ABSTRACT

Election is a fundamental instrument of democracy that provides an official mechanism for the people to convey their views to form a government by democratic means. Electronic voting has become the most important application in e-governance and e-democracy. Recently, few countries have taken the initiative to test and use electronic voting system. Many countries believe that internet voting will be possible within the next decade. In the traditional voting system, the voter authenticates themselves by showing credentials; this step is public and it is verified by the officials present in the polling place. In this authentication, verification is done manually and then they are allowed to cast their vote. The traditional voting method is expensive and involves more human resources. Due to these reasons, the whole world is moving towards the trend of e-voting. Electronic voting systems are expected to be the solution to overcome the shortfalls. Since 1980, electronic voting schemes attracted many researchers. In the last few years numerous numbers of researchers proposed different e-voting systems and some countries and states around the world have implemented their e-voting systems.

To overcome these drawbacks, many cryptographers have proposed a secure e-voting system using cryptographic techniques. While more and more protocols have been developed, the set of security properties that a protocol has to achieve is evolved. There are several
requirements for a secure e-voting system such as uniqueness, efficiency, fairness, security, privacy, authentication, anonymity and uncoercibility. The several requirements can be satisfied partially by cryptographic techniques. Thus, researchers kept combining existing or created cryptographic primitives to construct efficient electronic voting schemes, with respect to these security requirements.

As a result, a wide variety of e-voting cryptographic protocols have been proposed such as Simple Protocol, Two Agency Protocol, Blind Signature Protocol and E-voting based on Sensus Protocol. 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 them correctly.

Now-a-days, research works are carried out in electronic voting system using cryptographic techniques and frameworks because it was felt that there was a need to propose more algorithms based on the electronic voting system requirements. This dissertation titled “Some Studies on Protocols and their Implementation for Secured Electronic Voting Systems”, proposes conceptual frameworks and algorithms for secured electronic voting systems.
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, error 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.