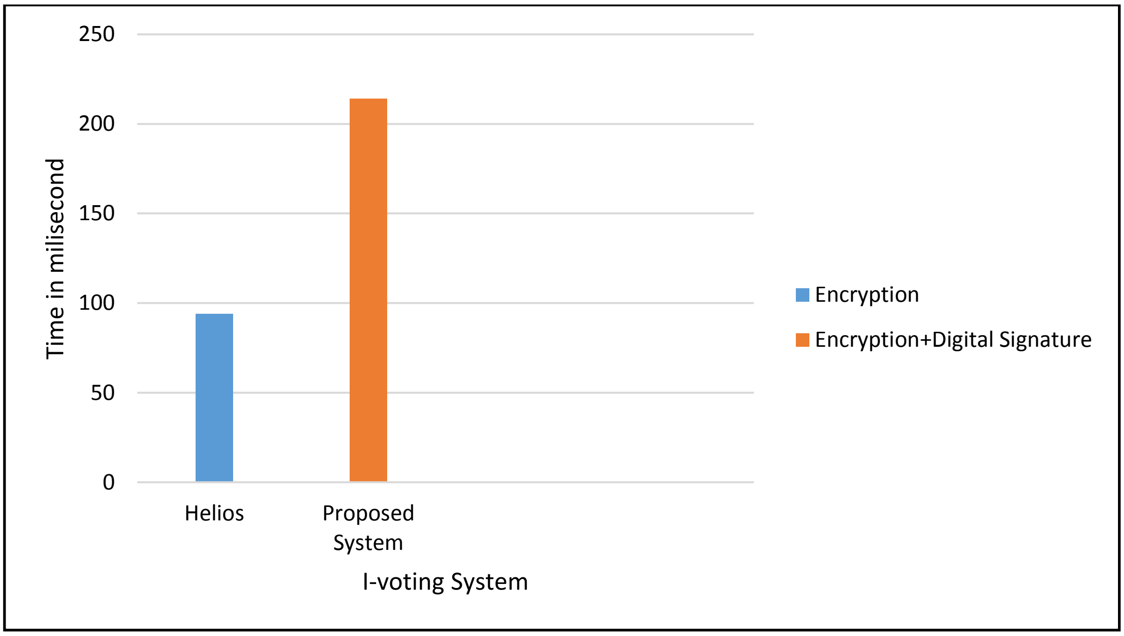


Figure 4.7: Comparison between Helios and Proposed System.

Furthermore, the proposed I-voting system can be analyzed for the basic security requirements of voting systems. In this respect, the following remarks can be made:

a) Eligibility of voter

Eligibility of voters means that no one can impersonate the voter and vote instead of her. In the proposed system, no one can vote until his identity is verified and issued a certificate for her. Each voter has a pair of public and private keys in her certificate, and she is responsible for the confidentiality of her private key. Once the voter votes, her vote will be signed and encrypted using her public and private key. In the proposed system, no private key is published so only voters know their own key. No one can impersonate the voter and submit a ballot instead.

b) Multiple-voting detection

In voting, each voter is entitled to vote only once and is prohibited from multiple ballots. The proposed system allows a voter to vote from more than one account and from each account more than one vote, but only one vote is counted. Anyone can check the bulletin board where they can see that the voter has voted, but they cannot know how she voted. Thus, multiple ballot detection is achieved by the proposed system, because it is always possible to detect whether a voter has already sent a vote.

c) End-to-end voter verifiability

End-to-end verification means that voters can verify the integrity of the ballot, the eligibility of the voters, and the validity of the final result. The voter can check her vote as she wants until she is satisfied that the system is reliable. For a recorded vote, the voter receives her encrypted vote, which can be verified from the bulletin board. The final result can also be computed by anyone because all encrypted votes have been tallied based on the homomorphic encryption property of ElGamal cryptosystem, which is a publicly accessible algorithm. End-to-end verification can be achieved if the bulletin board is honest.

d) Privacy of voters

Each ballot represents a voter's vote for a person of her preference, which can be considered as sensitive information, so it must be protected. If the ElGamal encryption is virtually secure and there is at least one of the honest authorities, the contents of the ballot will not be disclosed during the voting submission. In the proposed system, each vote is encrypted by homomorphic ElGamal encryption before it is submitted. No one can disclose the contents of the ballot as all ballots presented remain encrypted all the time. Decryption requires the cooperation of all authorities which means that decryption will not be implemented in cases where this is not required. In summary, the privacy of voters and contents of the ballot remain secure in the proposed system.

e) Usability

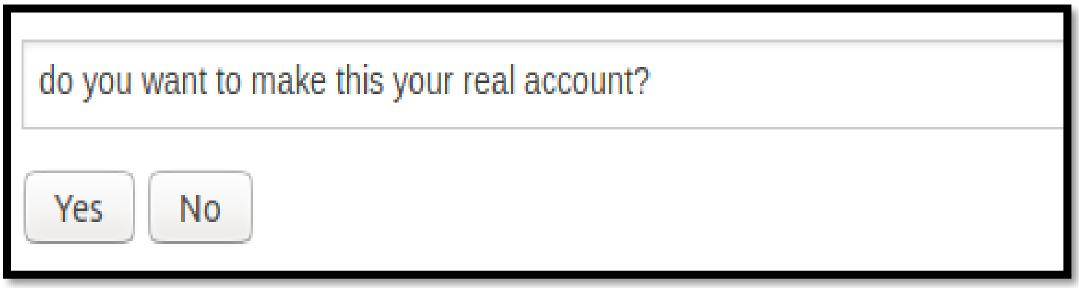
Usability means that the voter can understand what is required of him to vote and not face difficulty during the voting. The interfaces of Helios has been studied and it was found that the voters had difficulty in voting, even some of them did not complete the vote. In the proposed system, interfaces have been improved, some unnecessary orders have been reduced, and some voting steps have been explained. Also, the Arabic language has been added to the system, so that the Arab voters will have no difficulty in understanding the orders in the system.

f) Coercion resistance

Coercion resistance is the most demanding thing of privacy, as it proves that a voter cannot be forced to vote for a choice she does not want. In the Helios system, it does not offer solutions to resist coercion but is designed for low-risk and low-coercion elections. In the proposed system, coercion possibility has been minimally reduced. Since each voter has more than one account, a coercer is unaware of which account a voter has is a real account. Voters can also change their real account at any time. When a voter is forced, she can use any account to vote as the coercer wants, and then she can change her vote as she wants.

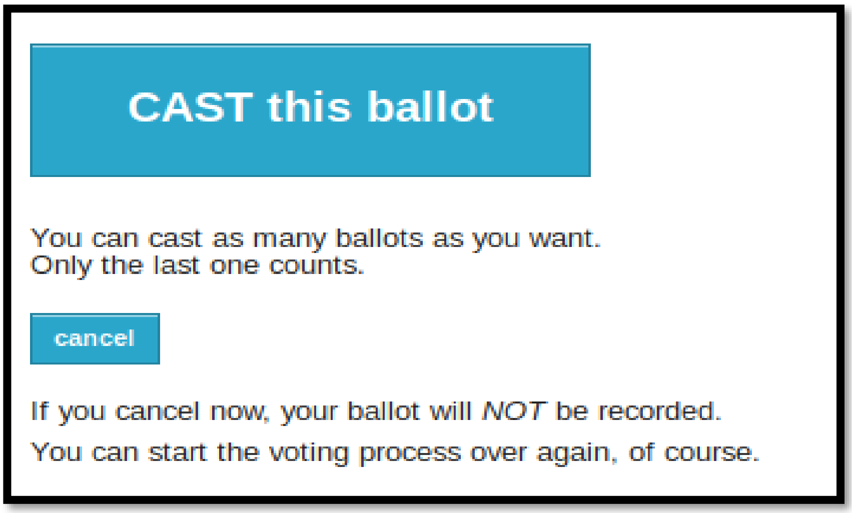
4.3 Adding Multi-accounts Aspect

When a voter logs into the system, she is asked if she wants to make this account her real account to vote, as shown in Figure 4.8. If the voter answers "yes", this account will be the real account (she can change it at any time) and if she presses "no" it will be considered as a fake account. In both cases, the voter will go to the voting page and vote. After she votes, she goes to the Casting Voting page as shown in Figure 4.9 and clicking on "CAST this ballot". In the event that the account used by the voter is the real account, the vote will be sent to the main database or it will go to the secondary database.



do you want to make this your real account?

Figure 4.8: Question for Voter.

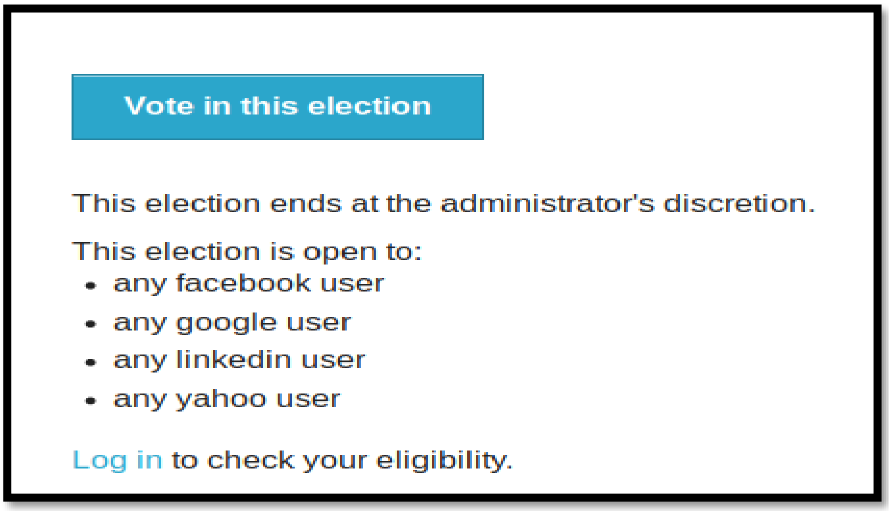


You can cast as many ballots as you want.
Only the last one counts.

If you cancel now, your ballot will *NOT* be recorded.
You can start the voting process over again, of course.

Figure 4.9: Cast the ballot.

If a voter wants to use another account or wants to change her vote, she will go to the voting again page, as shown in Figure 4.10. She presses the "Vote in this elections" button and logs in from any account she wants and then votes. After the election ends, the administrator logs in and presses the "Compute Results" button, as shown in Figure 4.11. In Figure 4.12, the final voting results are shown and it is noted that despite the voter voting from more than one account, one vote has been counted from her real account.



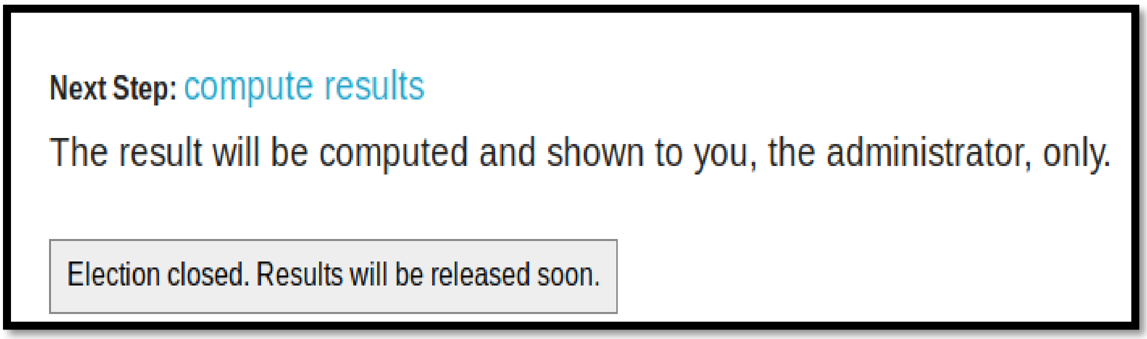
This election ends at the administrator's discretion.

This election is open to:

- any facebook user
- any google user
- any linkedin user
- any yahoo user

Log in to check your eligibility.

Figure 4.10: Voting again in the System.

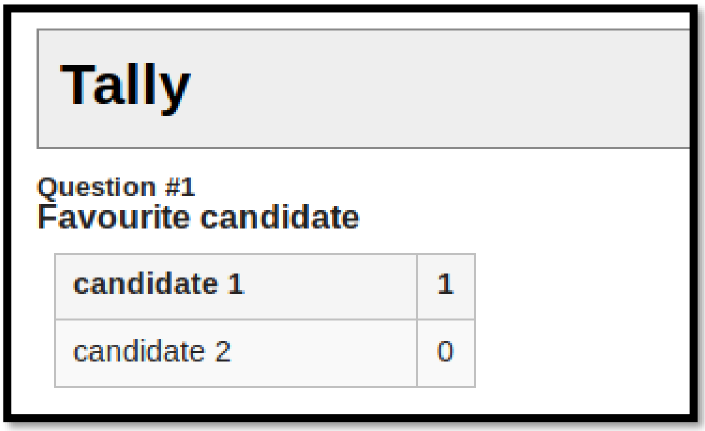


Next Step: compute results

The result will be computed and shown to you, the administrator, only.

Election closed. Results will be released soon.

Figure 4.11: Computing the Final Result.



Tally

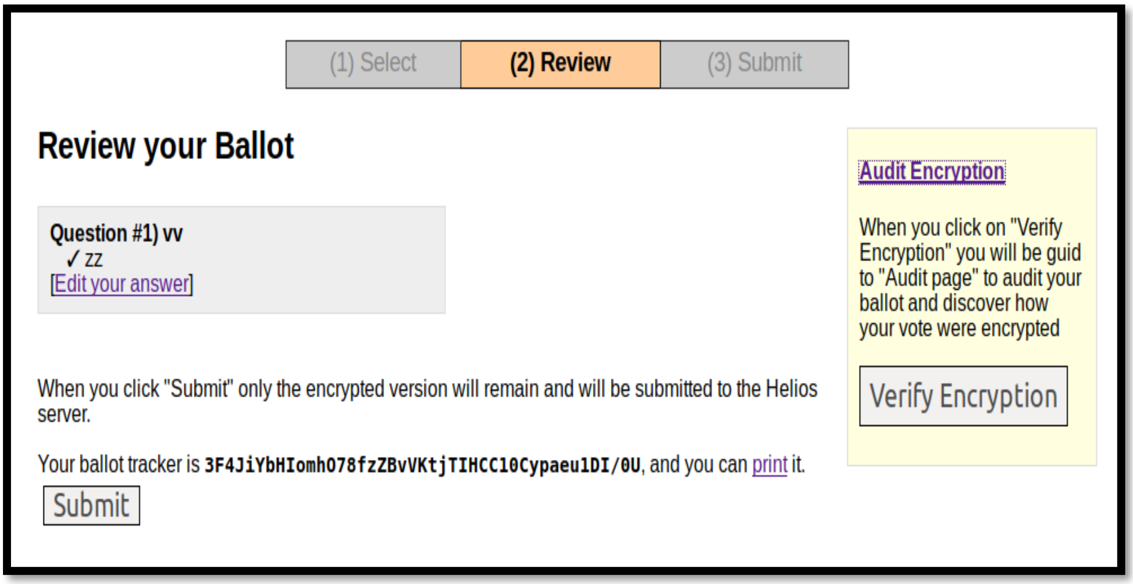
Question #1
Favourite candidate

candidate 1	**1**
candidate 2	0

Figure 4.12: Voting Final Result.

4.4 Improved Interface

The original Helios interface has been improved and made easier to use by voters. Figure 4.13 shows the "Review page" after it has been improved, where some of the commands have been clarified and some unimportant texts removed. Figure 4.14 represents the "Casting page" after the texts has been reduced and explaining why the voter was login out after completing her vote.



Review your Ballot

Question #1) vv
✓ zz
[Edit your answer]

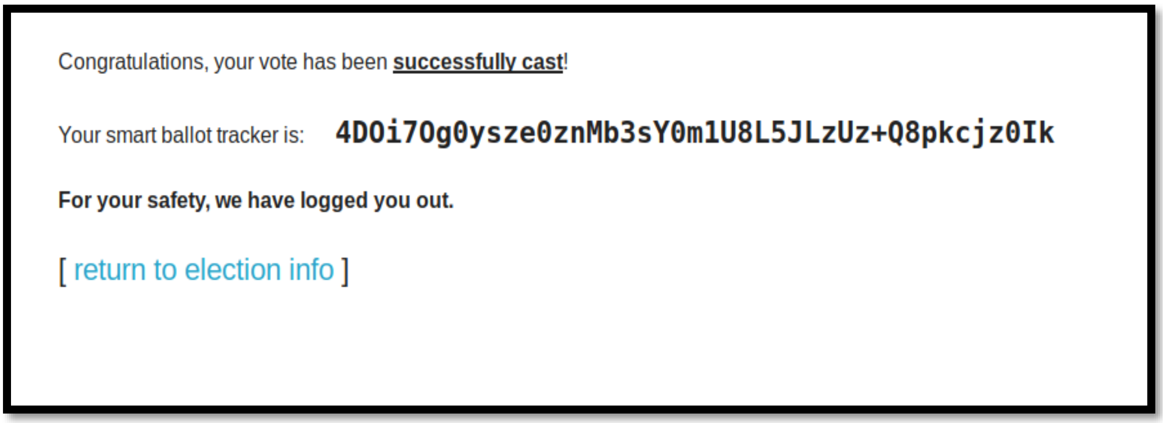
Audit Encryption

When you click on "Verify Encryption" you will be guid to "Audit page" to audit your ballot and discover how your vote were encrypted

When you click "Submit" only the encrypted version will remain and will be submitted to the Helios server.

Your ballot tracker is **3F4JiYbHIomhO78fzZBvVKtjTIHCC10Cypaeu1DI/0U**, and you can print it.

Figure 4.13: Review page.



Congratulations, your vote has been **successfully cast**!

Your smart ballot tracker is: **4DOi7Og0ysze0znMb3sY0m1U8L5JLzUz+Q8pkcjz0Ik**

For your safety, we have logged you out.

[return to election info]

Figure 4.14: Casting page.

An Arabic interface has been added to the system. Thus, Arab voters that do not speak or understand English can change the language of the system. The voter can change the language by pressing the “Arabic” button as shown in Figure 4.15. After that the language in the system is converted to Arabic. For example, some screen shots of the Arabic system interface have been taken. Figure 4.16 shows the main interface of the system in Arabic, Figure 4.17 represents the interface of the FAQ page, and Figure 4.18 represents the certification authority page. The system language can be switched back to English at any time by pressing the "English" button.

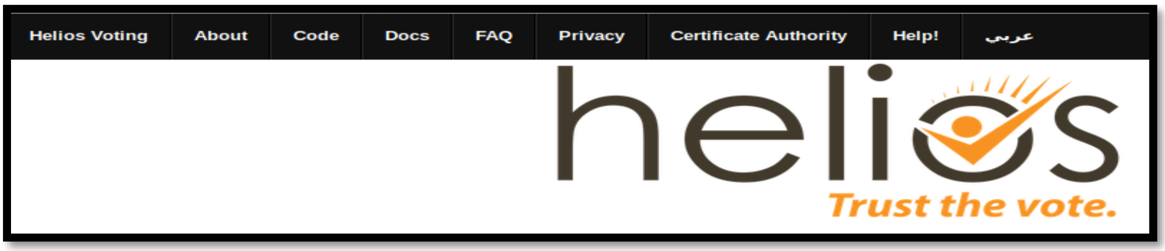
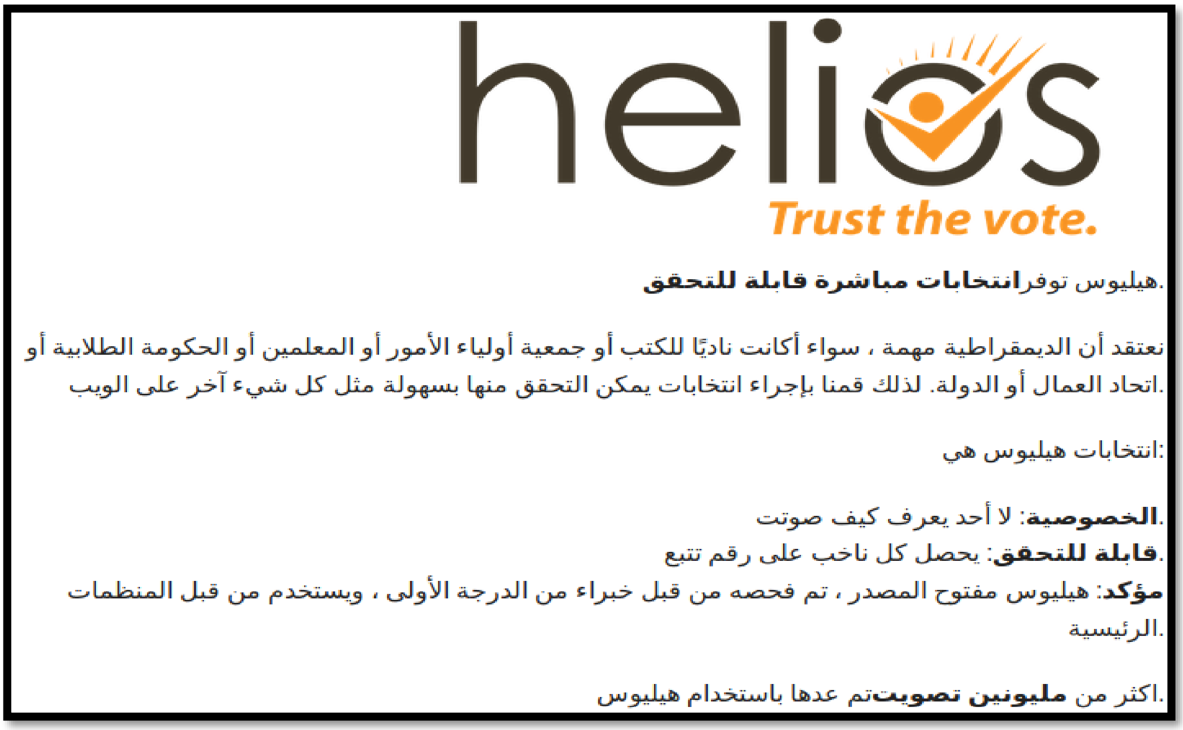


Figure 4.15: Button to Translate the Language.



هيليوس توفر**انتخابات مباشرة قابلة للتحقق**.

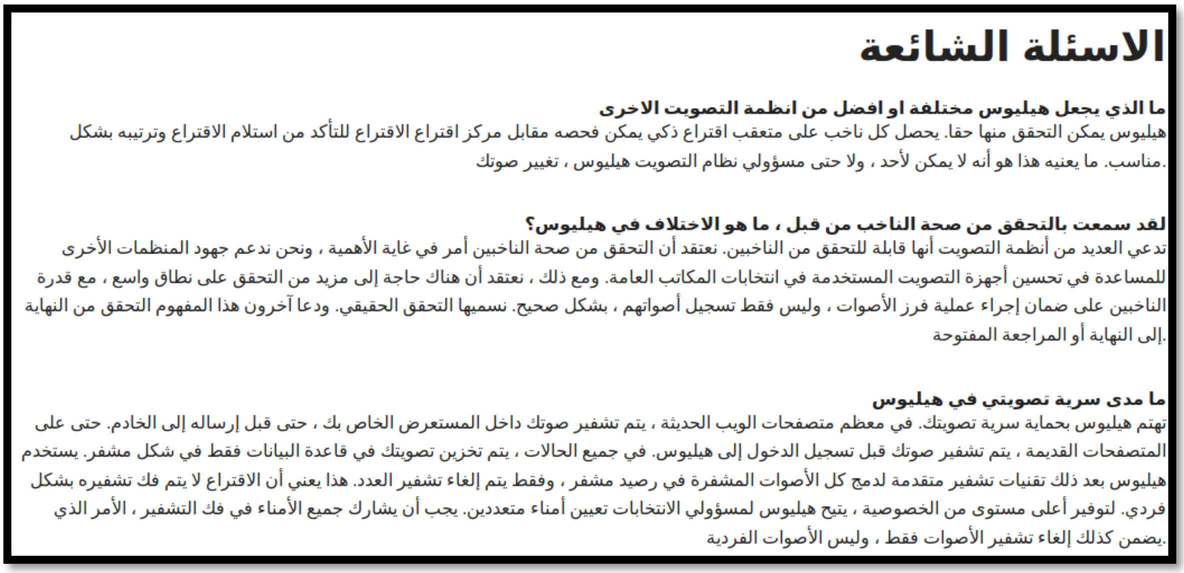
نعتقد أن الديمقراطية مهمة ، سواء أكانت ناديًا للكتب أو جمعية أولياء الأمور أو المعلمين أو الحكومة الطلابية أو
اتحاد العمال أو الدولة. لذلك قمنا بإجراء انتخابات يمكن التحقق منها بسهولة مثل كل شيء آخر على الويب.

انتخابات هيليوس هي:

الخصوصية: لا أحد يعرف كيف صوتت.
قابلة للتحقق: يحصل كل ناخب على رقم تتبع.
مؤكد: هيليوس مفتوح المصدر ، تم فحصه من قبل خبراء من الدرجة الأولى ، ويستخدم من قبل المنظمات
الرئيسية.

اكثر من **مليونين تصويت**تم عدها باستخدام هيليوس.

Figure 4.16: Arabic Main page.



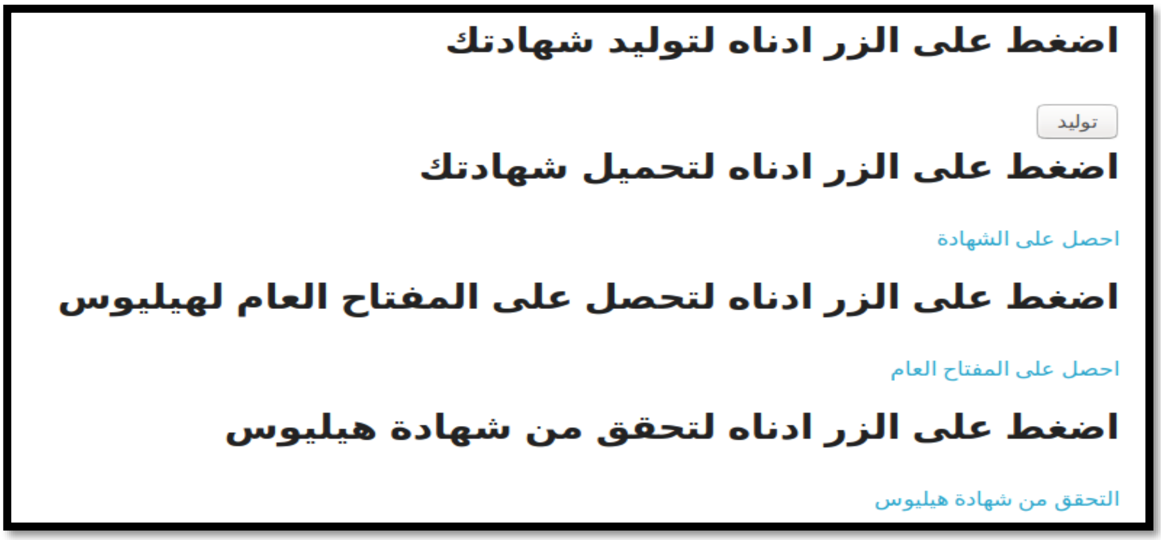
الاسئلة الشائعة

ما الذي يجعل هيليوس مختلفة او افضل من انظمة التصويت الاخرى
هيليوس يمكن التحقق منها حقا. يحصل كل ناخب على متعقب اقتراع ذكي يمكن فحصه مقابل مركز اقتراع الاقتراع للتأكد من استلام الاقتراع وترتيبه بشكل
.مناسب. ما يعنيه هذا هو أنه لا يمكن لأحد ، ولا حتى مسؤولي نظام التصويت هيليوس ، تغيير صوتك

لقد سمعت بالتحقق من صحة الناخب من قبل ، ما هو الاختلاف في هيليوس؟
تدعي العديد من أنظمة التصويت أنها قابلة للتحقق من الناخبين. نعتقد أن التحقق من صحة الناخبين أمر في غاية الأهمية ، ونحن ندعم جهود المنظمات الأخرى
للمساعدة في تحسين أجهزة التصويت المستخدمة في انتخابات المكاتب العامة. ومع ذلك ، نعتقد أن هناك حاجة إلى مزيد من التحقق على نطاق واسع ، مع قدرة
الناخبين على ضمان إجراء عملية فرز الأصوات ، وليس فقط تسجيل أصواتهم ، بشكل صحيح. نسميها التحقق الحقيقي. ودعا آخرون هذا المفهوم التحقق من النهاية
.إلى النهاية أو المراجعة المفتوحة

ما مدى سرية تصويتي في هيليوس
تهتم هيليوس بحماية سرية تصويتك. في معظم متصفحات الويب الحديثة ، يتم تشفير صوتك داخل المستعرض الخاص بك ، حتى قبل إرساله إلى الخادم. حتى على
المتصفحات القديمة ، يتم تشفير صوتك قبل تسجيل الدخول إلى هيليوس. في جميع الحالات ، يتم تخزين تصويتك في قاعدة البيانات فقط في شكل مشفر. يستخدم
هيليوس بعد ذلك تقنيات تشفير متقدمة لدمج كل الأصوات المشفرة في رصيد مشفر ، وفقط يتم إلغاء تشفير العدد. هذا يعني أن الاقتراع لا يتم فك تشفيره بشكل
فردي. لتوفير أعلى مستوى من الخصوصية ، يتيح هيليوس لمسؤولي الانتخابات تعيين أمناء متعددين. يجب أن يشارك جميع الأمناء في فك التشفير ، الأمر الذي
.يضمن كذلك إلغاء تشفير الأصوات فقط ، وليس الأصوات الفردية

Figure 4.17: Arabic FAQ page.



اضغط على الزر ادناه لتوليد شهادتك

اضغط على الزر ادناه لتحميل شهادتك

اضغط على الزر ادناه لتحصل على المفتاح العام لهيليوس

اضغط على الزر ادناه لتحقق من شهادة هيليوس

Figure 4.18: Arabic Certification Authority page.

Furthermore, a questionnaire including 60 people of different ages has been conducted to know their opinions about the easiness of using the proposed I-voting system compared to Helios. Figure 4.19 shows the age of the respondents. 50% of the participants are males, 50% females, 52% employees and 48% non-employees, 86% have completed their education 3% students 11% are uneducated.

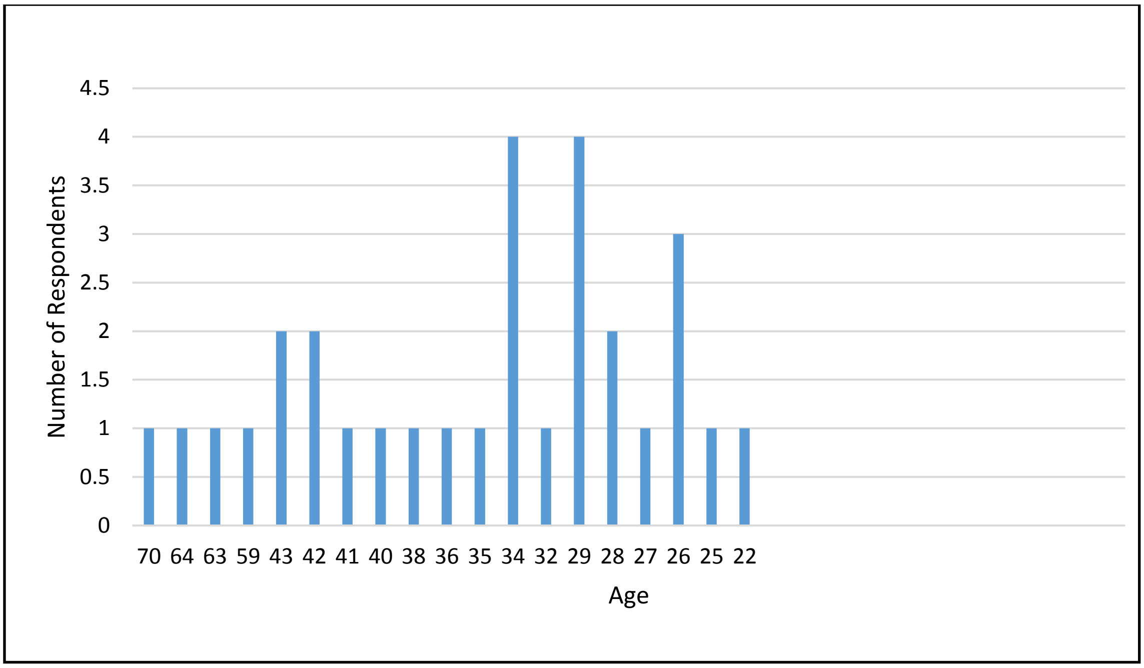


Figure 4.19: Age of the Respondents.

Participants have voted using Helios as well as the proposed system. Then, they have been asked 10 questions about their satisfaction with the voting system. The questions and answers were as follows:

1. Do you trust Internet voting systems?

Yes (60%) No (40%)

2. Was it difficult to use Helios?

Yes (66%) No (34%)

3. Do you understand all the orders in Helios?

Yes (56%) No (44%)

4. Will you use the Helios system to vote in the future?

Yes (40%) No (60%)

5. Was the language in Helios understood?

Yes (53%) No (47%)

6. Was the proposed system easy to use?

Yes (86%) No (14%)

7. Did you use the Arabic language to understand the orders in proposed system?

Yes (63%) No (37%)

8. Will you use the proposed system to vote in the future?

Yes (80%) No (20%)

9. Did you complete the voting using Helios?

Yes (70%) No (30%)

10. Did you complete the voting using the proposed system?

Yes (90%) No (10%)

4.5 Discussions

In this section the results obtained after testing the proposed system will be discussed further. The time it takes for the system to sign the vote is very short from a practical point of view as far as a voting task is concerned. The maximum time it takes is less than one second which is a record time. The time required to break the signature algorithm is very large as it is unlikely that the attacker will break the algorithm during election time. Note that the time it takes for Helios to encode the vote is less than the time used by the proposed system. This is because in the proposed system digital signature is used in addition to encryption. The proposed system meets most of the security requirements that must be met in any voting system.

The use of multiple accounts greatly reduces the risk of coercion and also gives the voter the freedom to choose the account through which he wants to log in. Since there are four ways to vote, this makes it difficult for the coercer to distinguish which of these accounts is the real account. The use of this feature added a lot to the proposed voting system.

Finally, the questionnaire shows that the proposed system is superior to Helios in terms of ease of use. Those who had difficulty using both systems had no knowledge of technology. The majority used the Arabic language during the voting because the group tested was Arab. It was also noted that some people did not complete the voting in both systems due to a large number of orders and pages to which they travel.

Chapter Five: Conclusions and Future Work

Chapter Five

Conclusions and Future Work

5.1 Conclusions

The most important points of conclusion that can be drawn from this works can be listed as follows:

1. An I-voting system based on Helios and a public key certificate has shown improvements to the security and scalability, coercion and usability aspects of the Helios voting system.
2. On the security and scalability side, it has been suggested to use a certification authority for creating a certificate for each voter. The possibility of signing each vote was added using either the RSA or DSA algorithm.
3. To reduce the risk of coercion suffered by the Helios system, it has been suggested that each voter have four accounts to use for voting. One of these accounts is real that means when a voter votes through it, that vote will be counted within final votes. This has been found to be an effective approach to reduce coercion acts as the voter can use her fake account to vote when she is coerced by the attacker and forced to vote for a particular person.
4. The simplifications and modifications made to Helios interfaces and adding Arabic language interface have increased system usability, especially for Arab users. The conducted questionnaire has indicated that voters are more satisfied with the proposed system compared to the Helios system.
5. The time required for the system to sign and encrypt votes was 210 ms, and the time required for the Helios system to encrypt votes was 96 ms. Despite the small increase in time, this is quite justified for the significant increase of system security due to the inclusion of digital signature.

5.2 Future Work

The work can be enhanced in several directions in the future. Some future work directions include:

1. Applying the proposed system in real elections and studying its usability and other characteristics.
2. The certificate is automatically generated when a voter logs into the system instead of being created by the voter himself.
3. The possibility of using multiple accounts from any device used by the voter, and not rely on the IP of the voter to know that she/he is the same person.
4. Integrating the system with an initial stage of biometric authentication for accurate identification of voters.
5. Add other languages to the system, not just Arabic, to make the system more extensive.

References

[1] G. Ofori-Dwumfuo and E. Paatey, "The design of an electronic voting system," *Research Journal of Information Technology*, vol. 3, no. 2, pp. 91-98, 2011.

[2] V. K. Priya, V. Vimaladevi, B. Pandimeenal, and T. Dhivya, "Arduino based smart electronic voting machine," in *2017 International Conference on Trends in Electronics and Informatics (ICEI)*, 2017, pp. 641-644: IEEE.

[3] M. M. Islam, M. S. U. Azad, M. A. Alam, and N. Hassan, "Raspberry Pi and image processing based electronic voting machine (EVM)," *International Journal of Scientific Engineering Research,* vol. 5, no. 1, pp. 1506-1510, 2014.

[4] V. Kalaichelvi and R. Chandrasekaran, "Secured single transaction e-voting protocol: Design and implementation," *European Journal of Scientific Research,* vol. 51, no. 2, pp. 276-284, 2011.

[5] V. Augoye and A. Tomlinson, "Analysis Of Electronic Voting Schemes In The Real World," 2018.

[6] A. A. Philip, S. A. Simon, and A. Oluremi, "A receipt-free multi-authority e-voting system," *International Journal of Computer Applications,* vol. 30, no. 6, pp. 15-23, 2011.

[7] R. Hanifatunnisa and B. Rahardjo, "Blockchain based e-voting recording system design," in *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, 2017, pp. 1-6: IEEE.

[8] K.-H. Wang, S. K. Mondal, K. Chan, and X. Xie, "A review of contemporary e-voting: Requirements, technology, systems and usability," *Data Science and Pattern Recognition,* vol. 1, no. 1, pp. 31-47, 2017.

[9] W. Bokslag and M. J. a. p. a. de Vries, "Evaluating e-voting: theory and practice," 2016.

[10] M. Germann and U. J. E. S. Serdült, "Internet voting and turnout: Evidence from Switzerland," vol. 47, pp. 1-12, 2017.

[11] F. Karayumak, M. M. Olembo, M. Kauer, and M. Volkamer, "Usability Analysis of Helios-An Open Source Verifiable Remote Electronic Voting System," *EVT/WOTE*, vol. 11, no. 5, 2011.

[12] F. Karayumak, M. Kauer, M. M. Olembo, T. Volk, and M. Volkamer, "User study of the improved Helios voting system interfaces," in *2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)*, 2011, pp. 37-44: IEEE.

[13] V. Cortier, D. Galindo, S. Glondu, and M. Izabachene, "Election verifiability for Helios under weaker trust assumptions," in *European Symposium on Research in Computer Security*, 2014, pp. 327-344: Springer.

[14] O. Kulyk, V. Teague, and M. Volkamer, "Extending helios towards private eligibility verifiability," in *International Conference on E-Voting and Identity*, 2015, pp. 57-73: Springer.

[15] D. Chung, M. Bishop, and S. Peisert, "Distributed Helios-Mitigating Denial of Service Attacks in Online Voting," 2016.

[16] O. Kulyk, K. Marky, S. Neumann, and M. Volkamer, "Introducing proxy voting to Helios," in *2016 11th International Conference on Availability, Reliability and Security (ARES)*, 2016, pp. 98-106: IEEE.

[17] M. Backes, C. Hammer, D. Pfaff, and M. Skoruppa, "Implementation-level analysis of the JavaScript helios voting client," in *Proceedings of the 31st Annual ACM Symposium on Applied Computing*, 2016, pp. 2071-2078: ACM.

[18] N. Chang-Fong and A. Essex, "The cloudier side of cryptographic end-to-end verifiable voting: a security analysis of Helios," in *Proceedings of the 32nd Annual Conference on Computer Security Applications*, 2016, pp. 324-335: ACM.

[19] E. A. Quaglia and B. Smyth, "Authentication with weaker trust assumptions for voting systems," in *International Conference on Cryptology in Africa*, 2018, pp. 322-343: Springer.

[20] B. Smyth, "Verifiability of helios mixnet," in *International Conference on Financial Cryptography and Data Security*, 2018, pp. 247-261: Springer.

[21] M. Meyer and B. Smyth, "Exploiting re-voting in the Helios election system," *Information Processing Letters*, vol. 143, pp. 14-19, 2019.

[22] L. P. Alonso, M. Gasco, D. Y. M. del Blanco, J. A. H. Alonso, J. Barrat, and H. A. Moreton, "E-voting system evaluation based on the Council of Europe recommendations: Helios Voting," *IEEE Transactions on Emerging Topics in Computing,* 2018.

[23] O. Pereira, "Internet voting with Helios," *Real-World Electronic Voting: Design, Analysis Deployment,* vol. 8604, pp. 279–310, 2016.

[24] C. Z. Acemyan, P. Kortum, M. D. Byrne, and D. S. Wallach, "From Error to Error: Why Voters Could not Cast a Ballot and Verify Their Vote With Helios, Prêt à Voter, and Scantegrity {II}," *Journal of Election Technology Systems,* vol. 3, pp. 1-25, 2015.

[25] C.-K. Wu and R. Sankaranarayana, "Internet voting: concerns and solutions," in *First International Symposium on Cyber Worlds, 2002. Proceedings.*, 2002, pp. 261-266: IEEE.

[26] L. P. Alonso, M. Gasco, D. Y. M. del Blanco, J. A. H. Alonso, J. Barrat, and H. A. J. I. T. o. E. T. i. C. Moreton, "E-voting system evaluation based on the Council of Europe recommendations: Helios Voting," 2018.

[27] X. Zou, H. Li, F. Li, W. Peng, and Y. J. C. Sui, "Transparent, Auditable, and Stepwise Verifiable Online E-Voting Enabling an Open and Fair Election," vol. 1, no. 2, p. 13, 2017.

[28] X. Zou, H. Li, F. Li, W. Peng, and Y. Sui, "Transparent, Auditable, and Stepwise Verifiable Online E-Voting Enabling an Open and Fair Election," *Cryptography,* vol. 1, no. 2, p. 13, 2017.

[29] Z. A. Saputri, A. Sudarsono, and M. Yuliana, "E-voting security system for the election of EEPIS BEM president," in *2017 International Electronics Symposium on Knowledge Creation and Intelligent Computing (IES-KCIC),* 2017, pp. 147-152: IEEE.

[30] Z. Rjašková, "Electronic voting schemes," *Diplomová práca, Bratislava,* 2002.

[31] C. Taddia, D. Ferraretti, M. Pastorelli, S. Nanni, and G. Mazzini, "Secure management of an Internet voting system: A case study for land reclamation authority," in *2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM),* 2017, pp. 1-5: IEEE.

[32] C. Lambrinoudakis, D. Gritzalis, V. Tsoumas, M. Karyda, and S. Ikonomopoulos, "Secure electronic voting: The current landscape," in *Secure electronic voting*: Springer, 2003, pp. 101-122.

[33] A. Omidi and S. Moradi, "Modeling and quantitative evaluation of an internet voting system based on dependable web services," in *2012 International Conference on Computer and Communication Engineering (ICCCE),* 2012, pp. 825-829: IEEE.

[34] A. Rajendra and H. Sheshadri, "Visual Cryptography in Internet Voting System," in *Third International Conference on Innovative Computing Technology (INTECH 2013),* 2013, pp. 60-64: IEEE.

[35] A. Schneider, C. Meter, and P. Hagemeister, "Survey on remote electronic voting," *arXiv preprint arXiv:.02798,* 2017.

[36] C. Paar and J. Pelzl, *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media, 2009.

[37] C. J. C. A. Zhiming and Software, "An improved encryption algorithm on ElGamal algorithm," vol. 22, no. 2, pp. 82-85, 2005.

[38] N. Koblitz, *A course in number theory and cryptography*. Springer Science & Business Media, 1994.

[39] C. Lambrinoudakis, V. Tsoumas, M. Karyda, and S. Ikonomopoulos, "SECURE e-VOTING The Current Landscape," 2002.

[40] Z. J. D. p. Rjašková, Bratislava, "Electronic voting schemes," 2002.

[41] P. Ribarski, L. J. J. o. c. Antovski, and i. technology, "Mixnets: Implementation and performance evaluation of decryption and re-encryption types," vol. 20, no. 3, pp. 225-231, 2012.

[42] D. Chaum, "Blind signatures for untraceable payments," in *Advances in cryptology,* 1983, pp. 199-203: Springer.

[43] L. Fouard, M. Duclos, and P. Lafourcade, "Survey on electronic voting schemes," *supported by the ANR project AVOTÉ,* 2007.

[44] A. Schneider, C. Meter, and P. J. a. p. a. Hagemeister, "Survey on remote electronic voting," 2017.

[45] D. Sandler, K. Derr, and D. S. Wallach, "VoteBox: A Tamper-evident, Verifiable Electronic Voting System," in *USENIX Security Symposium*, 2008, vol. 4, no. 0, p. 87.

[46] M. R. Clarkson, S. Chong, and A. C. Myers, "Civitas: Toward a secure voting system," in *2008 IEEE Symposium on Security and Privacy (sp 2008),* 2008, pp. 354-368: IEEE.

[47] P. Y. Ryan, D. Bismark, J. Heather, S. Schneider, Z. J. I. t. o. i. f. Xia, and security, "Prêt à voter: a voter-verifiable voting system," vol. 4, no. 4, pp. 662-673, 2009.

[48] A. A. Philip, S. A. Simon, and A. J. I. J. o. C. A. Oluremi, "A receipt-free multi-authority e-voting system," vol. 30, no. 6, pp. 15-23, 2011.

[49] R. Haenni and O. Spycher, "Secure Internet Voting on Limited Devices with Anonymized DSA Public Keys," *EVT/WOTE,* vol. 11, 2011.

[50] H. Pan, E. Hou, and N. Ansari, "Ensuring voters and candidates' confidentiality in E-voting systems," in *34th IEEE Sarnoff Symposium,* 2011, pp. 1-6: IEEE.

[51] H. Pan, E. Hou, and N. Ansari, "E-NOTE: An E-voting system that ensures voter confidentiality and voting accuracy," in *2012 IEEE International Conference on Communications (ICC),* 2012, pp. 825-829: IEEE.

[52] R. Abdelkader and M. Youssef, "Uvote: A ubiquitous e-voting system," in *2012 Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing*, 2012, pp. 72-77: IEEE.

[53] W. Itani, C. Ghali, A. El Hajj, A. Kayssi, and A. Chehab, "SinPack: A security protocol for preventing pollution attacks in network-coded content distribution networks," in *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, 2010, pp. 1-6: IEEE.

[54] H. Perl, Y. Mohammed, M. Brenner, and M. Smith, "Fast confidential search for bio-medical data using bloom filters and homomorphic cryptography," in *2012 IEEE 8th International Conference on E-Science*, 2012, pp. 1-8: IEEE.

[55] A. Essex, J. Clark, and U. Hengartner, "Cobra: Toward Concurrent Ballot Authorization for Internet Voting," in *EVT/WOTE*, 2012, p. 3.

[56] G. Tsoukalas, K. Papadimitriou, and P. Louridas, "From helios to zeus," *USENIX Journal of Election Technology Systems*, vol. 1, no. 1, pp. 1-17, 2013.

[57] S. Nevo and H. Kim, "How to compare and analyse risks of internet voting versus other modes of voting," *EG*, vol. 3, no. 1, pp. 105-112, 2006.

[58] W. Bokslag and M. de Vries, "Evaluating e-voting: theory and practice," *arXiv preprint arXiv:.02509*, 2016.

[59] A. E. Elewa, A. AlSammak, A. AbdElRahman, and T. ElShishtawy, "Challenges of electronic voting-a survey," *Advances in Computer Science: an International Journal*, vol. 4, no. 6, pp. 98-108, 2015.

[60] K. Butterfield and X. Zou, "Analysis and implementation of internet based remote voting," in *2014 IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems*, 2014, pp. 714-719: IEEE.

[61] H. Pardue, A. Yasinsac, and J. Landry, "Towards internet voting security: A threat tree for risk assessment," in *2010 Fifth International Conference on Risks and Security of Internet and Systems (CRiSIS)*, 2010, pp. 1-7: IEEE.

[62] B. Adida, "Helios: Web-based Open-Audit Voting," in *USENIX security symposium*, 2008, vol. 17, pp. 335-348.

[63] J. Benaloh, "Towards simple verifiable elections," in *Proceedings of Workshop on Trustworthy Election (WOTE'06)*, 2006, pp. 61-68.

[64] K. Sako and J. Kilian, "Receipt-free mix-type voting scheme," in *International Conference on the Theory and Applications of Cryptographic Techniques*, 1995, pp. 393-403: Springer.

[65] B. Adida, O. De Marneffe, O. Pereira, and J.-J. Quisquater, "Electing a university president using open-audit voting: Analysis of real-world use of Helios," *EVT/WOTE,* vol. 9, no. 10, 2009.

[66] R. Cramer, R. Gennaro, and B. Schoenmakers, "A secure and optimally efficient multi-authority election scheme," *European transactions on Telecommunications,* vol. 8, no. 5, pp. 481-490, 1997.

[67] O. Pereira, "Internet voting with Helios," *Real-World Electronic Voting: Design, Analysis Deployment,* vol. 8604, 2016.

[68] A. Filipiak, "Design and formal analysis of security protocols, an application to electronic voting and mobile payment," 2018.

[69] E. A. Quaglia and B. Smyth, "A short introduction to secrecy and verifiability for elections," *arXiv preprint arXiv:.03168,* 2017.

[70] V. Cortier, D. Galindo, S. Glondu, and M. Izabachene, "Distributed elgamal á la pedersen: application to helios," in *Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society*, 2013, pp. 131-142: ACM.

[71] M. Volkamer, O. Spycher, and E. Dubuis, "Measures to establish trust in internet voting," in *Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance,* 2011, pp. 1-10: ACM.

[72] D. Bernhard, V. Cortier, O. Pereira, B. Smyth, and B. Warinschi, "Adapting Helios for provable ballot privacy," in *European Symposium on Research in Computer Security*, 2011, pp. 335-354: Springer.

[73] S. F. Al-Janabi and A. K. Obaid, "Development of certificate authority services for web applications," in *2012 International Conference on Future Communication Networks*, 2012, pp. 135-140: IEEE.

[74] R. Hunt, "Technological infrastructure for PKI and digital certification," *Computer communications*, vol. 24, no. 14, pp. 1460-1471, 2001.

[75] L. M. Kohnfelder, "Towards a practical public-key cryptosystem," Massachusetts Institute of Technology, 1978.

[76] J. Weise, "Public key infrastructure overview," *Sun BluePrints OnLine, August*, pp. 1-27, 2001.

[77] W. M. Shbair, "Service-Level Monitoring of HTTPS Traffic," 2017.

[78] J. R. Vacca, *Cyber security and IT infrastructure protection*. Syngress, 2013.

[79] S. William, *Computer security: Principles and practice*. Pearson Education India, 2008.

الملخص

التصويت هو العملية التي يتم من خلالها اختيار ممثلي البلد (أو المنظمة). لكل شخص الحق في انتخاب مرشحين يعتبرونه مناسبًا لقيادة البلاد. يجب التأكد من أن الانتخابات عادلة وعدم التلاعب بالأصوات أو حذفها أو تغييرها ، أو حتى إجبار الناخبين على التصويت لمرشحين لا يريدونهم. بعض الناخبين لا يذهبون إلى صناديق الاقتراع للتصويت لأسباب شخصية أو عامة. أحد حلول هذه المشكلة هو التصويت عبر الإنترنت حيث يمكن التصويت من أي مكان وفي أي وقت.

التصويت عبر الإنترنت له العديد من المزايا وبالتأكيد هناك عيوب. تم اقتراح العديد من أنظمة التصويت عبر الإنترنت ، لكن استخدامها منخفض وغير واسع الانتشار في العالم. ويرجع ذلك إلى انعدام ثقة الناخبين بالإنترنت لأنه من الممكن أن يتعرض النظام للهجوم من أي مكان في العالم وأيضًا أن ليس الجميع في العالم يستخدمون الإنترنت. يعد نظام التصويت هيليوس ، وهو نظام مفتوح المصدر ، وهو أحد أكثر أنظمة التصويت شعبية.

تقدم هذه الرسالة نظام مقترح للتصويت عبر الانترنت مبني على أساس نظام هيليوس وشهادة المفتاح العام. سبب استخدام هيليوس هو أنه مفتوح المصدر ، واستخدامه واسع النطاق ويمكن الوصول إليه بسهولة. تم إدخال تحسينات على نظام هيليوس. تمت إضافة المرجع المصدق الذي ينشئ شهادات الناخبين التي تحتوي على مفاتيح عامة وخاصة يتم استخدامها لاحقًا في عملية التصويت ، حيث يتم استخدامها في التشفير والتوقيع الرقمي. تمت إضافة ايضاً توقيع للتصويت بواسطة خوارزمية (RSA) أو خوارزمية التوقيع (DSA). أعطي لكل ناخب حسابًا حقيقيًا وحسابات مزيفة أخرى لاستخدامها في حالة إكراه الناخب. أخيرًا ، تم تحسين واجهة هيليوس وإضافة اللغة العربية إلى النظام.

تم اختبار النظام وتم حساب التوقيت اللازم للتوقيع وتشفير التصويت ومقارنته بهيليوس. لقد وجد أن إضافة المرجع المصدق يزيد من الأمان والقابلية للتوسعة ، كما أن الوقت المستغرق للنظام المقترح مقارنة بالنظام الأصلي قريب جدًا على الرغم من إضافة التوقيع الرقمي. إن إضافة حسابات متعددة تجعل الناخب أكثر حرية في اختيار الحساب الذي يريده واستخدامه في المواقف القسرية. تم اختبار الواجهات الجديدة أيضًا ، وتم إجراء استبيان من 60 شخصًا. أشارت النتائج إلى أن مستوى رضا الناخبين أعلى للنظام المقترح مقارنة بواجهات هيليوس الأصلية.

جمهورية العراق

وزارة التعليم العالي والبحث العلمي

جامعة الانبار

كلية علوم الحاسوب وتكنولوجيا المعلومات

قسم علوم الحاسبات

نظام التصويت المحسّن على أساس هيليوس وشهادات المفتاح العمومي الرقمية

رسالة مقدمة الى

قسم علوم الحاسبات – كلية علوم الحاسوب وتكنولوجيا المعلومات –جامعة الانبار وهي جزء من متطلبات نيل درجة ماجستير علوم في علوم الحاسبات

قدمت من قبل

نور حمد عبد

بإشراف

أ. د. سفيان تايه الجنابي

١٤٤١ هـ **٢٠٢٠ م**