ABSTRACT

Over the years Electronic Voting Machines have replaced the paper ballot system. Even though many advantages are listed in current ballot systems, many issues have arisen basing on the security and physical strength of voting machines in public and media. Internet voting is an electronic system where in election allows voters to cast their ballot vote to corresponding election executive over the internet with secrecy and confidentiality. Issues in Internet are the security which is mainly dealt by concept of Internet Voting using Modified Elliptic Curve Cryptography with Multicore Parallel Particle Swarm Optimization to maintain each phase of the electoral procedure to ensure its privacy, transparency and security.

The election system is necessity of the every democracy and the administration formed is dependent on the results of the election. The election process paves the path for every voter to select a representative among themselves who can guide the democratic system towards the welfare of the society. Voting is the process required whenever there is more than one person competing for any position or statements or views to be chosen among multiple choices. The voting system has observed many effective changes over the past few decades, right from the traditional paper ballot voting to electronic voting and now towards the online voting. The voting system is improving step by step; advancement in the new system eliminates the drawbacks of the previous system.

The main idea of present work is to provide a secure means to encrypt vote and sign for authentication as verified in manual Voting System. Elliptic Curve Cryptography is a Public Key Cryptography System that provides same level of security in less number of bits as compared to other most widely used Public Key Cryptographic Systems. Elliptic Curve Cryptography uses a set of private and public keys where private key is randomly selected prime number and public key is further computed using Modular Multiplication. They transfer Discrete Logarithm Problem to Elliptic Curve Discrete Logarithm Problem.
Modified Elliptic Curve Cryptography uses a Multicore Parallel Particle Swarm Optimization algorithm to choose the private key instead of random generation. During this work, the risks and aspects concerned in Internet Voting architectures are considered and resolved.

Internet Voting with the widespread use of Internet is becoming increasingly appealing to groups in place of paper based elections or vote-by-mail elections to geographically distributed voters, as more people are gaining access to the Internet. However, I-Voting systems should be designed carefully or otherwise they may corrupt results or violate voter’s privacy. In this work, the aspects and risks involved in Internet Voting architectures are considered and a solution is derived for better usage.

The Secured Internet Voting System is simulated and the test results show that the proposed system is secured and flexible. The function of this system is to maintain the most basic principles of an elector process by using added communication methodology. The main functionality of the technique is to keep up the most basic values of an elector process, such as confidentiality, accuracy, ambiguity, anonymity, non-coercion.

**KEYWORDS:** Modified Elliptic Curve Cryptography (MECC), Multicore Parallel Particle Swarm Optimization (MPPSO), Public Key Cryptography (PKC), Elliptic Curve Discrete Logarithm Problem (ECDLP)
List of Peer-Reviewed Publications from This Study

Journals

1. “Reliable Verified Internet Voting System based on Modified Elliptic Curve Cryptography”, IJAER.

Conferences


Communicated

8. “Secured Internet Voting System based on Modified Elliptic Curve Cryptography with Parallel Multicore Particle Swarm Optimization”, communicated to IEEE Security & Privacy, SP-2015-12-0221