Security is of prime concern in electoral process in a democratic country which depends on broad trust in the honesty of elections. There has been a lot of awareness to an electronic voting by cryptographers. Many scientific investigations have been done in order to obtain security, privacy, certainty and correctness in electronic voting systems by improving cryptographic protocols of e-voting systems. Currently, the cryptographic schemes are not the main issue. The main attraction is the feasible security in e-voting systems to justify the security of execution.

This thesis is an attempt to explore mechanisms and technologies for designing secure Electronic Voting (E- voting) systems. E- Voting information systems belong to the area of computer applications, exploring ICT to increase participation in governance and democracy. This thesis is intended to find a common point of intersection where both electronic governance and Information and Communication Security meets. In this thesis, our focus is of security issues as designing a secure E-voting system needs to satisfy the technical and procedural requirements at all level of assurance with respect to social and regulatory framework.

The last few years have brought a focus onto the technology used in the voting procedure and a hunt for voting machines that promote confidence. Computerized voting systems bring better usability and cost benefits but also the baggage of buggy and unprotected software. Existing voting systems are penetrating with security holes, and it is difficult to prove even simple security properties about them. A voting system that can be proven correct would reduce many concerns. This thesis explores methodologies and technologies for designing a secure electronic voting system using biometrics.

Biometrics is a pattern recognition technology that enhances the identification and verification of citizens being part in election procedure. Finger print recognition is a type of biometric software application to identify a specific person using his/her digital image by analyzing and comparing some patterns. These systems are commonly used for security and authentication purposes. This work mainly focused on authentication of voter to cast his/ her vote. Artificial neural network based model has been used in this thesis to capture the digital
image of voter which is compared with the digital images of individuals on the day of election to authenticate a voter to avoid bogus voting.

In this work, we have focused on improvement of security in E-Voting System using Biometric techniques such as fingerprint. The theory and experimental study validate the effectiveness and efficiency of this research to enhance the security in Electronic voting system. Highlights of the work in this thesis are as under:

- On the basis of advantages and disadvantages as well as implications of error rates of different biometric techniques, it is concluded that the finger impression based biometric techniques are fast, accurate and more reliable and secure.
- A system model of Electronic voting has been developed wherein fingerprint is captured through biometric technique for voter authentication.
- A framework for electronic voting system based on fingerprint biometric is proposed and implemented with the objectives of eliminating bogus voting and vote repetition, less election expenditure, more transparency and fast results.
- An artificial neural network based intelligent E-voting model finally has been presented in this research to address most of the security issues of E-voting in electoral process. This model presents a two way authentication mechanism to avoid fake voting and repetition of vote cast.