**CHAPTER TWO – LITERATURE REVIEW**

This chapter discusses various related and past researches that have been conducted on Electronic Voting Systems and emphasis on the security of such systems.

**PREVIOUS AND RELATED WORKS**

In an attempt to design a reliable, efficient and credible voting system, many solutions have been proposed by plethora of authors to ensure correctness, coherence, consistency, security and transparency of an election process in a country, state, community or even an institution. For instance, Patil et al in [12] proposed a smart voting system with highly secured biometric authentication system and OTP (One Time Password) based verification system. In this system, Aadhar card number (a special type of card number like that on the National Voters Card) was used as a means of verifying voters to ensure they do not vote more than once. Authentication of users is achieved for those with smart phones with an OTP that would be automatically sent to the users’ phones or fingerprint recognition for voters without smart phones or biometric devices. In order to further improve the security of this system, users’ vote is being encrypted using cryptography with a method called Mixed Nets method which performs permutations on input and gives out the encrypted message assuring that only authorized people who have the decryption key can count the cast votes. It was finally conjectured that this system would increase the rate of turnout of voters since they can vote from their convenient places. In addition to that, time and resource during election would be greatly reduced. With this approach, a highly secured voting system is being achieved.

In [13, 14], fingerprint based secured electronic voting machine based on arduino was proposed. Unlike [12], voters do not have the flexibility of voting from their locations at their convenient times. Since the fingerprint of different individuals is unique, it is used as a means of verification and authentication. A fingerprint sensor is used to capture the fingerprint of voters. Voters are able to vote by selecting from a panel of push buttons their preferred candidates and the results is finally being displayed on an LCD after the voting process. One of the limitations of this project is that it is not scalable. Once the fingerprint scanner memory becomes full, it can no longer capture the data of voters which makes this project suitable for a small community or an institution. Another drawback of this project is that it is not connected to any external server or database which implies that any damage to the electronic voting system results in the total or complete loss of data of all voters.

Deepika et al discussed in [15] the various issues and drawbacks accrued to existing voting systems and proposed a new architecture based on GSM module and IoT technology to improve the speed and security of the voting system. The project is microcontroller based unlike [13, 14] which were based on arduino. In this paper, voters can easily verified that they have voted because a message is directly sent to their mobile using the GSM module. With the help of IoT, the vote cast is being sent to a centralized database and server where the overall votes is being collated. The fingerprint images of eligible voters were also used as a means of security in this project which were captured with a fingerprint scanner.