# A Proposed Research Plan for M.Sc./PhD Degree By

**Monira Monir Haroon Khater**

Department of Computer Science,

Faculty of Computer and Information Sciences,

Benha University

B.Sc. of Computer Science

Faculty of Computer and Information Sciences, Benha University

2011

## Under Supervision of

**Prof. Dr. Hala Helmy Zayed**

**Assoc. Prof. Mazen Selim**

Department of Computer Science,

Faculty of Computers and Informatics,

Benha University

**Dr. Ayman M. AlAhwal**

Higher Institute for Engineering and Technology

## Thesis Title

# Secure E-Voting System

## Keywords

E-Voting, Authentication, Confidentiality, Integrity, Cryptography, Steganography, Security

# Abstract

With the rapid growth of the internet and technologies, E- voting appears to be a reasonable alternative to conventional elections. Various Information Security and Privacy Technologies including cryptography, steganography, and combination of both have been formulated in literatures to make democratic decision through e-voting systems to be fair and credible.

In practice, different data cryptographic standards like Data Encryption Standard (DES), and Advanced Encryption Standard (AES), Rivest, Sharim and Adleman (RSA) is needed to ensure the security of the votes and maintain the confidentiality and integrity. Homomorphic encryption scheme is used to encrypt all the votes and perform the calculation of the votes without revealing any information about them.

Current research focuses on designing and building "electronic voting protocols" such as zero knowledge authentication protocol, based on Diffie-Hellman key exchange algorithm, to ensure a mutual authentication between the election authority server and the voters.

This thesis proposes a new protocol that covers and maintains the security requirements which are: (authentication, privacy, integrity, Anonymity and non-repetition) of the voting process.

# 1. Introduction

The research on electronic voting (e-voting) is a very important topic for the progress of democracy. E-voting is the voting process held over electronic media, which enables voters to cast a secure and secret ballot over the Internet.

Traditional paper-based voting can be time consuming and inconvenient. Electronic voting not only accelerates the whole process, but makes it less expensive (reduced costs as the materials required for printing and distributing ballots as well as the manpower required to govern poll sites are considerably reduced).

Traditional election procedures cannot satisfy all of voter's demands. Simplicity is also necessary to ensure the participation of common people. Besides security and simplicity, other issues that need to be considered such reliability, convenience, flexibility, mobility and cost.

E-vote is more comfortable for the voters in that it allows voters to vote from any poll site in the country without the use of absentee ballots as well as it provides the authorities (Improve the registration process by allowing voters to check their registration status prior to vote and to centralize registration databases, to increase voter confidence and improve the voting experience. It also reduces the chances of the errors (Reduce the number of legitimate votes not counted by reducing the number of over-votes, and eliminating vote tampering. In addition to dominate the result of voting by the access that he or she has of the result before the end of Election Day.

If a secure and convenient electronic voting system is provided, it will be used more frequently to collect people's opinion for much kind of political and social decisions through cyber space. So that e-voting is very critical process and it requires several requirements to achieve secure e-voting system such as:

a. **Democracy:** A system is democratic if; it permits only eligible voters to vote and, it ensures that each eligible voter can vote only once.
b. **Accuracy:** A system is accurate if; it is not possible for a vote to be altered, it is not possible for a validated vote to be eliminated from the final tally, and it is not possible for an invalid vote to be counted in the final tally.
c. **Privacy:** A system is private if; neither election authorities nor anyone else can link any ballot to the voter who cast it, and no voter can prove that he or she voted in a particular way.
d. **Verifiability:** A system is verifiable if anyone can independently verify that all votes have been counted correctly.
e. **Convenience:** A system is convenient if it allows voters to cast their votes quickly, in one session, and with minimal equipment or special skills.
f. **Mobility:** A system is mobile if there are no restrictions (other than logistical ones) on the location from which a Anonymity voter can cast a vote
g. **Authentication:** is distinct from *authorization* , which is the process of giving voters access to system based on their identity. Authentication merely ensures that the voter is who he or she claims to be, but says nothing about the access rights of the voter.
h. **Integrity:** A system is integrity if votes can only be accessed or modified by those authorized voters.
i. **Non-Repetition:** guarantee that no repetition of that vote will be present in the final tally (No voter is allowed to cast their vote more than once).
j. **Anonymity**. Guarantee that the ballot does not indicate who do this voting. Secret ballots are fundamental to democracy, and voting systems must be designed to facilitate voter anonymity.
k. **Scalability**: Voting systems need to be able to handle very large elections. One hundred million people vote for president in the United States. About 372 million people voted in India's June elections, and over 115 million in Brazil's October elections. The complexity of an election is another issue. Unlike many countries where the national election is a single vote for a person or a party, a United States voter is faced with dozens of individual election: national, local, and everything in between.
l. **Speed**: Voting systems should produce results quickly. This is particularly important in the United States, where people expect to learn the results of the day's election before bedtime. It's less important in other countries, where people don't mind waiting days -- or even weeks -- before the winner is announced.

The success rate of an electronic voting system in electronic decision making is dependent on security, authenticity and integrity of pre-electoral, electoral and post electoral phases of the election process.

## 2. Problem Statement

As information technology evolves over time, the need for a better, faster, 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.

## 3. Research Objective

The main objective of this study is:

- Study the electronic voting protocols from the security perspective.
- The privacy, authentication, integrity, non-repetition mechanisms for the e-voting system.
- Develop a general electronic voting protocol 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.

## 4. Methodology and Research Plan

The Methodology consists of six main phases:-

### 4.1Awareness of Problem

Understanding of the problem which needs to be solved, as well as the objective and the scope of this study. This project is aimed at developing a secured electronic voting system which will prevent casting of votes twice and also disallow people who are not right persons to vote from casting votes. After the problems are identified, the objectives and significance of the study are defined clearly after that. In completing this phase, the output of this phase is a proposal for a new research effort.

### 4.2 Suggestion

Several alternatives are examined and discussed. There are many approaches to the problem of this project, which are discussed over a period of months.

### 4.3 Develop an e-voting protocol for secure e-voting system

The evaluation of the existing system and the organization structure of the e-voting system are presented. Then select specific method which was used in order to achieve the objectives of this thesis, particular requirements for implementation of the project and a brief explanation of why such methods were used for implementing the proposed system, also included is a brief description of the current system of voting.

### 4.4Test and analyze the developed e-voting system.

### 4.5 Summarizing the results and Publication

### 4.6 Thesis writing is started from the beginning the thesis.

## Research Plan

- ❑ **Phase0:** understanding research topic [1 month].
- ❑ **Phase1:** literal review and survey [1 month].
- ❑ **Phase2:** Suggesting several alternatives for e-voting protocols for secure voting system [3 month].
- ❑ **Phase 3:** Developing an e-voting protocol to achieve secure voting system [3 month].
- ❑ **Phase 4:** Testing and analyzing the implemented system [3month].
- ❑ **Phase 5:** Summarizing the results [2 month].
- ❑ **Phase 6:** Produce system for securing e-voting system [3 month].
- ❑ **Phase 7:** Writing documentation [2 month].

## 1. References

1. *Bellis,Et Al,” **The History Of Voting Machines**”, November 9, 2006 .*

2. *Malwade Nikita1, Et Al, "**Secure Online Voting System Proposed By Biometrics And Steganography”,** International Journal Of Emerging Technology And Advanced Engineering (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3,Issue 5, Pp. 1,May 2013).*

3. *Dr. Magdi Amer, Et Al," **Towards A Fraud Prevention E-Voting System”** ,(IJACSA) International Journal Of Advanced Computer Science And Applications, Vol. 4, Pp. 1-2, 2013.*

4. *Olayemi Mikail1, Et Al, "**A Survey Of Cryptographic And Stegano-Cryptographic Models For Secure Electronic Voting System”,** Covenant Journal Of Informatics And Communication Technology (CJICT) Vol. 1; Pp. 5-10, December, 2013.*

5. *Gianluca Dini,* **“A *Secure And Available Electronic Voting Service For A Large-Scale Distributed System*”,** *Pp. 1-3, 27 June 2002.*

6. *FERAS A. HAZIEMEH, Et Al, "**New Applied E-Voting System”,** Journal Of Theoretical And Applied Information Technology Vol. 25, Pp. 1-6,31st March2011.*

7. *M. El Hadidi, Et Al,**”Revisiting Legal And Regulatory Requirements For Secure E-Voting”.*** Pp.*6-8, May 2002.*

8. *Sanjay Kumar1and Manpreet Singh2,"**Design A Secure Electronic Voting System Using Fingerprint Technique"**, IJCSI International Journal Of Computer Science Issues, Vol. 10, Issue 4, No 1, Pp. 1-3, July 2013.*

9. *Dr.Aree Ali Mohammed, Et Al," **Efficient E-Voting Android Based System",** International Journal Of Advanced Research In Computer Science And Software Engineering  Research Paper, Volume 3, Issue 11, November 2013.*

10. *ANDREA HUSZTI," **A Homomorphic Encryption-Based Secure Electronic Voting Scheme",** Pp. 1, 2011.*

11. *Mahmood Khalel Ibrahem,Et Al,"**Secure Messaging System Using ZKP",**IJCSET, Vol.3, Issue 11, Pp. 1-3, November 2013.*

12. *Nigel Smart And Frevercauteren (2010), "**Fully Homomorphic Encryption With Relatively Small Key And Ciphertext Sizes",** May 9, 2010.*

13. *Y Govinda Ramaiah,et al,**"Towards Practical Homomorphic Encryption with Efficient Public key Generation",** ACEEE Int. J. on Network Security , Vol. 03, No. 04,pp.1, Oct 2012.*

14. *Dr. Mahmood Khalel Ibrahem and Nada Mahdi Kiatan, **"Homomorphic Encryption Protocol for Secure Electronic Voting System".***

15. *Nigel Smart and Fre Vercauteren, (2010), "**Fully Homomorphic Encryption with Relatively Small Key and Cipher text Sizes"**, May 9, 2010.*

16. *Austin Mohr," **A Survey of Zero-Knowledge Proofs with Applications to Cryptography",** pp. 1-5.*

17. *Krantz, Steven G., (2007), "**Zero Knowledge Proofs**", AIM Preprint Series, Volume 10-46, July25, 2007.*

18. *Yunho Lee a, et al,"**Towards trustworthy e-voting using paper receipts",** pp.1-3, 2010.*

19. *Thomas E. Carroll, Daniel Grosu ," **A secure and anonymous voter-controlled election scheme",** Journal of Network and Computer Applications 32 (2009) 599–606, 29 July 2008.*

20. *Francesc Sebé,"**Simple and efficient hash-based verifiable mixing for remote electronic voting**", Computer Communications 33 (2010) 667–675, 12 November 2009.*

21. *Prof. Dr. Dimitris Gritzalis," **Secure Electronic Voting",** September 2002.*

22. *Steve Kremer,"**Election verifiability in electronic voting protocols",** June 28, 2010.*