بسم الله الرحمن الرحيم

SUDAN UNIVERSITY OF SCIENCE AND TECHNOLOGY

COLLEGE OF GRADUATE STUDIES

MASTER OF INFORMATION TECHNOLOGY PROGRAM

Secure E-voting System using Symmetric Encryption

تامين نظام الانتخابات بإستخدام التشفير المتماثل

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Information Technology

By:

Aml Mohamed Ahmed Elawed Amasib

Supervision:

Dr.Faisal Mohammed Abdalla

May 2018

Dedication

To my family

To my teachers

To my best friends

Acknowledgment

I would like to express my sincerest appreciation and profound granitite to my supervisor Dr. Faisal Mohammed Abdallah, Chair Person, Department of Computer Science and information technology, Kerrey University, encourage guidance. In the course of the project development he discussed problems. He helped to overcome hurdles. His keen interest and valuable suggestions and advice were the source of all inspiration to me.

I would also like to thank my Parents who have always been prepared to go out of their almost support during my time at university.

Finally I would like to thank my best friend Mawada Adam.

Abstract

Secure Voting System’ is heart of any democracy. There are number of nationwide voting system adopted all over the world, but each of them has their own shortfalls. The remote Internet voting systems still suffer many problems. These are some reasons that, manual voting is still in practice in many developing and developed nations in this internet era. Thus, complete, strongly secured and user friendly ‘E-Voting System’ is need of time. The aim of this thesis is to design a secure electronic voting system choosing AES algorithm for encrypt and decrypt vote and chose MD5 algorithm to achieve integrity. The vote is encrypted and stored in the database, thus securing all the voting steps, and ensure confidentiality, authentication, and privacy in electoral operation. And also choosing UML (unified modeling language) for analytical purpose.

Lastly, security analysis is done to show how the proposed model can resist know attacks.

المستخلص

جودة وشفافيه نظام التصويت هو أساس أي نظام ديمقراطي .هناك عدد من أنظمة التصويت التي تم تبنيها في جميع انحاء العالم لكن كل واحد منهم يعاني من حالات النقص الخاصة به .لا تزال انظمه التصويت عن بعد عبر الانترنت تعاني العديد من المشاكل من ضمنها انعدام الشفافيه والتزوير أيضا لازال التصويت التقليدي يمارس عمليا في العديد من الدول الناميه والمتقدمة في عصر الانترنت هذا ايضا له عدة عيوب ومساؤي منها الاخطاء التي تحدث أثناء عمليات التصويت و سهوله التزوير في نتائج الانتخابات وايضا انعدام اساليب النزاهة في العمليه الانتخابية وبالتالي فان استحداث نظام للتصويت الالكتروني الكامل والموثوق به مطلوب بشدة في الوقت الراهن.

الهدف من هذا البحث هو تصميم نظام تصويت الكتروني امن باستخدام خوارزميات AES لتشفير الصوت وخوارزميه MD5.لتحقيق المصداقيه وبالتالي تأمين جميع خطوات التصويت ، وضمان السريه والمصادقة والخصوصية في العمليه الانتخابيه. وايضا تم استخدام لغه النمذجة الموحدة للتحليل.

وأخيرا ، تم التحليل لإظهار كيف أن النموذج المقترح يمكن أن يقاوم الهجمات المعرفة في أمن البيانات.

Table of contain

Contents

List of figures

List of Abbreviations

AES: Advance Encryption Standard

DRE: Direct Recording Electronic

ESD: Electronic Service Delivery

EVS: Electronic Voting System

ICT: Information and Communication Technology

IV: Internet-voting

UML: Unified Modeling Language

UN: United Nation

CHAPTER One

INTRODUCTION

CHAPTER ONE

INTRODUCTION

1.1 Background

Elections allow the populace to choose their representatives and express their preferences for how they will be governed. A voting system must preserve the anonymity of a voter's ballot, must be tamper-resistant, and be comprehensible to and usable by the entire voting population. In traditional elections, voters go to their home precinct and prove that they are allowed to vote there, by presenting an ID card. After this, the voter is given a validated envelope that allows them to approach a voting booth, choose a piece of paper, make a mark in a preprinted paper or similar for their candidates of choice, save the paper in the official envelope and close it. Later, in presence of voting authorities, the voter put the envelope in a box. When the contest time expired, a handmade count and tabulate vote process must be do in each precinct. Later, the communication of results to a central general office (sometimes a hierarchical path) will produce a preliminary final score subject to a recounting process. Different types of voting equipment are used to speed up the ballot emission and counting process, but the technologies implemented do not capture the power of the information revolution. There have been several studies on voting systems using computer technologies especially the Internet. These studies caution against the security risks in tasks of election process: voters authentication, ballot secrecy, communications confidence. Different cryptographic algorithms are suited to provide or enhance security levels [1].

The emerging Information Society has enabled people in the developed countries to perform several of their activities in a direct, electronically automated and efficient way. To keep up with the need to provide citizens with the ability to benefit from services over networks, as well as to reduce the cost and bureaucracy of public administration, governments are striving to transfer an increasing number of their activities to the new medium.

E-voting can be an efficient and cost effective way for conducting a voting procedure and for attracting specific groups of people (e.g. young or disabled electors) to participate. The term e-voting (electronic voting) is used hereby to denote a voting process, which enables voters to cast a secure and secret ballot over a network [2].

1.2 Motivation

Elections are the essential part of every democratic society and organization. Hence it is very important to hold up as many elections as possible. Unfortunately, elections come with big administrative efforts and costs.

In order to circumvent the drawbacks of conventional “physical elections”, a lot of people suggested the use of cheaper online voting systems. Today a lot of alternative e-voting systems have been proposed. Some of them are already used .unfortunately most of them do not even fulfil the most basic security requirements, whereas other systems are provably secure, but completely impractical. Furthermore a few e-voting scandals destroyed the peoples trust into these voting schemes.

As a result, we have the need for a new easy to use, practical, secure and transparent online voting scheme, that can not only convince experts but also citizen, lawyers, ... In this thesis such a new easy to use, secure and transparent online voting system is proposed. The new scheme is furthermore secured against very dangerous, man in the middle. [3].

1.3 Problem statement

As information technology evolves over time, the need for a better, faster, and more convenient and secure electronic voting is essential requirement. The security is one of the main concerns, such as authentication, confidentiality, integrity and non-repetition. It is not an easy task to achieve secure e-voting

1.4 Objectives

The main objectives of this study are:

1-Study the electronic voting system from the security perspective

2-Develop a general electronic voting system that provides privacy, transparency, integrity, with accuracy, verifiability, Mobility, with authentication mechanism, integrity, non-repetition mechanism and trusted electronic voting and in addition to the requirement for electronic voting

3-The privacy, authentication, integrity, non-repetition mechanisms for the e-voting system

1.5 Research methodology

In the proposed model that E-Voting system, using AES algorithm to encrypt and decrypts vote, and using MD5 algorithm for integrity shown in Figure(1-1) and also using UML technique for analytical purpose.

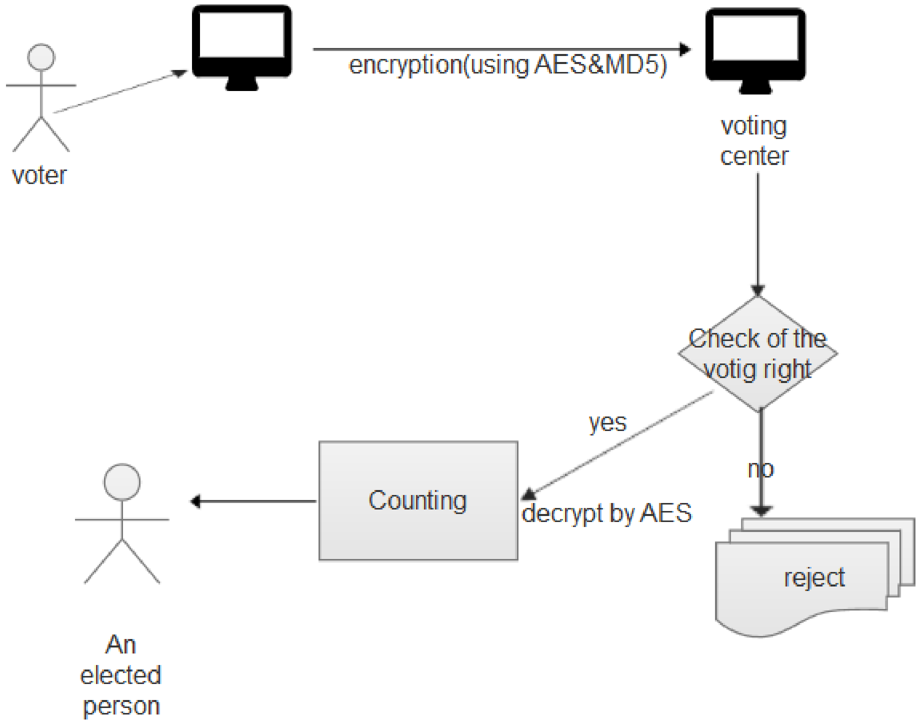


Figure (1-1) methodology

1.6 Thesis Organization

This thesis consists of five chapters, Chapter one is the introduction that present the problem and the solutions. Chapter two describes the related work of e-voting schemes currently available. Chapter three presents the proposed e-voting scheme. Chapter four discusses the testing and results of the proposed scheme. Finally Chapter five gives the conclusions and Future work

CHAPTER Two

LITERATURE REVIEW

CHAPTER TWO

LITERATUREREVIEW

2.1 Background

For a democratic country public opinion is the most important determinant to establish a government and voting is the process through which people display their opinion and help to setup a democratic government. So the voting system should be reliable, accurate and it must be transparent. Traditionally, the process of voting is quite cumbersome because voter must come in person to Vote. This problem results in the low participation rate of voting. Vote-by-mail can cater for certain voters such as those who live in sparsely populated areas and who work far away from the voting centers. However, this method is time-consuming and cumbersome for the authority to manage since it requires extra work to send, collect and count the ballots manually electronic voting system or Electronic Voting System (EVS) can overcome those problems. EVS is expected to make our modern social life more convenient, efficient and inexpensive. By using EVS in national election, a voter can vote from his home or office. EVS must meet security requirements such as confidentiality, integrity, authentication, and verifiability. This is because EVS is more vulnerable than traditional voting due to the nature of digital processing of election data which can be easily manipulated, hence may result in widespread fraud and corruption. In this research, we have implemented a prototype of an EVS, called E-Voting, that satisfies four security requirements for a safe election. This is achieved by designing some protocols that guarantee those requirements. We believe that E-Voting can reduce human error in voting process by providing easy-to-use user interface.

2.1.1 Internet

Internet was invented by the department of defense, United States of America in 1960s as a communication network for defense research purposes; no one could have foreseen how it would transform society three decades later. Today, the internet has become a part of the daily life of many people around the world. Explosive growth in Internet usage and rapid development of e-commerce in the private sector have put growing pressure on the public sector to serve citizens electronically, which is often known as the e-government and this initiative is taken to provide public services and to empower citizens and communities through information technology, especially through internet. The Internet provides low-cost and efficient solutions for the exchange of information but there are serious security and trust issues that need to be addressed when dealing with sensitive government information. The use of Internet for mission-critical transactions must provide solutions to ensure that only authorized government officials have access the sensitive data. It must also address concerns about reliability, origin and integrity. In addition to the security issues, the use of Internet for critical government services must provide trust and integrity in both the data and the transactions [4]

2.1.2 E-Government

E-government applies concepts of electronic commerce (e.g. information and marketing through web sites, selling to customers on-line) to government operations. E-Government is simply defined as the use of information and communication technology (ICT) to improve the process of government. In a narrow sense it is sometime define as citizens' services, re-engineering with the technology, or procurement over the Internet. Digital (electronic) government is about transforming government service delivery through the use of technology. United nation (UN) world report on public sector says that 90 percent of member countries have operational government websites. E-Government is the use of technology to enhance the access to and delivery of government services to benefit citizens, business partners and employees .Users (Citizens) expect the same level of services from government as they have from the private sector and the government itself expects more effective, productive and improved services as the private sector is. Having this all in common the e-Government still differs in its uniqueness of its interaction between government and its users. [4]

2.1.3 E-Services

The use of electronic delivery for government information, programs, strategies and services can named as e-services. These are available on-line “24h/7days”. It also refers to Electronic Service delivery (ESD) and such expression as ‘one-stop service centers”. The latter describes situation in which citizen needs are met through a single contact with the government. In many cases it assumes a modernized front office but not necessarily redesigned back office capacity. At the same time, e-services emphasize innovative forms of citizen involvement and offer services that demonstrate serious valuation of citizens as customer of administration. The strategic challenge is to deliver services to members of public along with dimensions such as quality, convenience and cost. [4]

2.1.4 E-Democracy

This is the most difficult to generate and sustain feature of e-Governance. In framework of e-democracy ICT is used as an instrument to help set agendas, establish priorities, make important Policies and participate in their implementation in a deliberative way. It refers to activities that Increase citizen involvement including virtual town meeting, open meeting, cyber campaigns, feedback polls, public surveys and community forums (such as through e-consultation, e-voting). In short, if e-government is successfully implemented new empowered citizens may emerge .They are able to form the Internet biased alliance to respond to various issues and achieve Economic and social objectives[4]

2.2 The importance of voting

It gives you the power to create change .Voting gives you the power to decide how the Countries is run. If you have a complaint about the way the country is being run, voting is a way simple you can make a change. You can choose a candidate to suit to your views and they can represent your views at a national and local level. It’s not the only way to participate but it’s the quickest and easiest way!

2.3 Traditional Voting

Traditional Voting shall be defined as the use of paper ballots, traditional voting in all Countries elections shall occur as follows:

1. The voter shall present picture identification to an election clerk and sign their full name and current address. The election clerk shall not return the student's picture identification until after he/she has returned their ballot.

2. The student will have to furnish their student identifications number if they do not use their Countries Eagle card.

3. The election clerk shall give the voter a ballot and direct the voter to a voting booth.

4. Upon receiving the complete ballot, the election clerk shall drop the

Ballot into the ballot box while in the presence of the voter.

5. It is the responsibility of the election clerk to regularly check and remove any campaign paraphernalia left at or around the polling booth.

2.4 Some of the problems facing traditional voting

1-traditional voting, makes voters go to a specific place at a specific time in order to vote

2-more physical infrastructure: When running on a traditional voting. You need of paper, printing, physical urns or staff may, therefore, lead to a lower monetary investment.

3- Slow and difficult votes tally: Since the tally in traditional voting is tally by human counting that it will in most cases run slower than a count carried out by machines, so the results of your election will be not available sooner.

4- Vote may be vote more than one

6- Modifying   vote totals

2.5 electronic voting system

An electronic voting (e-voting) system is a voting system in which the election data is recorded, stored and processed primarily as digital information

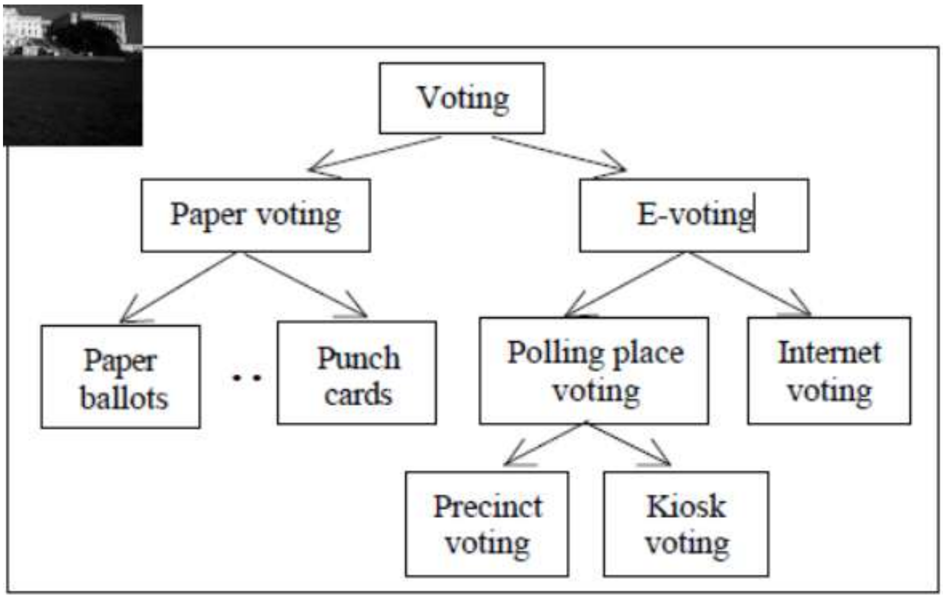


Figure (2-1) display Traditional Voting and E-voting [5]

2.5.1 Electronic voting

(e-voting) is any voting method where the voter’s intention is expressed or collected by electronic means. There are considered the following electronic voting ways. [6]

2.5.2 Kiosk voting

Means the use of dedicated voting machines in polling stations or other controlled locations. Voters mark their choice electronically (perhaps on touch sensitive screen) rather than on paper ballot. The votes are counted on individual machines, known as Direct Recording Electronic (DRE) machines, and the votes cast are transferred to the central tallying point by unspecified means. A ballot paper can be printed and retained in confidence in a ballot box as an additional check. [6]

2.5.3 Remote electronic voting

Is the preferred term for voting that takes place by means from any location. This could include the use of the Internet, text message, interactive digital TV or touch tone telephone.

2.5.4 Internet voting

(I-voting) is a specific case of remote electronic voting, whereby the vote takes place over the Internet such as via a web site or voting applet. Sometimes also used synonymously with Remote Electronic Voting. That usage is however deprecated and it will be used instead as a strict subset of remote electronic voting.

In this work, we use the term e-voting with the specific meaning of Internet voting. If we use it as a general term, then we specify the meaning. Despite the privileges and benefits of the electronic voting program, there are difficulties and gaps facing the electronic voting program, which is:

1-Technological gap: Disparity between expectations from software/hardware and the performance being delivered (security flaws, etc.).

2-Socio-technical gap: Difference between social policies (laws, codes, etc.) and computer policies (procedures, functionalities, etc.).

3-Social gap: Difference between social policies and human behavior (equipment misuse, etc.).

2.6 Benefits of electronic voting systems

They could lead to increased voter turnout [5], thus supporting democratic process.

1-They could give elections new potential (by providing ballots in multiple languages, accommodating lengthy ballots, facilitate early and absentee voting, etc.) thus enhancing democratic process.

2-They could open a new market, thus supporting the commerce and the employment

2.7 Voting systems design principles

2.7.1 Generality

Universal suffrage is a generic principle for democratic elections, requesting that every eligible voter can participate in the election process, and nobody can be excluded or discriminated. The consequences deriving from this principle are the following:

1. Every voter has the right to participate in an election process.
2. The ability to participate in an election process (eligibility) must be founded on and be controllable by the law.
3. Voting possibilities and technologies should be accessible by every voter.
4. e-voting should be considered as an alternative way of exercising one's voting rights.
5. The democratic principle (i.e. every eligible voter should be included in the election process) leads to publicly available appropriate infrastructure (e.g. public internet kiosks, internet voting in state offices, etc.), in order to allow citizens to exercise their rights. E-voting improves the generality of election procedures by providing an additional option of participation to the electoral process. [7]

2.7.2 Freedom

The principle of free election requires that the election process take place without any violence, coercion, pressure, manipulative interference, or any other influence, exercised either by the state or by one or more individuals. Regarding postal voting, the voter may be asked to sign a declaration on the vote-by-mail certificate, promising that she has filled out the ballot personally. Providing such a signature is not trivial in e-voting. E-voting procedures pose new threats to the freedom and integrity of a voter decision, beyond those that postal voting does. For example, in the case of the workplace, even if the employer, the supervisor or a colleague are not standing over the shoulder of the e-voting employee, system administrators can monitor or record the activity at each workstation and obtain a copy of the ballot.

UN coercibility and prevention of vote buying and extortion can be ensured by an e-voting system designed so that no voter can prove that she voted in a particular way (UN traceability on the part of the voter). Since the employment relationship is not power-balanced, it is suggested to avoid e-voting from the workplace. In any case, coercion can hardly be prevented by technology alone. One solution to this is to develop a publicly accessible infrastructure, allowing voters to exercise their rights free of the coercion of any third party. The freedom of decision may be violated if a propaganda message is blended on the computer screen while the voter is casting her electronic ballot. In current election schemes it is not allowed to advertise in (the vicinity of) the polling place. The e-voting procedure should also make the advertisement of political entities on the e-voting website technically infeasible. The free expression of the preferences of the voter should be ensured. Therefore, the possibility for casting a consciously invalid (or “white” paper) ballot should be ensured. [7]

2.7.3 Equality

The requirement of equality, in the context of general elections, is a reflection of the generic principle of equality and constitutes one of the cornerstones of modern democracies. Under the principle of equal suffrage, two major requirements are identified:

1) Equality regarding the participating political parties and candidates

2) Equality regarding the voting rights of each voter.

A requirement deriving from the principle of equality is that electronic ballots should be edited and displayed in a way analogous to that used for the paper ballots. Electoral equality requires that there are no meaningful deviation 542 Principles and requirements for a secure e-voting system Dimitris A. Grizzlies between the printed ballot and its electronic equivalent look. Furthermore, the placement of electronic ballots in the voting site (i.e. on a computer screen) should ensure equal accessibility.

Thus, the “look and feel” of the e voting website and ballots should not favor or discriminate against any of the participating parties.

Because of the emerging characteristics of the technology, the right to equal accessibility to the voting process should become the right of equal accessibility to election technology. As a result, a non-discriminating procedure should be offered to the voters, allowing them to efficiently exercise their voting rights with no obstructions. Equal accessibility means, also, that the system should be user-friendly and independent of a voter education, age, and physical condition (to accommodate physically disabled voters).

An e-voting system should ensure that the one voter - one vote principle is respected, that is only eligible voters can vote, only once, either online or off-line. Therefore, an e-voting system should be designed in such a way as to prevent the:

1) Duplicability of the vote (either by the voter herself or by someone else)

2) Reusability of the vote (either by voting online more than once or by voting both online and offline)

3) Modification of the cast vote (after a voter has dispatched her vote).

2.7.4 Directness

The principle of direct election requires that there can be no intermediaries in the process of voting decision. This principle may be also adapted to fit with an e-voting procedure. The relevant requirement is that each and every online ballot is directly recorded and counted.

A problem may arise in case the voting period differs from the voting procedure (on-line or off-line) used to cast the vote. Online voting results may influence the outcome of the entire election process and limit the integrity and legitimacy of the whole process. To avoid this, a system can be developed allowing the recording and maintaining of the cast vote, while prohibiting any counting before the end of the (off-line) voting period

2.7.5 Democracy

A democratic e-voting system should at least meet the requirements of a traditional election system. However, additional requirements should be also met, particularly due to the remote nature of e-voting. These requirements pertain to the preservation of attributes and properties such as transparency, accountability, security, accuracy and legitimacy of the system.

E-voters should be able to understand how the elections are conducted. The traditional voting procedures operate in a way that is transparent to both, the voters and the other election actors. On the contrary, e-voting procedures are not transparent because the average voter does not have the knowledge necessary to understand how the system works. Therefore, in e-voting much more trust in the technology used and the persons involved (election officials, technology providers, etc.) is be required by the voters.

Verifiability conflicts with transparency. An e voting system should allow its verification by voters (individual verifiability) or by election officials, parties and independent observers (institutional verifiability). However, verifiability is orthogonal to secrecy (confidentiality), in the sense that individual verifiability (i.e. the possibility of a voter to verify his vote and receive confirmation about casting and counting of the vote) is conflicting with the requirement of secrecy (as a condition of free choice).

Accountability is an additional requirement of an e-voting system, which is meant as the logging and monitoring of all operations related to e-voting. Reliability and security requirements are derived by the democratic need, to ensure that the outcome of the election reflects correctly the voter will. A reliable system should ensure that the outcome of the voting process corresponds to the votes cast. The ballot that is transmitted to the voting counting equipment should be an accurate and not modifiable copy of the voter choice (integrity). Moreover, it should be infeasible both to exclude a valid vote from the tabulation and to validate a non-valid on

2.8 General description of e-voting systems

Generally, e-voting systems consist of six main phases:

1-The voters' registration is a phase to define voters for the e-voting system and give them authentication data to log into the e-voting system

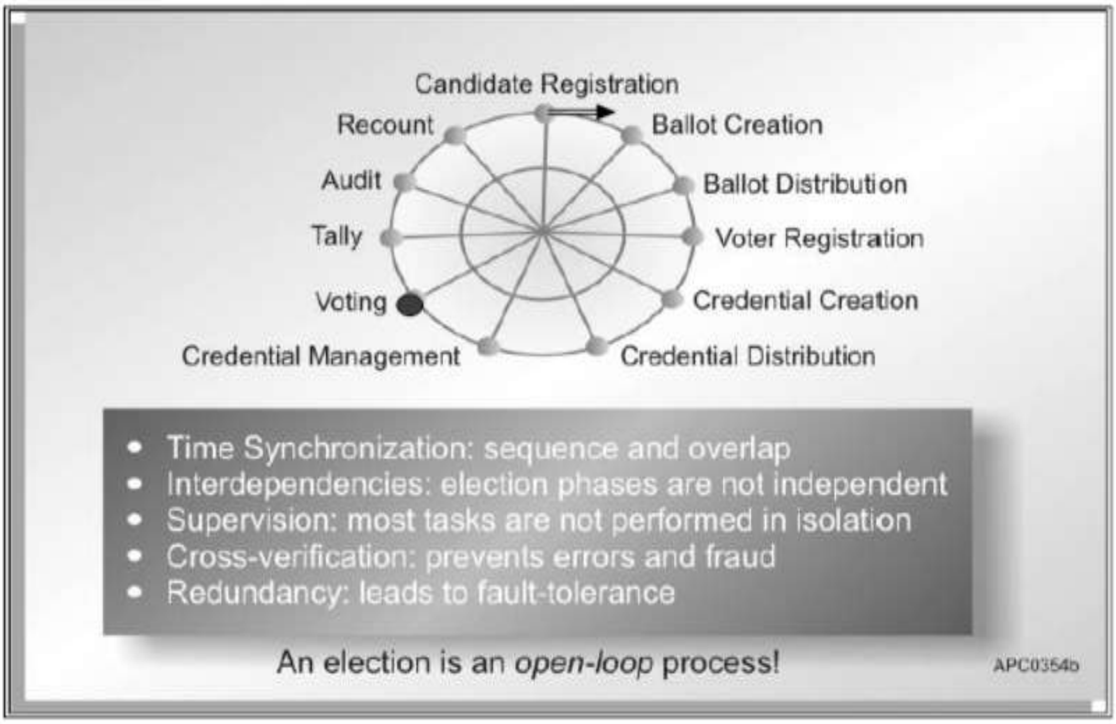
2-The authentication is a phase to verify that the voters have access rights and franchise.

3-The voting and vote's saving is a phase where eligible voters cast votes and e-voting system saves the received votes from voters.

4-The votes' managing is a phase in which votes are managed, sorted and prepared for counting.

5-The votes' counting is the phase to decrypt and count the votes and to output the final tally.

6-The auditing is a phase to check that eligible voters were capable to vote and their votes participate in the computation of final tally. Additionally there are some other e-voting specific rules verified in this phase



- Time Synchronization: sequence and overlap
- Interdependencies: election phases are not independent
- Supervision: most tasks are not performed in isolation
- Cross-verification: prevents errors and fraud
- Redundancy: leads to fault-tolerance

An election is an *open-loop* process!

Figure (2-2) display Time-sequence of a typical voting process. [5]

2.9 Security voting systems technologies

1-Cryptography (Homomorphic encryption, digital signatures, blind signatures, trusted third

Parties, digital certificates, etc.)

2-Antiviral software 3-Firewall

4-Biometric 5-Smart cards

2.10 Strengths associated with e-voting

1- Faster vote count and tabulation.

2- More accurate results as human error is excluded.

3- Efficient handling of complicated electoral systems formulae that require laborious counting procedures.

4- Improved presentation of complicated ballot papers.

5- Increased convenience for voters.

6- Potentially increased participation and turnout, particularly with the use of Internet voting.

7- More attuned to the needs of an increasingly mobile society.

8- Prevention of fraud in polling stations and during the transmission and tabulation of results by reducing human intervention.

9- Increased accessibility, for example by audio ballot papers for blind voters, with Internet voting as well for housebound voters and voters from abroad.

10- Possibility of multilingual user interfaces that can serve a multilingual electorate better than paper ballots. [8]

2.11 Voting systems design criteria

1. Authentication: Only authorized voters should be able to vote

2. Accuracy: Voting systems should record the votes correctly

3. Uniqueness: No voter should be able to vote more than once

4. Integrity: Votes should not be able to be modified without detection

5. Verifiability: Should be possible to verify that votes are correctly counted for in the final tally

6. Auditability: There should be reliable and demonstrably authentic election records

7. Reliability: Systems should work robustly, even in the face of numerous failures

8. Secrecy: No one should be able to determine how any individual voted

9. Non-Coercibility: Voters should not be able to prove how they voted

10. Flexibility: Equipment should allow for a variety of ballot question formats

11. Convenience: Voters should be able to cast votes with minimal equipment and skills

12. Certifiability: Systems should be testable against essential criteria.

13. Transparency: Voters should be able to possess a general understanding of the whole process

14. Cost-effectiveness: Systems should be affordable and efficient

2.12 Estonian e-voting system

Estonia is the first country in the world to introduce nation-wide Internet voting. The Estonian Internet voting system has been under development since 2002 with the final pilot held at the end of 2004. In 2005 the system was used for the first time for local government council elections.

In 2007, for the first time in the world, it was possible to vote online during Estonian parliamentary elections. A total of 30 275 out of 940 000 registered voters used that opportunity and cast their ballots via the Internet. I-voting system is gaining popularity. In 2009, 58 669 voters used I-voting during the European Parliament elections, which is 15% of all the people who voted. In the local government council elections in October 2009, a total of 104 413 persons used I-voting. The percentage of i-votes among all the votes cast was 15.7%. The new record for I-votes was set during the parliamentary elections in March 2011, when 140 846 people cast their votes electronically, which is 24.3% of all the people who voted. In 2014, during the European Parliament elections, a third of voters participated in elections over the Internet – from 98 different countries.

Internet voting is meant to supplement, not to replace the traditional methods of voting. The idea is to give voters the opportunity to vote from the location of their choice (home or office), without the necessity of going to the polling station. Therefore remote voting is used.

Estonia takes the security of Internet voting very seriously. Voting over the Internet is as secure as ballot voting. A variety of technical, administrative, legal and other measures are used to safeguard the integrity of the system and most importantly, the security and secrecy of the votes.

Electronic voting takes place during advance polls (the tenth to fourth day before Election Day) and government-issued ID-cards are used for voter identification.

If an ID-card is used, the voting procedure is as follows:

1. The voter inserts the ID-card into a card reader and opens the webpage for voting
2. The voter verifies him/herself using the PIN1 of the ID-card.
3. The server checks if the voter is eligible (using the data from the population register).
4. The voter is shown the candidate list of the appropriate electoral district.
5. The voter makes his/her voting decision, which is encrypted.
6. The voter confirms his/her choice with a digital signature (by inputting the PIN2-code).
7. The voter receives a notice on the computer screen that the vote has been accepted.

During the vote count, the voter's digital signature is removed and at the final stage, the members of the National Electoral Committee can collegially open the anonymous I-votes and count them.

Since parliamentary elections in 2011, it is also possible to use a mobile phone to identify oneself for I-voting. This is even more convenient, since then the voter doesn't need an ID-card reader for his/her computer. A mobile phone with the respective SIM card acts as a card and a card reader at the same time. However, one still needs a computer for the voting procedure.

If mobile-ID is used, the voting procedure goes like this:

1. The voter opens the webpage for voting.
2. The voter enters his/her mobile number into the computer. After that a control code is sent to the voter's mobile phone by SMS.
3. The voter identifies him/herself by entering the PIN1 code into the mobile phone.
4. The voter is shown the candidate list of the appropriate electoral district on the computer screen.
5. The voter makes his/her voting decision, which is encrypted. A control code is once again sent to the voter's mobile phone by SMS.

6. The voter confirms his/her choice with a digital signature by entering the PIN2-code into the mobile phone.

7. The voter receives a notice on the computer screen that the vote has been accepted.

There is the possibility of an electronic re-vote – an I-voter can electronically cast his/her vote again and the previous vote will be deleted. The traditional means of voting (with a paper ballot) is given priority. Should the voter go to a polling station during advance polls and cast a vote, his or her i-vote shall be deleted. On Election Day, the registered i-vote cannot be changed or made void. After Internet voting ends and advance polls close (4 days before Election Day), the list of voters who have voted electronically is comprised and sent to polling stations. The polling station marks on the voter list that the person has already voted. This prevents them from voting for a second time on Election Day. [9]

2.13 Related Work

Asghar et.al. [10] Had Present a paper-based voting method that attempts to achieve the privacy of voters and election universal verifiability and integrity with only paper ballots and without using any cryptography method. The voting procedure is easy and it needs only selecting the intention of voter over screen of an electronic device. The rest of the voting procedure will be carried out by the device. Voter gets a receipt that can be used to verify that his vote has been counted in final tally as he intended. However the receipt cannot help voter to reveal who he voted for. Also vote selling or coercion is not possible even with the voter’s cooperation. The ballot in our voting method has two side, one positive and one negative. Ballots have been prepared for voting in prepackaged form (i.e. 5 ballots per package). Some bubbles of each ballot are prefilled in random way. Numbers of positive and negative filled bubbles are equal with each other and also for each candidate in a package. For example if every package has 30 filled bubbles and if there are three candidates, there would be 10 filled bubbles for each candidate in a package. As it is clear half of those are positive and the other half are negative. The procedure of One Ballot voting is as follows: Voter puts the ballot inside of an electronic device and then he chooses his candidate on the device screen. Then device print another ballot exact same as the original one by one difference; the device fills one positive bubble or unfills one negative bubbles for the selected candidate. First action can be done on the original ballot but the second one needs to print new ballot inevitably. Then device makes a copy from new ballot as voter's receipt and transfers original ballot to the ballot box. After election, there will be a copy from all of ballots in a public board

Subariah Ibrahim et.al. [11] had Present a paper based developed an electronic voting system, E-Voting for a general election. E-Voting system employs cryptographic techniques to overcome the security issues in the election process. In this system, voter's privacy is guaranteed by using a blind signature for confidentiality and voter's digital signature for voter's authentication. E-Voting is implemented by employing Java socket technology and Bonncy Castle cryptography provider. The provider, which is an open source library, is used to provide the secure communication channel. The voter's private key for digital signature is protected by using password-based encryption with SHA and Two fish-CBC algorithm so that only valid voter can use it.

Baisa et.al. [12] had Present a paper. The aim of this paper is to present multilayer secured, internet based voting system using biometric and wavelet based image watermarking. Strongly secured watermarking technique for voter's color photograph in YCgCb color space is processed by embedding voter's fingerprint as watermark. The watermark embedding is done securely through number of levels. This technique yields Peak Signal to Noise Ratio (PSNR) up to 54.26 and Normalized Correlation (NC) equals to 1 indicating exact recovery of fingerprint. The complete system is maintained 'user friendly'.

Yifan [13] had Present a paper. The aim of this paper is to present design implemented a new web voting system software through PHP and JavaScript programming languages. A security analysis, software performance analysis and evaluation .On account of the pseudonymous of Bitcoin address and the openness of the block chain, which is consistent with part of e-voting requirement. This paper proposed an e-voting protocol based on block chain by using the ring signature algorithm. The requirements can be satisfied with ballot-privacy, individual verifiability, eligibility, completeness, uniqueness, robustness, and coercion-resistance.

Electronic voting (e-voting) is a symbol of modern democracy activities. Due to the high ballot privacy and variability, e-voting system has been booming in the recent years. Particularly, Bitcoin, a digital currency system based on the cryptography, is highly open and transparent for the individual transaction. In other words, anyone can access to the transaction contents via block chain. Besides, regarding to anonymous way it trades, the transaction of Bitcoin is untraceable

CHAPTER Three

METHODOLOGY

CHAPTER THREE

METHODOLOGY

3.1 Introduction

In this chapter brief description of proposal methodology used in this thesis. The proposed model depends on two hybrid algorithms that are combined with each other to provide a secure voting system. The AES algorithm [15] used to provide confidentiality of data and MD5 for integrity. Figure (3.1) show proposed framework for e-voting.

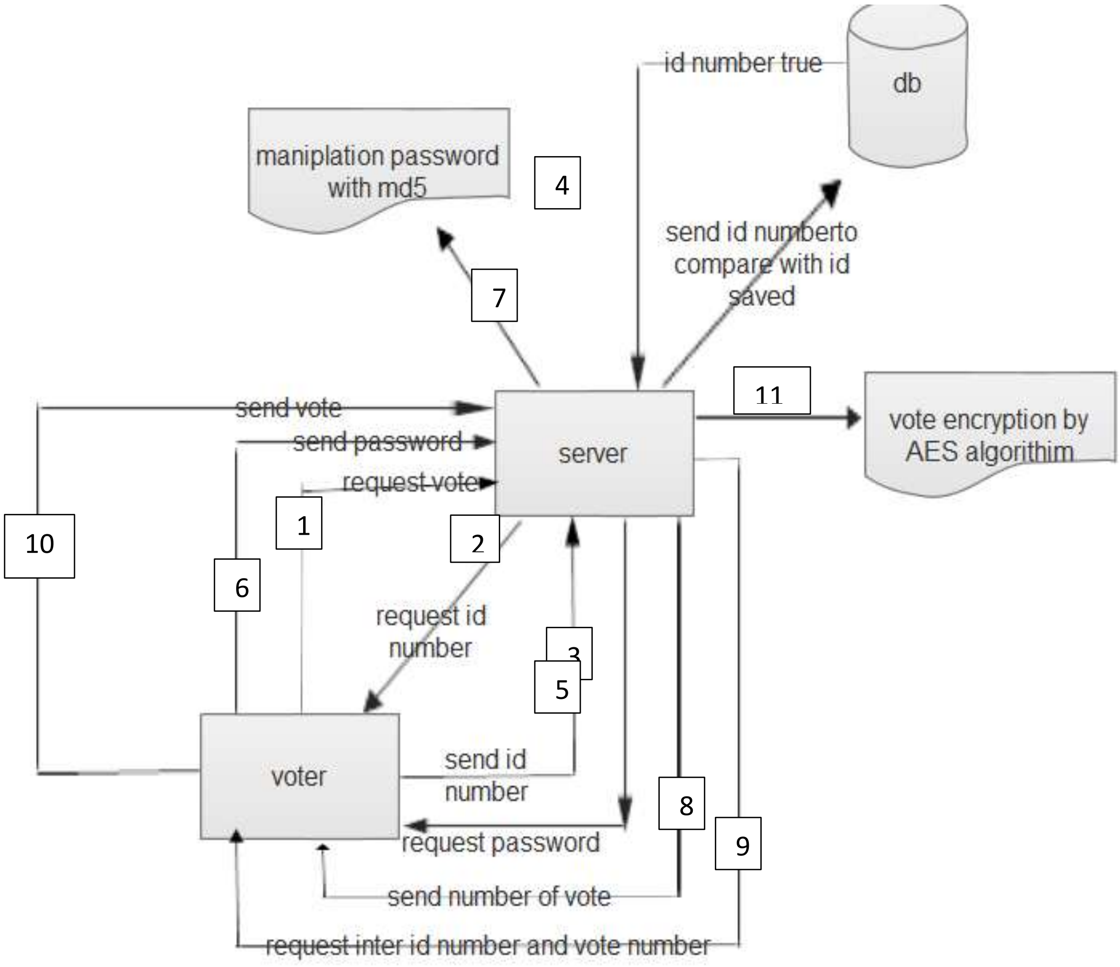


Figure (3.1) proposed framework for e-voting

3.2 Architecture

The system architecture contains two main component voter and server shown in figure (3.1)

Voter:

Step 1: Enter the national number

Step 2: Enter the password

Step 3: Enter the national number along with the voting number

Step 4: Choose favorite candidate and vote for him

Server:

Step 1: request from voter enter the national number

Step2: asked from voter enter the password and handles the password with the MD5 algorithm

Step 3: Give voter his / her voting number

Step 4: request from voter enter both the national number and the voting number together

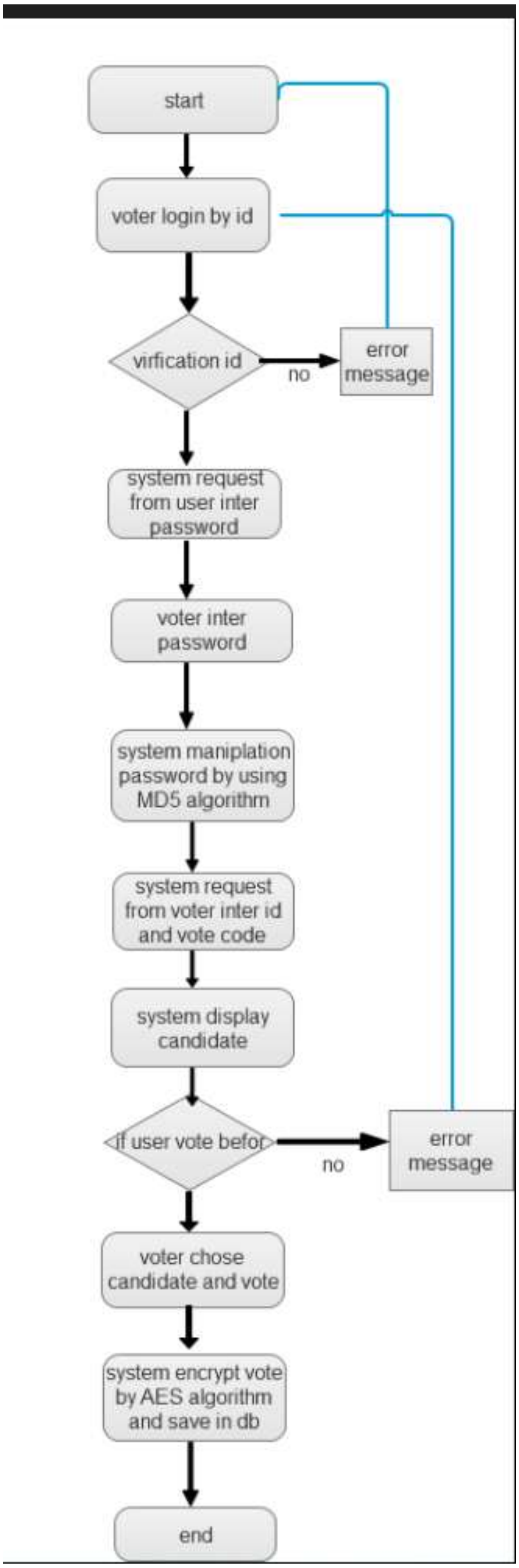
Step 5: Verify that the voter has not already voted

Step 6: encrypt vote with the AES algorithm and saves the vote in the database

Step 7: display the results.

3.3 Flow chart diagram

Figur (3-2) illustrating the sequence of electronic voting operations. First, the voter enters the national number and checks it. The system then asks the voter to enter the password and verify it if the password is correct and approval of the national number allows the voter to enter. If one of the conditions is violated, the system sends a message and stops the operation the system offers the voter a list of candidates so that the voter can choose


start
voter login by id
virfication id
no
error message
system request from user inter password
voter inter password
system maniplation password by using MD5 algorithm
system request from voter inter id and vote code
system display candidate
if user vote befor
no
error message
voter chose candidate and vote
system encrypt vote by AES algorithm and save in db
end

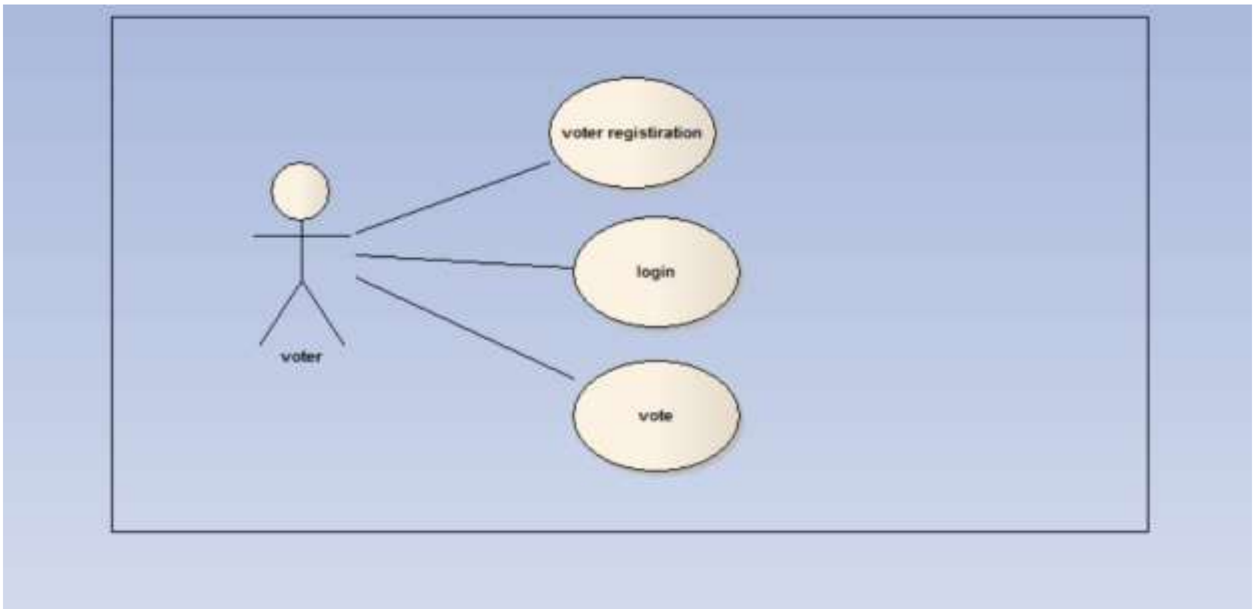
Figur (3-2) electronic voting process

3.4 UML analysis

In this section discuss the analysis process of the proposed model (electronic voting). The analysis process performed by the Unified Modeling Language in two parts: use case diagram and sequence diagram.

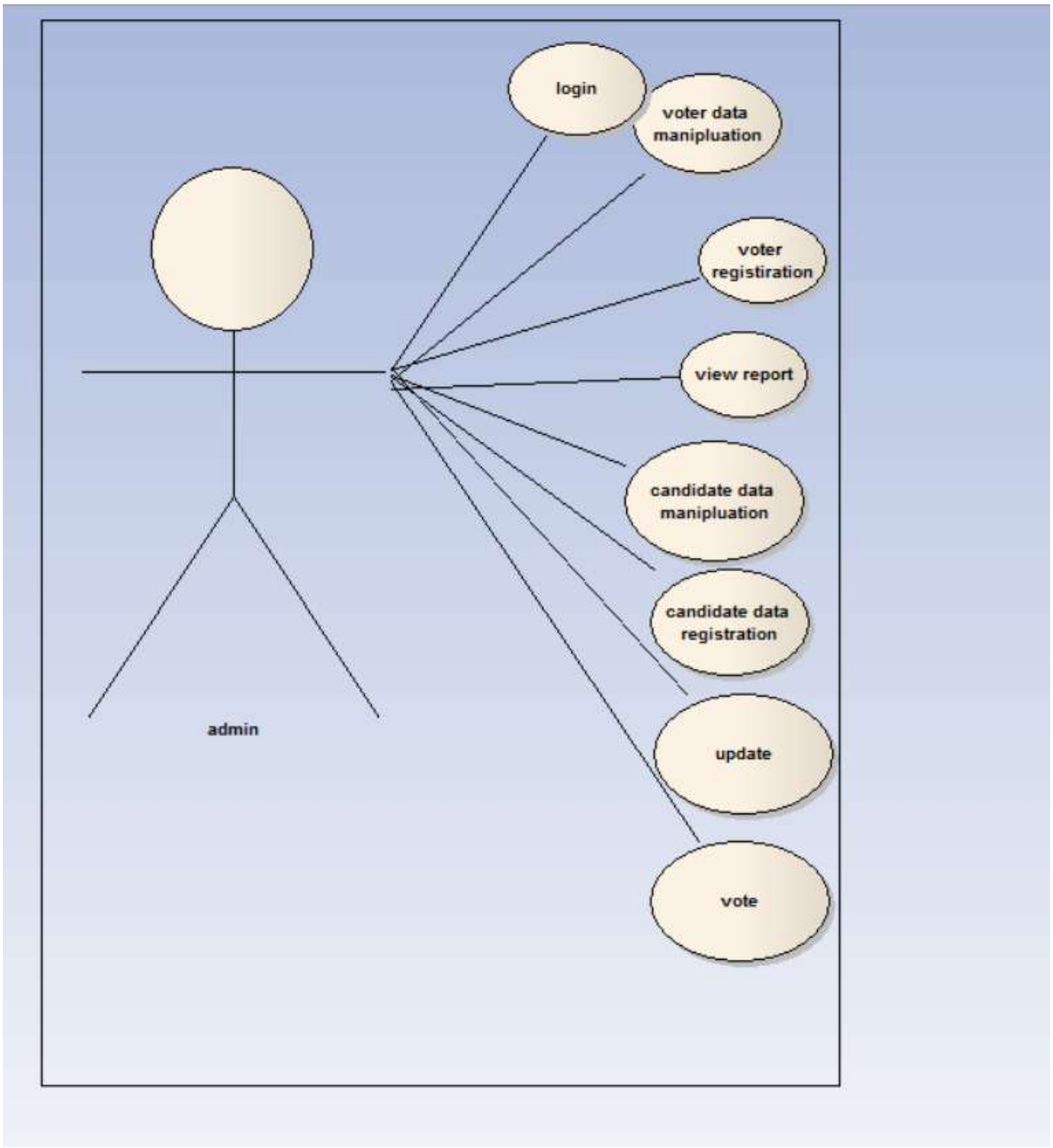
3.4.1 Use case diagrams

Figur (3-3) shows the voter as actor takes the simple steps listed above and shows them as actions the voter might perform. These procedures are the process of registration, entry and voting.



Figur (3-3) use case of voters login

- Figure (3-4) shows the admin as a actor . The diagram takes the simple steps listed above and shows them as actions the admin might perform. These procedures are the process of registration, voter registration, candidate registration, voter and candidate data collection, and the process of update and voting



Figur (3-4) use case of admins procees

3.4.2 Sequence diagrams

Sequence diagrams demonstrate the behavior of objects in a use case by describing the objects and the messages they pass. The diagrams are read left to right and descending. The example below shows an object of class 1 start the behavior by sending a message to an object of class 2. Messages pass between the different objects to the object of class 1 receives the final message.

Figur (3-5) showing the voter registration process The voter sends the national number of the system The system checks the national number and asks the voter to enter the password The voter sends the password The system receives the password and checks if it is identical If the registration process is not identical, the system sends a message

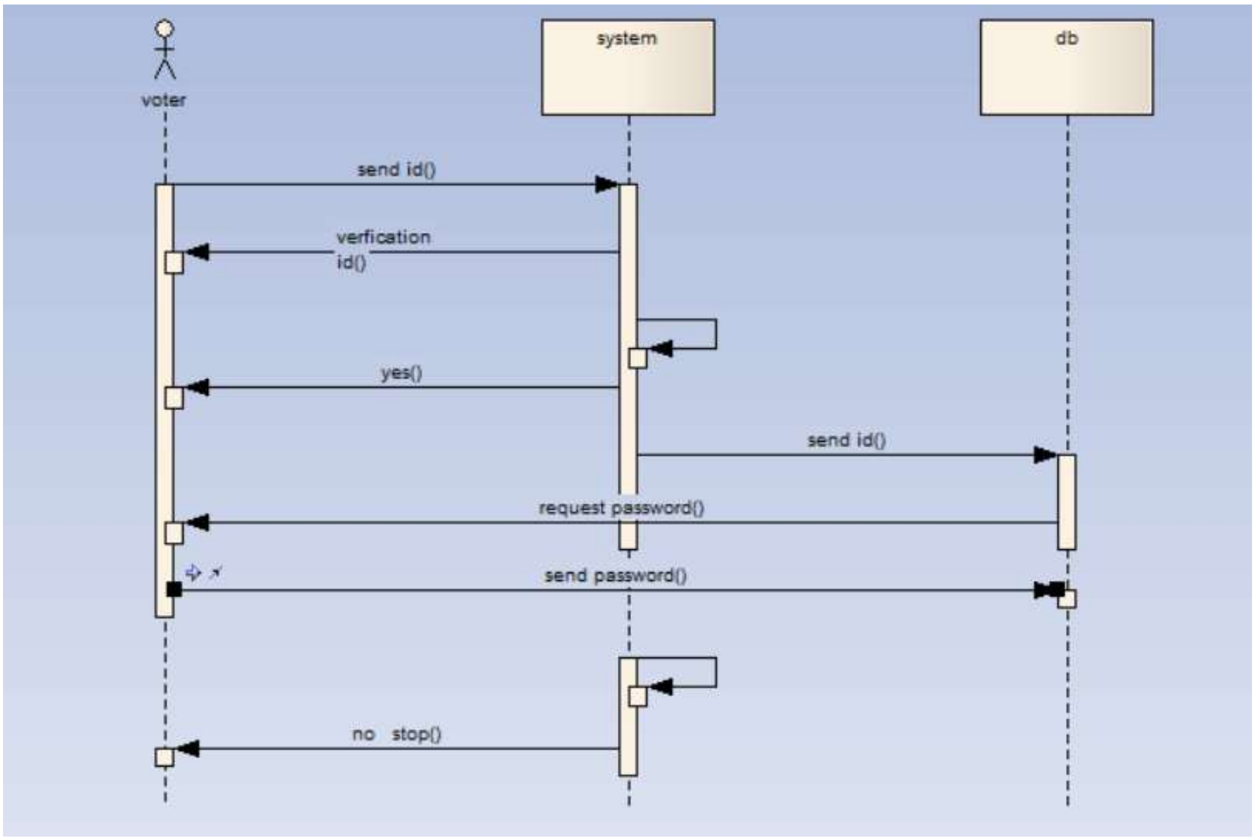


Figure (3-5) sequence of login

Figure (3-6) explain the voter shall send the national number of the system and the password. The system shall verify that the voter has already been registered at the registration stage. If he is not registered, the system shall send the voter a message. If he has registered, the system shall present the list of candidates so that the voter Of the vote If the voter has voted before this time, the system prevents him from voting again and finally the system encrypts the vote and saves it in the database and sends a message to the voter that the vote has been successful

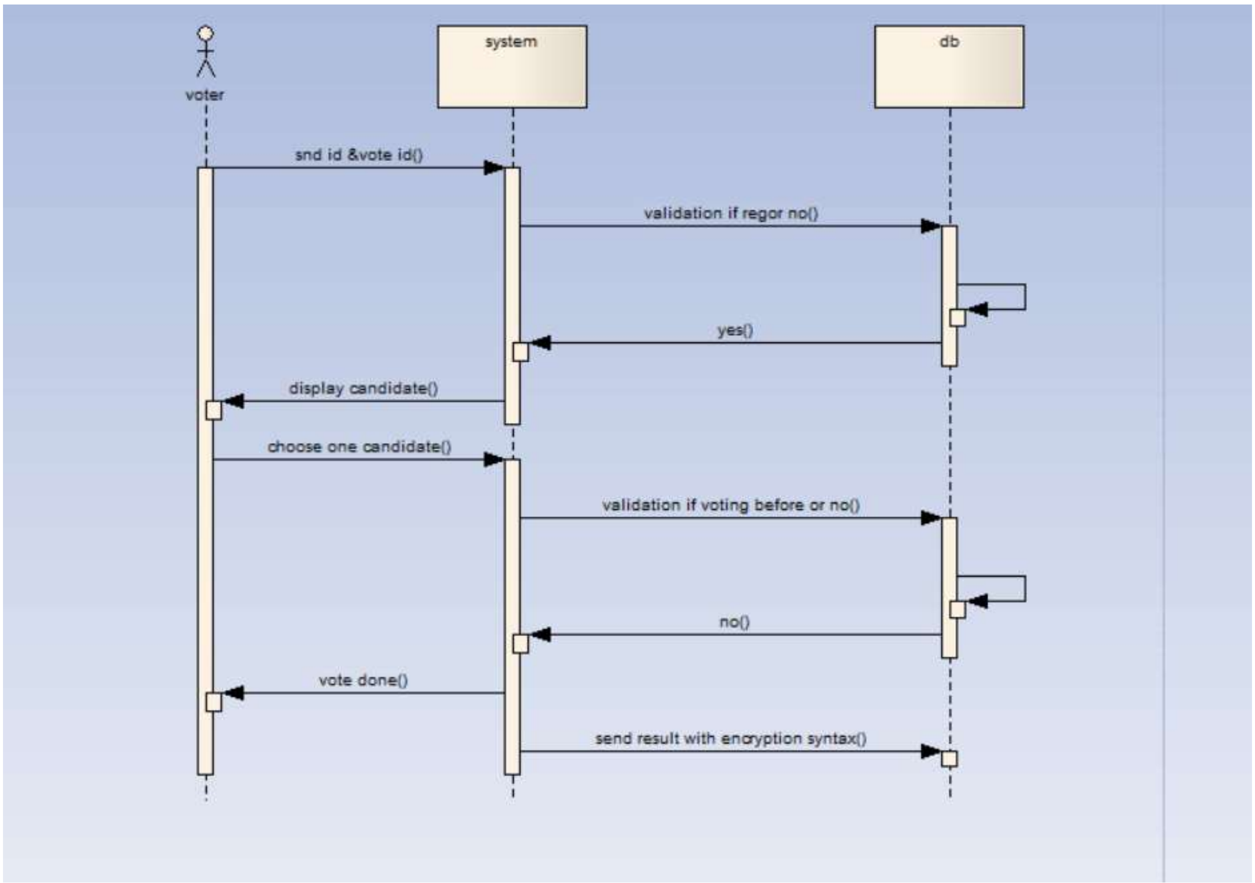


Figure (3-6) sequence of voting

CHAPTER Four

IMPLEMENTATION

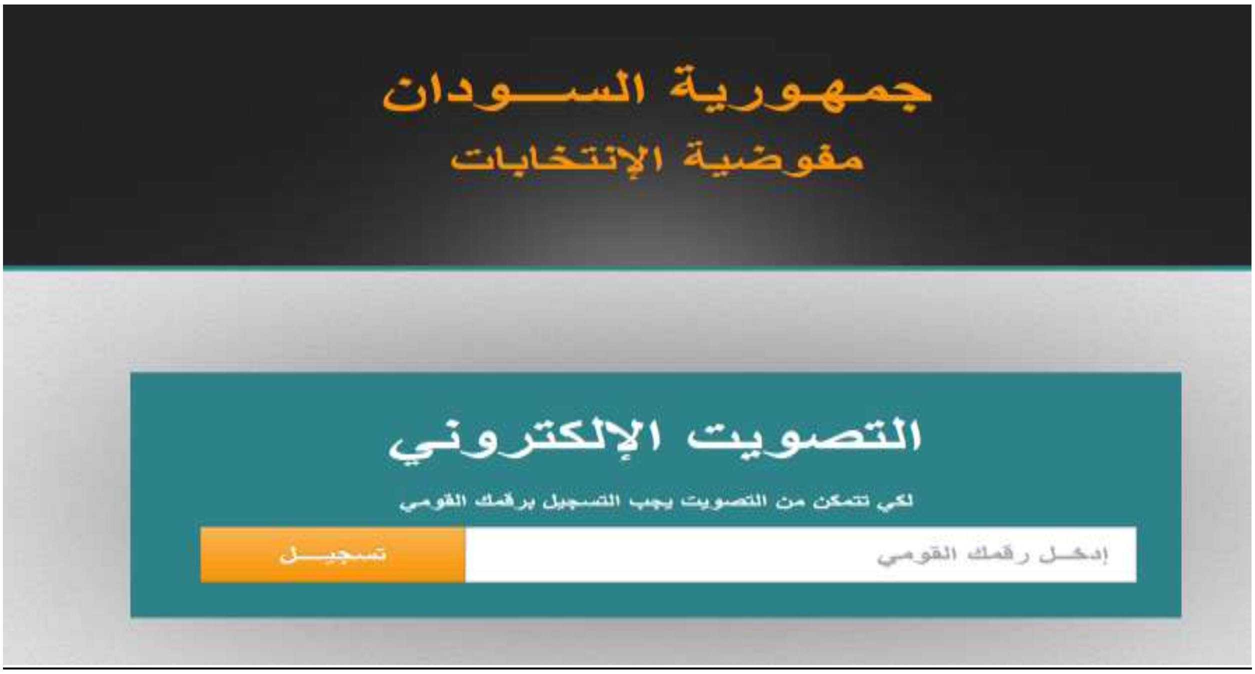
CHAPTER FOUR

IMPLEMENTATION

4.1 Introduction

This chapter display implementation and security analysis .the first section shows the sequence of screens and the function of each screen in the system and second section the display the attacks and the test whether this system has achieved security and integrity and confidentiality and enjoy the security analysis.

Figure (4-1), system requires from voter to enter the national number to verify his age based on the civil registry data stored in the databases and then pass it to the server



جمهورية السودان

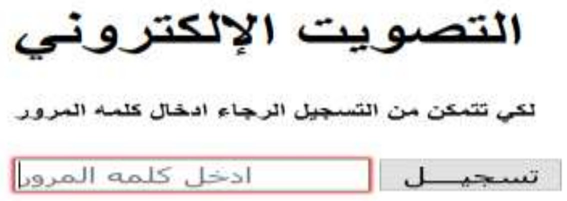
مفوضية الإنتخابات

التصويت الإلكتروني

لكي تتمكن من التصويت يجب التسجيل برقمك القومي

Figure (4-1) login screen

Figure (4-2), system request the voter to enter the password and after voter entering the password, the system uses the Hash algorithm to achieve integrity and verify the integrity of the data then the system to configure the voting number

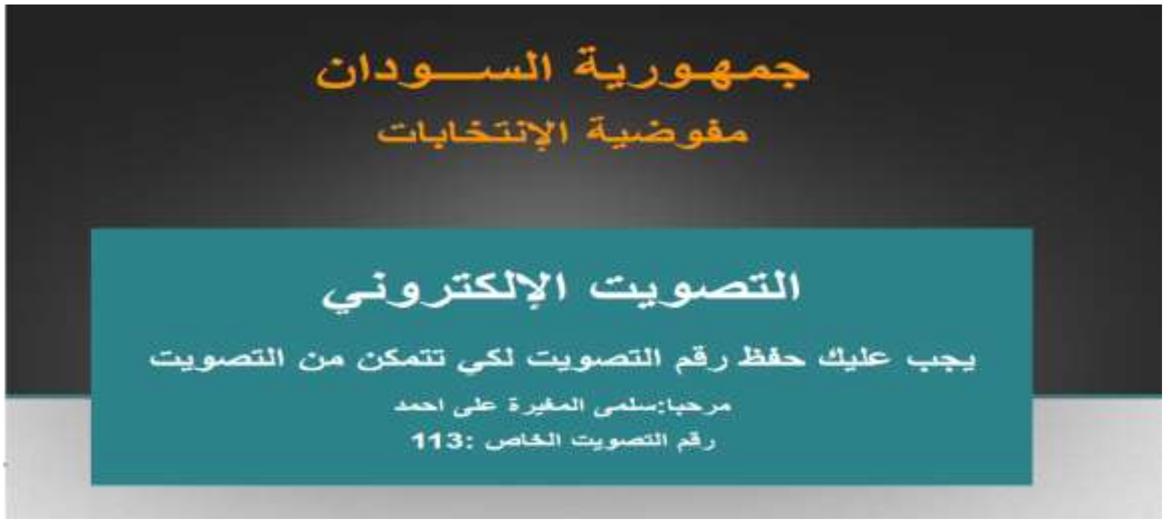


التصويت الإلكتروني

لكي تتمكن من التسجيل الرجاء ادخال كلمه المرور

Figure (4-2) password screen

Figure (4-3), system sends the voting number coupled with the name of the voter after the process of Hash in the previous step after that the voter presses the voting icon so that the voter can vote



جمهورية الســـودان

مفوضية الإنتخابات

التصويت الإلكتروني

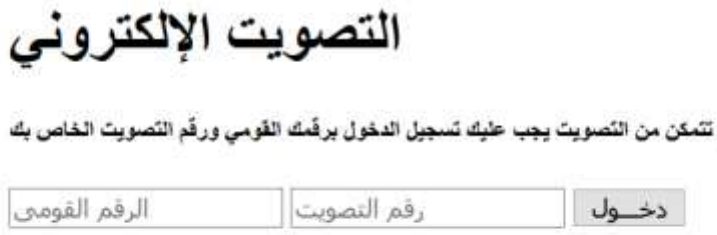
يجب عليك حفظ رقم التصويت لكي تتمكن من التصويت

مرحبا:سلمى المغيرة على احمد

رقم التصويت الخاص :113

Figure (4-3) special voter number page

Figure (4-4) system requires the voter to enter his national number and voting number so that the system can present the candidates to the voter and allow him to choose the candidate and vote for him.

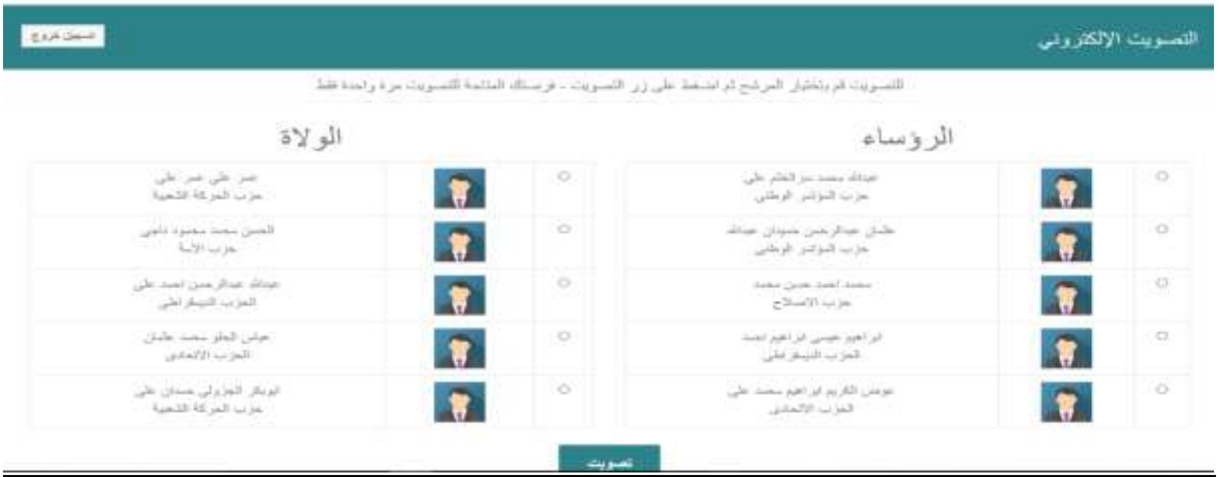


التصويت الإلكتروني

لكي تتمكن من التصويت يجب عليك تسجيل الدخول برقمك القومي ورقم التصويت الخاص بك

Figure (4-4) voting login page

Figure (4-5) candidates are displayed and the voter selects best candidate and make votes. The system uses the AES algorithm so that the voter's voice is encrypted and stored in data base



للتصويت قم باختيار المرشح ثم اضغط على زر التصويت - فرصتك المتاحة للتصويت مرة واحدة فقط

الرؤساء

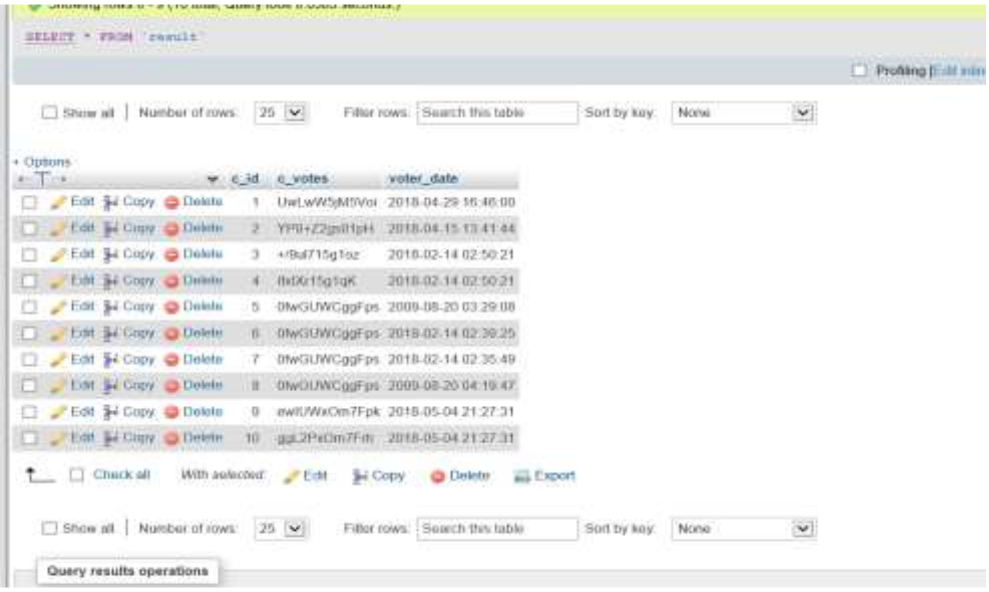
○	عبدالله محمد عزالختم علي حزب المؤتمر الوطني
○	عثمان عبدالرحمن حمدان عبدالله حزب المؤتمر الوطني
○	محمد احمد حسن محمد حزب الاصلاح
○	ابراهيم عيسى ابراهيم احمد الحزب الديمقراطي
○	عوض الكريم ابراهيم محمد علي الحزب الاتحادي

الولاة

○	عمر علي عمر علي حزب الحركة الشعبية
○	الحسن محمد محمود دانفي حزب الأمة
○	عبدالله عبدالرحمن احمد علي الحزب الديمقراطي
○	عباس الحلو محمد عثمان الحزب الاتحادي
○	ابوبكر الجزولي حمدان علي حزب الحركة الشعبية

Figure (4-5) vote page

Figure (4-6) result of the vote and is encrypted in the database the encrypt data using Advance Encryption Standard (AES), which is symmetric block cipher using 128 block size [15]



Showing rows 0 - 9 (10 total, Query took 0.0003 seconds.)

```
SELECT * FROM `result`
```

□ Profiling [Edit inline]

□ Show all | Number of rows: 25 Filter rows: Search this table Sort by key: None

+ Options

	c_id	c_votes	voter_date
□ Edit Copy Delete	1	UwLwW5jM5Voi	2018-04-29 16:46:00
□ Edit Copy Delete	2	YP0+Z2gs01pH	2018-04-15 13:41:44
□ Edit Copy Delete	3	+/8ul715g1oz	2018-02-14 02:50:21
□ Edit Copy Delete	4	IfxDXr15g1qK	2018-02-14 02:50:21
□ Edit Copy Delete	5	0IwGUWCggFps	2009-08-20 03:29:08
□ Edit Copy Delete	6	0IwGUWCggFps	2018-02-14 02:39:25
□ Edit Copy Delete	7	0IwGUWCggFps	2018-02-14 02:35:49
□ Edit Copy Delete	8	0IwGUWCggFps	2009-08-20 04:19:47
□ Edit Copy Delete	9	ewlUWxOm7Fpk	2018-05-04 21:27:31
□ Edit Copy Delete	10	ggL2PxOm7Fm	2018-05-04 21:27:31

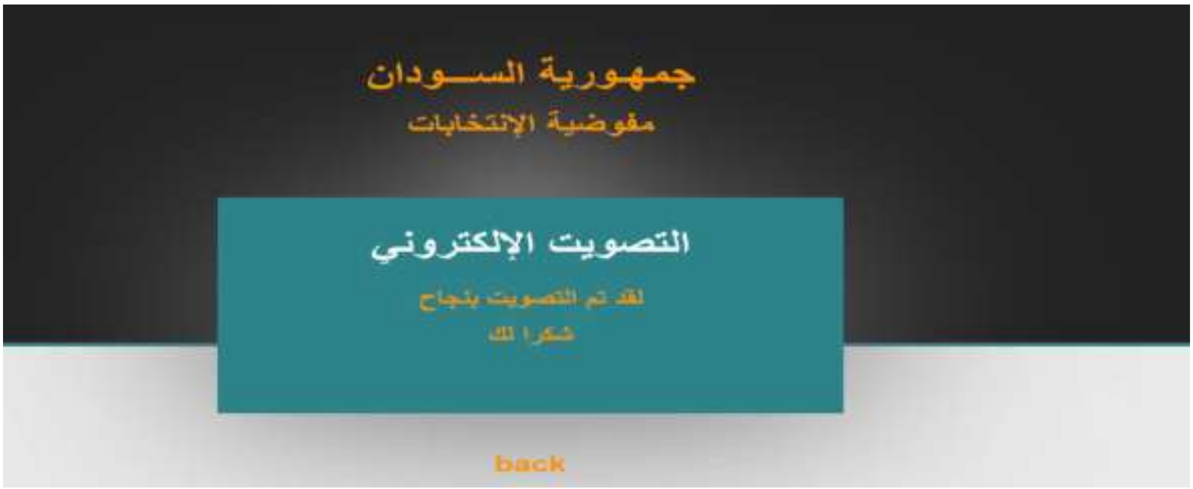
□ Check all With selected: Edit Copy Delete Export

□ Show all | Number of rows: 25 Filter rows: Search this table Sort by key: None

Query results operations

Figure (4-6) result encryption page

Figure (4-7) screen appears after the voter completes the voting process successfully



جمهـورية السـودان

مفوضية الإنتخابات

التصويت الإلكتروني

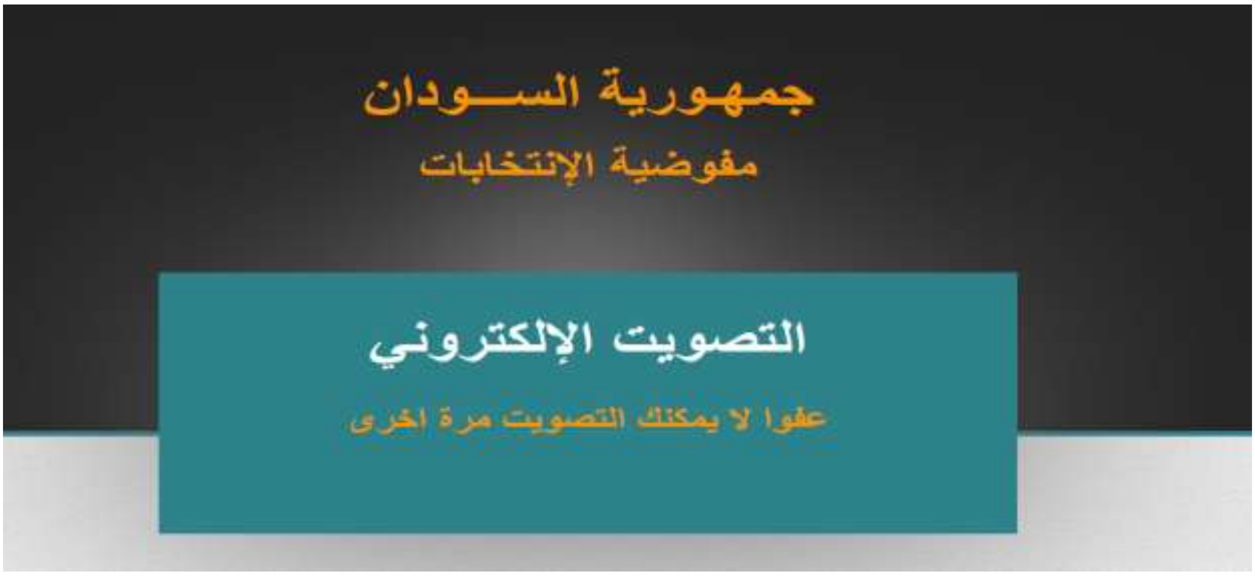
لقد تم التصويت بنجاح

شكرا لك

back

Figure (4-7) successful vote page

Figure (4-8) screen appears if the voter who has already voted before the vote tries again.



جمهـورية الســـودان

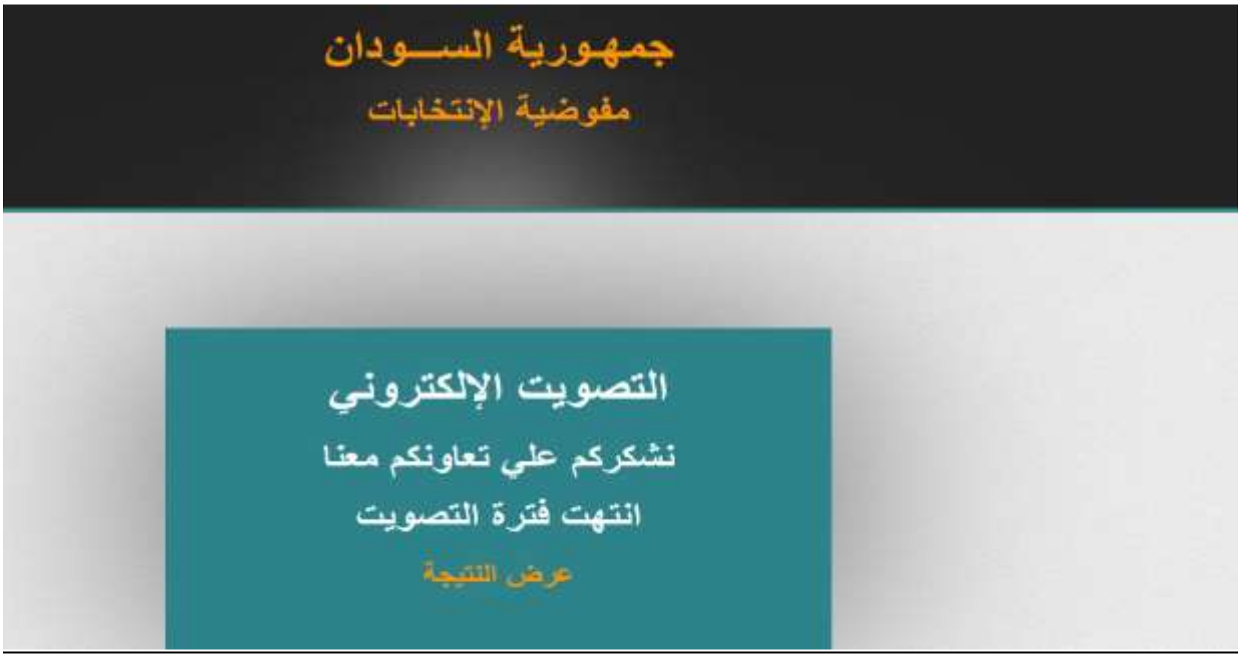
مفوضية الإنتخابات

التصويت الإلكتروني

عفوا لا يمكنك التصويت مرة اخرى

Figure (4-8) validation page

Figure (4-9) screen appears if the voting period is over and the voter decides to enter after the voting period because the system adheres to a fixed time for voting, where the voter can press the display button and the system displays the result to the voter



جمهـورية الســـودان

مفوضية الإنتخابات

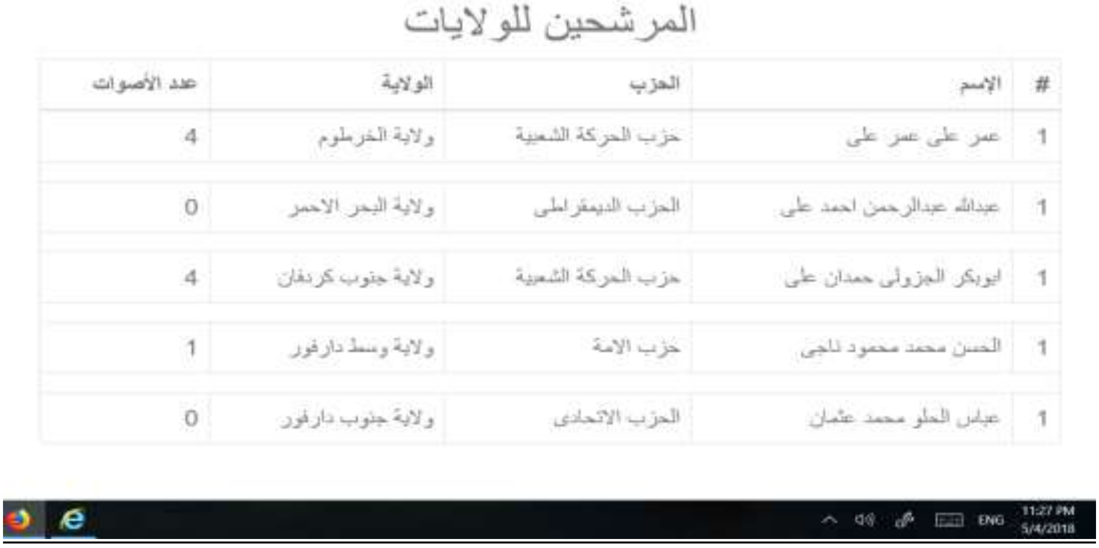
التصويت الإلكتروني

نشكركم علي تعاونكم معنا

انتهت فترة التصويت

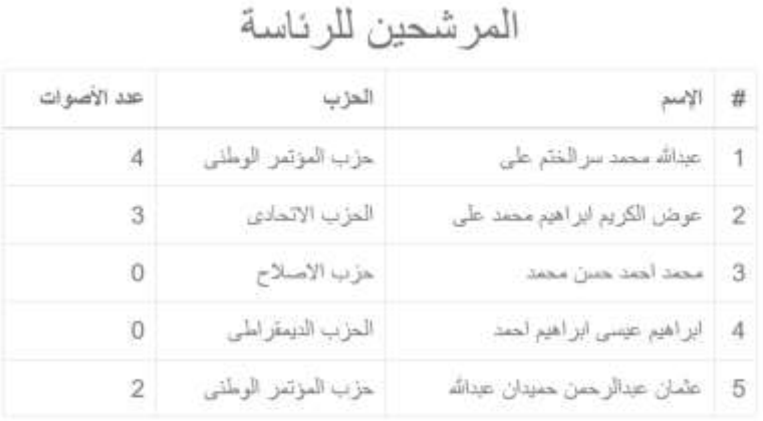
Figure (4-9) show result

Figure (4-10) result appears after the election period ends and after decoding the votes



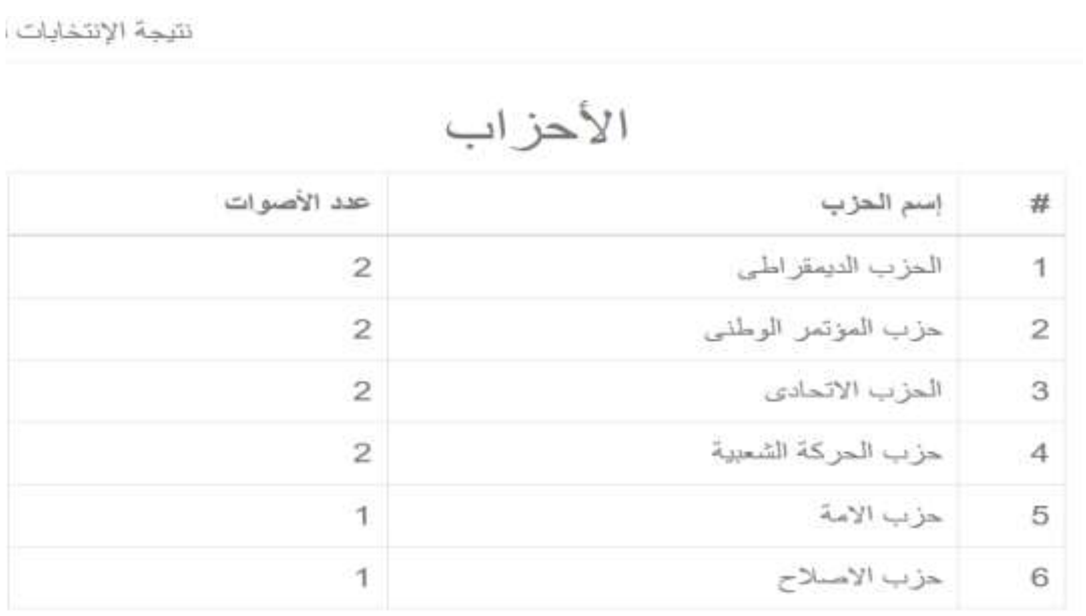
المرشحين للولايات

#	الإسم	الحزب	الولاية	عدد الأصوات
1	عمر على عمر على	حزب الحركة الشعبية	ولاية الخرطوم	4
1	عبدالله عبدالرحمن احمد على	الحزب الديمقراطى	ولاية البحر الاحمر	0
1	ابوبكر الجزولى حمدان على	حزب الحركة الشعبية	ولاية جنوب كردفان	4
1	الحسن محمد محمود ناجى	حزب الامة	ولاية وسط دارفور	1
1	عباس الحلو محمد عثمان	الحزب الاتحادى	ولاية جنوب دارفور	0



المرشحين للرئاسة

#	الإسم	الحزب	عدد الأصوات
1	عبدالله محمد سرالختم علي	حزب المؤتمر الوطنى	4
2	عوض الكريم ابراهيم محمد على	الحزب الاتحادى	3
3	محمد احمد حسن محمد	حزب الاصلاح	0
4	ابراهيم عيسى ابراهيم احمد	الحزب الديمقراطى	0
5	عثمان عبدالرحمن حميدان عبدالله	حزب المؤتمر الوطنى	2



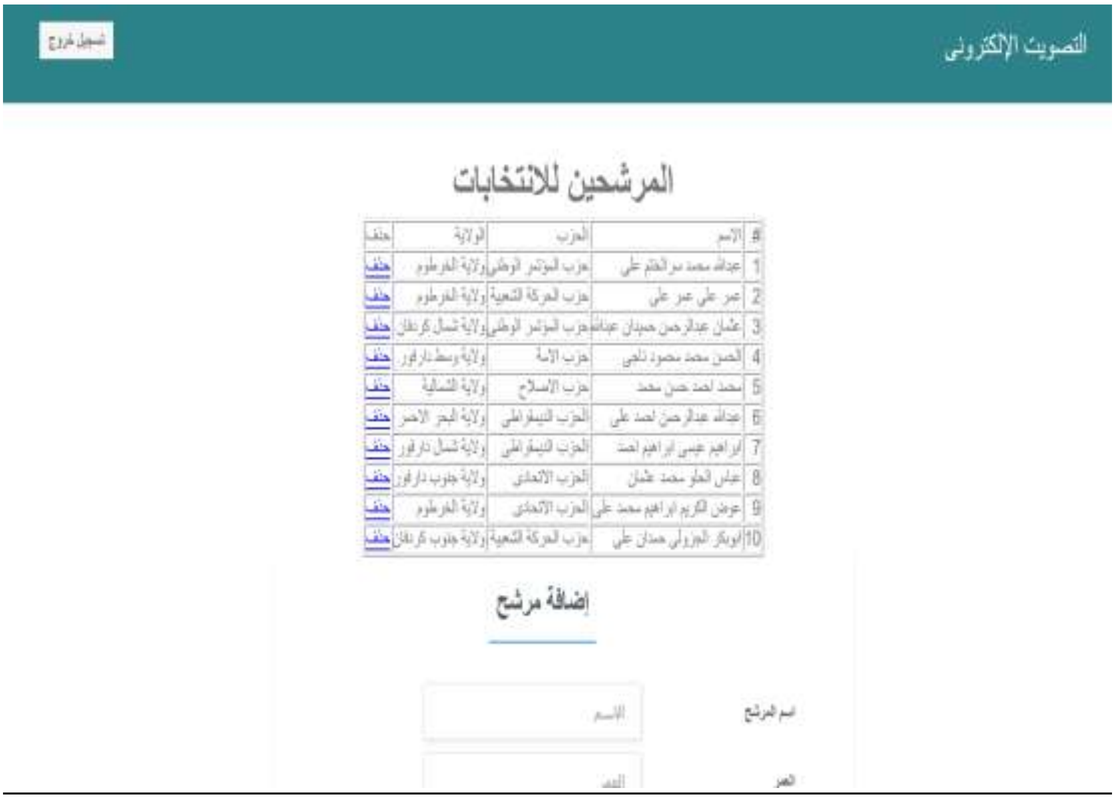
نتيجة الإنتخابات

الأحزاب

#	إسم الحزب	عدد الأصوات
1	الحزب الديمقراطى	2
2	حزب المؤتمر الوطنى	2
3	الحزب الاتحادى	2
4	حزب الحركة الشعبية	2
5	حزب الامة	1
6	حزب الاصلاح	1

Figure (4-10) result page

Figure (4-11) screen displays the work of the system administrator from registering, adding and deleting candidates for election



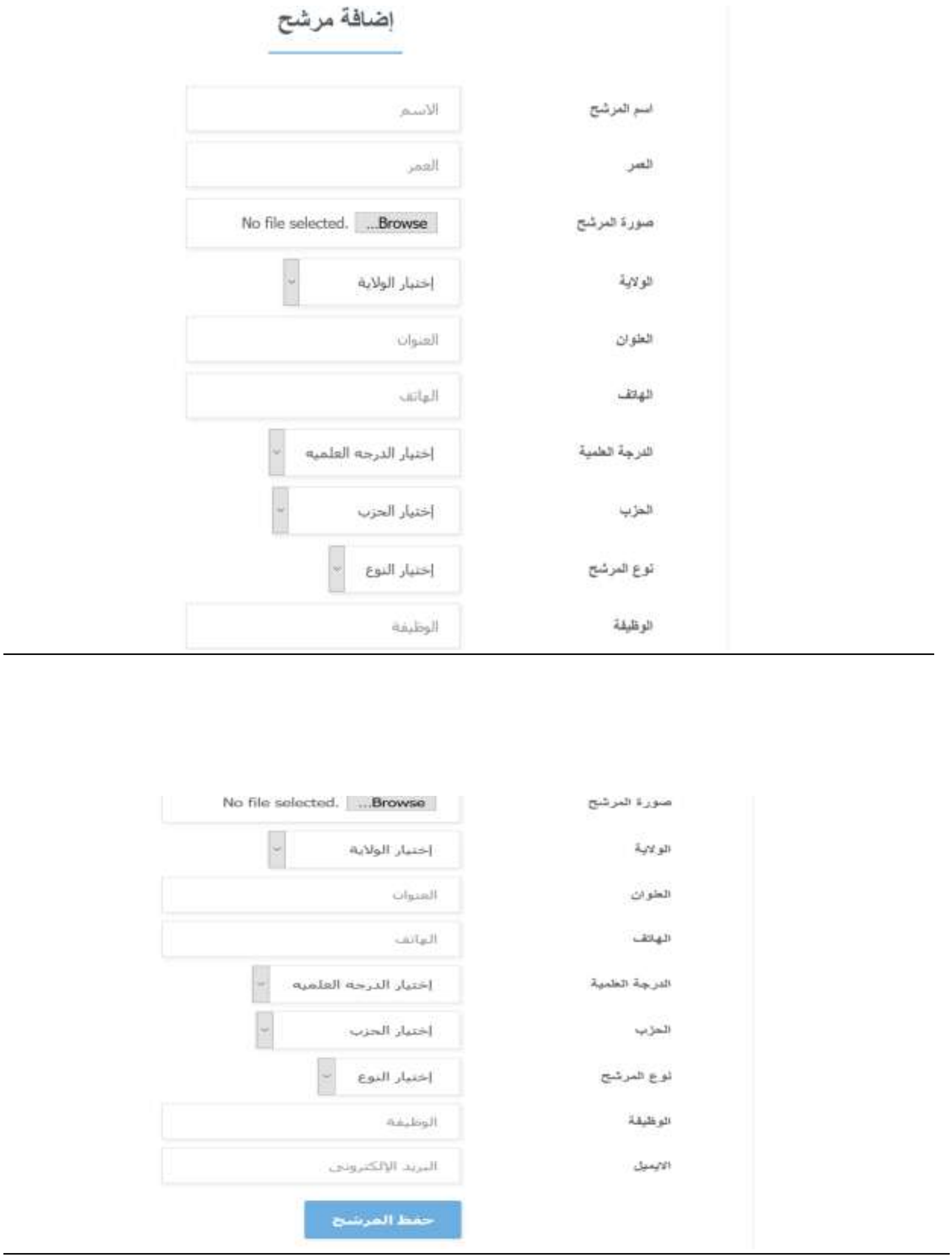
المرشحين للانتخابات

#	الاسم	الحزب	الولاية	حذف
1	عبدالله محمد سر الختم علي	حزب المؤتمر الوطني	ولاية الخرطوم	حذف
2	عمر علي عمر علي	حزب الحركة الشعبية	ولاية الخرطوم	حذف
3	عثمان عبدالرحمن حمدان عبدالله	حزب المؤتمر الوطني	ولاية شمال كردفان	حذف
4	الحسن محمد محمود ناجي	حزب الامة	ولاية وسط دارفور	حذف
5	محمد احمد حسن محمد	حزب الاصلاح	ولاية الشمالية	حذف
6	عبدالله عبدالرحمن احمد علي	الحزب الديمقراطي	ولاية البحر الاحمر	حذف
7	ابراهيم عيسى ابراهيم احمد	الحزب الديمقراطي	ولاية شمال دارفور	حذف
8	عباس الحلو محمد عثمان	الحزب الاتحادي	ولاية جنوب دارفور	حذف
9	عوض الكريم ابراهيم محمد علي	الحزب الاتحادي	ولاية الخرطوم	حذف
10	ابوبكر الجزولي حمدان علي	حزب الحركة الشعبية	ولاية جنوب كردفان	حذف

إضافة مرشح

اسم المرشح: الاسم

العمر: العمر



إضافة مرشح

اسم المرشح	الاسم
العمر	العمر
صورة المرشح	Browse... No file selected.
الولاية	إختيار الولاية
العنوان	العنوان
الهاتف	الهاتف
الدرجة العلمية	إختيار الدرجه العلميه
الحزب	إختيار الحزب
نوع المرشح	إختيار النوع
الوظيفة	الوظيفة

صورة المرشح	Browse... No file selected.
الولاية	إختيار الولاية
العنوان	العنوان
الهاتف	الهاتف
الدرجة العلمية	إختيار الدرجه العلميه
الحزب	إختيار الحزب
نوع المرشح	إختيار النوع
الوظيفة	الوظيفة
الايميل	البريد الإلكترونى

Figure (4-11) admin page

4.2 Security analysis

4.2.1 Spoofing and Man-in-the-Middle Attacks

In man-in-the-middle attacks the adversary interposes itself between legitimate communicating parties and simulates each party to the other. To simplify the discussion in the context of this article, we focus primarily on ways that a man-in-the-middle attack can subvert voter privacy, although the same general technique can be used for other attacks, such as vote buying.

The use of SSL does little to mitigate man-in-the middle attacks on privacy.

Any man-in-the-middle could act as an SSL gateway, forwarding application data between the voter and the vote server unaltered. The attacker could see all of the traffic by decrypting and re encrypting as communications pass between the two. In effect, the attacker would communicate using two SSL sessions, one between itself and the voter, and the other between itself and the vote server, and neither would know that there was a problem. These attacks are possible because the voter's browser does not verify that it is talking to the real serve web server—only that it is talking to someone in possession of a valid SSL certificate (who could be an attacker). Man-in-the-middle attacks also could be used to disenfranchise voters by spoofing the entire interaction with the voter. SERVE has some safeguards in place, but they assume the voter knows exactly what to expect from the voting experience; it is likely that an attacker could create a voting experience the voter

Would believe is real. Similarly, voters could be led to believe they registered successfully, when in fact they were communicating directly with an adversary instead of the legitimate registration server. The voters would discover when attempting to vote that they were not registered, but at that point there might be nothing they could do to resolve the situation. Perhaps the most serious consequence of man-in the-middle attacks is that attackers could engage in election fraud by spoofing the voting server and observing how a particular voter votes. If the vote is to the attacker's liking, the voter is redirected to SERVE's legitimate voting site. If the attacker does not like the vote, then the entire voting session is spoofed; in this case, the user thinks he or she has voted, but in fact the vote will not be received or counted by serve.

The proposed system (the electronic voting system) faced the center man's attack with several procedures. One of these procedures is that the system requires the voter to enter the password in Figure (4-2) password screen this password is not entered by anyone except the voter and the system manipulate password by using hash algorithm. The second procedure is that the system encrypts the voting process in in Figure (4-5) by using AES algorithm and saves it in the database.

4.3 Results

In (A Secure E-Voting System Using RSA and Md5 Algorithms Using Random Number Generators) proposed by N. Aditya Sundar [7] RSA and MD5 algorithms are used for encrypt/decrypt data. System provides a new e-voting system which fulfills the security requirements of e-voting process. System has three steps are required e-registration of voter, vote uploading and result display. System provides secure and efficient e-vote system

In our proposed system there are two types of encryption have been combined in order to exploit the advantages of each one to build a high security system. AES is used to encrypt sent data, exploiting its high encryption speed and its low RAM requirements. MD5 is used to protect the encrypted key or the data. The key and encrypted data are sent to the receiver and get decrypted by using the private. Comparing with system in [7] the proposed system is simple and fast with low computational requirements and provides reasonable system security.

CHAPTER Five

CONCLUSION & RECOMMENDATION

CHAPTER FIVE

CONCLUSION AND RECOMMENDATION

5.1 Conclusion

Voting system suffer many drawback such as electoral fraud, in order to overcome these problems, a proposed e-voting system is introduced, and the proposed voting system will be accurate, transparent, and faster and will ensure a single vote for a single person. Our proposed system has covered all of these issues successfully. Moreover this system will provide boundary less voting. Using AES and MD5 to provide confidentiality and integrity to voting process which will prevent modification in voting results also it secure the process of voting for individuals which reflect in confidence in our voting organization and hence provide more transparency to the electoral process at all stages. And for our political system.

A security analysis of the proposal was carried out against the expected attacks and gaps and the proposal was found to be safe and secure.

5.2 Recommendation

They are two areas in which this project could be extended .First implementations make an application in the phone from which the voter enters the system and send the message to the voter via telephone. The second implementations use is biometric for authentication instead of password.

REFERENCES

References

(1) Wanza, H. A. V. (1900). Cryptographic Algorithms for Communicating Results from Distributed Electronic Voting Systems.

(1) Wanza, H. A. V. (1900). Cryptographic Algorithms for Communicating Results from Distributed Electronic Voting Systems.

(2)Principles and requirements for a secure e-voting system. (2002), 21(6), 539–556.

(3) Grünauer, G. (n.d.). Proposal of a new online voting system, 1–14.

(4) Zafar, C. N., & Pilkjaer, A. (2007). MASTER ' S THESIS E-Voting in Pakistan.

(5) Security, C., Response, I., & Workshop, T. (2002). Secure Electronic Voting, (September).

(6) Triinu Mägi , Prof. Ahto Buldas , Faculty of Information Technology Practical Security Analysis of E-voting Systems(2007) TALLINN. UNIVERSITY OF TECHNOLOGY Faculty of Information Technology Department of Informatics

(7) N.Aditya Sundar[1],M.V.Kishore[2], Prof . Ch.Suresh[3] international Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 11 (2018) A Secure E-Voting System Using RSA and Md5 Algorithms Using Random Number Generators

(8) Paper, P. (2011). Introducing Electronic Voting

(9)Estonian internet voting system. (2009), 2004.

(10) Tavakoly, A., & Atani , R. E. (n.d.). A Secure Paper-Based Electronic Voting With No Encryption, 1–5.

(11) Ibrahim, S., Kamat, M., Salleh, M., Rizan, S., & Aziz, A. (2003). Secure E-Voting With Blind Signature, 193–197.

(12) Gunjal, B. L. (n.d.). SECURE E-VOTING SYSTEM WITH BIOMETRIC AND WAVELET BASED WATERMARKING TECHNIQUE IN YCgCb COLOR SPACE, 1–6.

(13) Yifan WU , david ,An E-voting system based on blockchain and ring signature .(2017), school of computer science ,University of Birmingham 54.

(14) https://www.techopedia.com/definition/3243/unified-modeling-language-uml

[15]Stallings, W. (2006). Cryptography and network security principles and practice (6th ed.).