CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

Election is the fundamental instrument of democracy that provides an official mechanism for the people to convey their views to form a government by democratic means. Nowadays, one of the most important government services like election becomes a severe pressure on people involved in that process, according to many constraints that must be applied to the beneficiaries of this service and who are divided into two parts, candidates and voters. Voting is an efficient method for the public to show their opinion about a given topic or issue. Electronic voting becomes the most important application in e-governance and e-democracy. In other words, voting is the key for democracy. The traditional election is normally held under the supervision of the government to assure the right application of the constraints during the election process and to assure that only eligible voters are permitted to join the election process avoiding any kind of forgery and the attempts of multi-voting.

One of the most famous violations of any government is vote buying, which is too difficult to control. In addition, the process of human supervision over the election process requires a lot of effort and money in order to achieve the desired level of privacy, security and trust. Moreover, when the election is done, another problem appears which is vote checking and counting. These require great efforts that are supposed to be exerted by
humans and no single mistake is accepted during this process. This phase of the election is considered as a time consuming process and its accuracy is always mistrusted. These drawbacks enforce the public to think about another voting system that could overcome the above mentioned drawbacks. Due to these problems, the whole world is moving towards the trend of e-voting. E-voting systems are expected to be the solution to reduce the weaknesses in traditional voting systems.

Recently, few countries have taken the initiative to test and use electronic voting system. In India, the largest democratic country, also these electronic voting systems were practiced in recent elections. The act of freely expressing some choices between publicly known alternatives is known as voting. Some of the countries which uses electronic voting and on-line voting are United States, Brazil, Australia, Canada, Belgium, Germany, Romania, France, Venezuela, Philippines, The European Union, Switzerland, Italy, Norway, Romania and United Kingdom. Many countries believe that Internet voting will be possible within the next decade.

Electronic voting is easily accessible by individuals with disabilities. They have the ability to use joysticks, earphones, sip and puff technology and foot pedals. These machines have touch screens which can display the information in several languages and voting choices in audio for visual impaired voters. These features make voting easier and comfortable for people with disabilities.

Since 1980, electronic voting schemes were the topic of many researches and lots of voting systems have been designed. So far, while more and more protocols have been developed, the set of security properties that a protocol has to achieve has evolved. Thus, researchers keep combining existing or created cryptographic primitives to construct efficient electronic voting schemes, with respect to these security requirements.
1.2 THE FRAMEWORK OF TRADITIONAL VOTING SYSTEM

One of the most popular voting systems is the paper based voting system. In this system, on the day of the election, voters come to polling station and after authentication they receive a ballot and cast their vote in a polling-booth. Finally they deposit ballot paper in a box in front of the authority and sign a register to confirm that they have voted. When the voting phase is finished, the ballot box is publicly opened by the authority, ballots are counted and result of the election is declared.

Traditional Voting system consists of the following four phases illustrated in Figure 1.1.

i. **Authentication:** Alice walks into a voting precinct and authenticates herself by showing her voting credentials; this step is public and verified by the officials present in the room. At the end of the authentication process, Alice is given a paper ballot on which to write her vote.

ii. **Vote:** The casting of vote takes place in a protected booth where she is not seen by anyone. Alice casts her vote by writing it with a pencil on the paper ballot; she then folds the paper ballot and puts it in the ballot box where all the votes are mixed. No one can see what Alice writes and there are no identification marks on the paper ballots, and hence it is confidential.

iii. **Count votes:** At the end of the voting time, the officials open the box containing the paper ballots and publicly count the votes; the result is announced after completion of counting.
iv. **Verification**: Various types of verification are used or possible; most procedures are indeed public and overseen by representatives of competing parties. The opposite interests of the parties warrant the first level of protection against fraud. A recount is also possible if there is a presumption of fraud or error.

![Figure 1.1 Phases of Conventional Voting](image)

Even today, in traditional voting system frauds and malpractices are still inevitable. In the authentication phase, there are risks of corrupt authorities allowing ineligible persons to vote, or to vote more than once, and of malicious voters attempting to impersonate other eligible voters. The risk of compromising privacy is also significant at this stage. In the voting phase,
there is the possibility for the destruction or duplication of ballots and ballot stuffing. Accuracy and verifiability are most prominent in the counting and verification stage and rely deeply on the security achieved in the previous stages. But people are quite convinced that some properties as anonymity or verifiability of the vote are satisfied by a paper based election.

1.3 ISSUES IN TRADITIONAL VOTING SYSTEM

Traditional voting system (such as voting by paper or signature voting) has many problems:

- Printing of ballot paper is expensive.
- Voting consumes lot of time.
- Counting is prone to errors.
- Maintaining convenient poll booths is very difficult.
- There is no good relationship between the government and popular, popular cannot trust the government and depend on it.
- Sometimes, government coerced and carries on the voters to vote for a particular candidate, and eliminate them from voting freely.
- Some candidates try to buy the votes from the voters.
- Government can cheat by substitute the original ballot by derivative ones.
- Disabled people must rely on others to cast their votes.
Due to the above said reasons, the whole world is moving towards the trend of e-voting. Electronic voting systems are expected to be the solution to overcome the above said weaknesses in traditional voting systems.

1.4 FRAMEWORKS AND ALGORITHMS OF CRYPTOGRAPHY

Cryptography is one of the most important areas in the computer industry. Cryptography is the science of keeping things secret, this is known formally as confidentiality. Encryption allows an application to secure its data from being accessed by hackers.

Cryptography is used to achieve the following goals:

- **Confidentiality**: To protect a user's identity or data from being read.
- **Data integrity**: To protect data from being changed.
- **Authentication**: To ensure that data originates from a particular party.
- **Non-repudiation**: To prevent a particular party from denying that they sent a message.

There are two kinds of cryptosystems: symmetric and asymmetric.

1.4.1 Symmetric vs. Asymmetric Cryptosystem

In symmetric algorithms, both parties share the same key for encryption and decryption. To provide privacy, this key needs to be kept secret. Symmetric algorithms have the advantage of not consuming too much computing power. A few well-known algorithms are: DES (Data Encryption Standard), Triple-DES (3DES), IDEA (International Data Encryption
Algorithm), CAST5 (Carlisle Adams and Stafford Tavares), BLOWFISH, AES (Advanced Encryption Standard) and TWOFISH.

Asymmetric algorithms use pairs of keys. One key is used for encryption and the other key for decryption. The decryption key is typically kept secretly, therefore called "private key" or "secret key", while the encryption key is spread to all who might want to send encrypted messages, therefore called "public key". Everybody having the public key is able to send encrypted messages to the owner of the secret key. The secret key can't be reconstructed from the public key. The idea of asymmetric algorithms was first published in 1976 by Diffie and Hellmann.

Asymmetric algorithms seem to be ideally suited for real-world use: as the secret key does not have to be shared, the risk of getting known is much smaller. Every user only needs to keep one secret key in secrecy and a collection of public keys that only need to be protected against being changed. With symmetric keys, every pair of users would need to have an own shared secret key. Well-known asymmetric algorithms are RSA (Ron Rivest, Adi Shamir and Len Adleman), DSA (Digital Signature Algorithm), and ElGamal.

However, asymmetric algorithms are much slower than symmetric ones. Therefore, in many applications, a combination of both is being used. The asymmetric keys are used for authentication and after the successful authentication, one or more symmetric keys are generated and exchanged using the asymmetric encryption. This way the advantages of both algorithms can be used.

The Table 1.1 gives the comparison between symmetric key cryptosystem and public key cryptosystem based on the parameters such as Functionality, Efficiency, Key size, Hardware and Security.
### Table 1.1 Comparison between Symmetric and Asymmetric Key Cryptosystem

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Symmetric Key Cryptosystem</th>
<th>Asymmetric Key Cryptosystem</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Functionality</strong></td>
<td>Allows efficient communication between two parties in a closed environment.</td>
<td>Enables security in settings in which symmetric encryption simply does not work or is more difficult to implement.</td>
</tr>
<tr>
<td><strong>Computational efficiency</strong></td>
<td>Computes incredibly fast, since the relatively simple operations used are executed very efficiently.</td>
<td>Computes slowly, using computationally heavy and complex operations, based on the difficulty of solving number-theoretic problems</td>
</tr>
<tr>
<td><strong>Key size</strong></td>
<td>Uses 128-bit symmetric keys, which are considered very secure.</td>
<td>Employs key sizes of at least 1000 bits to achieve sufficient, lasting security</td>
</tr>
<tr>
<td><strong>Hardware</strong></td>
<td>Performs simple algorithms, requiring relatively inexpensive hardware.</td>
<td>Implements complex and time-consuming algorithms that need more powerful hardware.</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>No difference. Security is based on the strength of the algorithm and size of the key. Good algorithms exist for both encryption methods. Key size effectiveness, as shown above, is dependent on the encryption method.</td>
<td></td>
</tr>
</tbody>
</table>
1.4.2 Hybrid Cryptosystem

Hybrid Cryptosystem is one which combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem as shown in Figure 1.2. With the help of asymmetric key cryptosystem one can achieve authentication and using symmetric key cryptosystem can achieve confidentiality.

Figure 1.2 Confidentiality and Authentication

Encryption:

In the hybrid cryptosystem, Plain text is encrypted using Sender’s Private key (KR_A) and then again it is encrypted using Receiver’s Public key (KU_B) (Equation 1.1).
\[ Z = E_{KUB} \left( E_{KRA} (X) \right) \] (1.1)

**Decryption:**

Initially, the received Cipher text should be decrypted only by receiver’s private key (KR_B). No other person (unauthorized person), can open the message. In this way, it achieves confidentiality. And then only, the intermediate cipher text(Y) will be decrypted using sender’s public key (KU_A). Because of this, it achieves authentication (Equation.1.2).

\[ X = D_{KUA} \left( D_{KRB} (Z) \right) \] (1.2)

### 1.5 **ELETRONIC VOTING SYSTEM**

Electronic voting refers to computerized voting machines that use electronic ballots rather than paper ones. An electronic voting system is a voting system in which the election data is recorded, stored and processed primarily as digital information. Electronic voting also known as e-voting includes optical scanning vote systems, punched cards, voting kiosks, transmission of ballots and votes via Telephone, Internet or Private computer networks.

Many cryptographers have proposed a secure e-voting system using cryptographic techniques. There are several requirements for the secure e-voting system. The several requirements can be satisfied partially by cryptographic techniques.

In this section, several requirements for secure e-voting systems are introduced. These requirements can be satisfied partly by cryptography techniques. However, many cryptography researches have been carried out to provide the perfect techniques for these requirements.
**Fairness**: No one can learn the voting outcome before the tally.

**Eligibility**: Only eligible voters are permitted to vote.

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

**Privacy**: No one can access any information about the voters vote.

**Completeness/ Accuracy**: All valid votes should be counted correctly.

**Soundness**: Any invalid vote should not be counted.

**Uncoercibility**: No voter can prove how he voted to others to prevent bribery.

**Efficiency**: The computations can be performed within a reasonable amount of time.

**Robustness**: A malicious voters cannot frustrate or disturb the election.

### 1.6 FRAMEWORKS AND ALGORITHMS OF AN ELETRONIC VOTING SYSTEM

A very first attempt was designed by Cranor et al., (1996) without employing any cryptographic techniques. In this technique, voter would submit his vote along with a unique identification number to a Validator who would remove his name from the list of registered voters. Then the Validator would strip off the Unique Identification number and submit the votes to the Tallier who would count the votes. Both **privacy** and **accuracy** lack with this protocol.
Cranor et al (1997) proposed and implemented a protocol based on Fujioka’s scheme called *Sensus*. The main difference between both schemes is that Sensus allowed users to vote in a single session, whereas Fujioka’s proposal required two sessions. However, one disadvantage of these schemes is that the network traffic increases since the voter is required to send the same ciphered messages twice, making the protocol less efficient.

Fujioka et al (1992) developed a practical voting scheme using blind signatures. In their proposal, each voter signs his/her vote with a secret key, and then sends it to the counting center through an anonymous channel.

One disadvantage of this scheme is that the protocol is complex since the voting phase consists of two steps. Liaw et al (2004) discussed the properties of electronic voting system and how their proposed electronic voting scheme try to satisfy these properties is also mentioned. Mohamed et al (2007) discussed the how electronic voting is carried out in Egypt using biometric smartcard. It also discusses and analyzes how the various security requirements are satisfied.

Nurmi et al (1991) developed two agency protocols. In this, the electronic validator distributes a secret identification tag to each voter just prior to the election. The Validator then sends the Tallier a list of all identification tags, with no record of the corresponding voters. Each voter sends the Tallier his/her identification tag and an encrypted file containing a copy of the tag and the voted ballot. At this point the Tallier can make sure the identification tag is valid, but the program has no way of examining the contents of the ballot. The Tallier publishes the encrypted file, and the voter responds by sending the Tallier the key necessary to decrypt it. When the election is over, the Tallier publishes a list of all voted ballots and the corresponding encrypted files. This protocol also has several problems. Most
importantly it doesn’t protect the voter’s privacy if the Tallier and Validator collude.

Peter et al (2003) discusses a secure PKI (Public Key Infrastructure) based system for e-voting that was developed. They tested the application, several organizational aspects, and usability in fourteen field trials. In their paper they describe the method and findings. What they learn about turnout, about the logistics of organizing e-voting, and about usability and reliability of the system in practice.

Qadah et al (2007) detailed the requirements, design and implementation of a special type of electronic voting systems, the remote online voting system, suitable for university setting where students can cast their votes anytime, anywhere and using fixed and mobile electronic devices including personal computers, personal digital assistants and smart and regular phone.

Sarah et al (2008) reported about the comparison of efficiency of the DRE (Direct Recording Electronic voting system) with the traditional machines. It indicates that there were little differences between DRE and traditional methods in efficiency.

1.7 PROBLEM DESCRIPTION

Traditional voting system has many problems which are discussed in Section 1.3. Because of those reasons, the whole world is moving towards the trend of e-voting. Electronic voting systems are expected to be the solution to overcome the weaknesses of traditional voting systems.

All the existing electronic voting protocols such as Two agency protocol, Blind signature and Sensus protocols are based on the asymmetric
key cryptosystem. Asymmetric key cryptosystem is much slower and more complex than symmetric cryptosystem. Moreover, these protocols are more difficult to implement and it is very difficult for the average user to follow it correctly. So, this thesis proposes a new high speed electronic voting protocol based on symmetric key cryptosystem.

1.8 SCOPE AND OBJECTIVES OF RESEARCH WORK

In democratic countries, voting is the most important tool in decision making. Therefore, elections and referenda should be accessible for as much people as possible, especially for the people living in different states within the country and abroad. It is difficult for these people to participate in elections. On the other hand, elections influence the democracy in a country directly. In addition to this, there are lots of problems in the traditional voting. So it is significant to make sure that elections are carried out electronically.

The requirements in conventional voting (ballot paper vote) apply for e-voting, these requirements can be expected to be universal, and any system must satisfy these requirements:

**Fairness** : No one can learn the voting outcome before the tally.

**Eligibility** : Only eligible voters are permitted to vote.

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

**Privacy** : No one can access any information about the voters vote.

**Accuracy** : All valid votes should be counted correctly.

**Non-coercion** : No voter can prove how he voted to others to prevent bribery.
Efficiency: The computations can be performed within a reasonable amount of time.

Verifiability: A system is verifiable if all voters can independently verify that their votes have been counted correctly without sacrificing privacy.

Anonymity: There should be no way to derive a link between the voter’s identity and the marked ballot.

Convenience: It should allow voters to cast their votes quickly, and with minimal equipment or special skills.

In an electronic voting system, privacy (confidentiality), authentication and security are mandatory features. The development of computer networks and the elaboration of the cryptographic techniques facilitate the implementation of electronic voting. Accordingly, the study of security mechanisms in electronic voting elections has received considerable attention in the last two decades. As a result, a wide variety of e-voting cryptographic protocols have been proposed such as Simple Protocol (Cranor 1996), Two Agency Protocol (Nurmi 1991), Blind Signature Protocol (Fujioka 1992) and E-voting based on Sensus Protocol (Cranor 1997).

All the existing protocols such as Two agency protocol, Blind signature and Sensus protocols are based on the asymmetric key cryptosystem. Asymmetric key cryptosystem is much slower and more complex than symmetric cryptosystem. Moreover, these protocols are more difficult to implement and it is very difficult for the average user to follow it correctly.
Keeping all these above aspects in mind, the present work has been carried out to develop frameworks and algorithms for Secured Electronic Voting Systems to achieve the following objectives:

- Develop an alternative feasible secured electronic voting system model.
- Construct a fool-proof, flaw less and high speed electronic voting system.
- Develop a convenient and flexible electronic voting system.
- Design a new high speed cryptographic protocol to achieve privacy (confidentiality).
- Use biometric smart card (smart token) mechanism to achieve authentication.

1.9 BRIEF OUTLINE OF THIS THESIS

This thesis titled “Some Studies on Protocols and their Implementation for Secured Electronic Voting Systems” proposes conceptual frameworks and algorithms for secured electronic voting system. In explaining the various possibilities of the frameworks and algorithms, the work reported in this investigation is organized into nine chapters.

The need for electronic voting system and importance is discussed in the introductory Chapter 1. The details of electronic voting system, characteristics and issues are discussed. Factors influencing the Electronic Voting System such as confidentiality and authentication and their significant contribution towards secure communication in Electronic Voting System are described. Objective of the thesis, motivation and scope of the thesis are also narrated.
A review of the existing voting protocol schemes which are used in electronic voting system are presented in Chapter 2. This chapter explains the algorithms and related methodologies in detail. Each of the methodologies has their own strengths and weaknesses. However, none of the methodologies can be said to escort to an inclusive solution. So this investigation expected to provide a better solution compared to existing schemes after comparison.

Chapter 3 explains the concepts and needs for an electronic voting system. It also discusses the various types of electronic voting system such as punch card, computer counting, Direct Recording Electronic, Poll site e-voting, Kiosk e-voting and Remote e-voting system. It presents the comparison between computer counted system and Direct Recording Electronic (DRE) system. The framework of electronic voting system and security requirements for an electronic voting system are presented in detail.

Chapter 4 presents the details about internet voting system and how it can be used to achieve the requirements such as fairness, uniqueness, accuracy, privacy, anonymity, authentication and un-coercion and it also presents the problems that will encounter while implementing internet voting system.

Chapter 5 presents the significance and benefits of smart card in e-voting system. The different types of smartcards used in various security related applications are discussed. The working principle of memory management in smartcards, read and write operations in smart cards are discussed in detail.

Chapter 6 discusses the various existing voting protocols like Simple protocol, Two agency protocol, Blind signature protocol and Sensus protocol in detail. It also discusses how and which security requirements are
satisfied by each protocol in detail. It also presents the various drawbacks occurred in each protocol.

Chapter 7 explains the services which are provided by cryptography in detail. The various cryptosystems such as Symmetric key, Asymmetric key and Hybrid cryptosystems are given. Algorithms developed using symmetric key cryptosystem for high speed electronic voting system are explained. Frameworks and Protocol developed using hybrid cryptosystem approaches for secured electronic voting system are explained. A comparison of proposed frameworks with existing schemes, limitations and applicative features of the present investigation on secured electronic voting system is tabulated and explained.

Chapter 8 discusses about the Proposed Voting protocol in detail. It also discusses about how the proposed protocol achieves the various voting requirements/properties in detail. Finally, the proposed protocol is compared with the existing voting protocols. It also depicts the use case specification of each functional requirement.

Chapter 9 presents the important conclusions of this investigation and also suggests the scope for further research in this evolving field.