ABSTRACT

Online voting guarantees to improve the democratic participation as it allows to cast the votes from remote locations. It is one of the cost effective solution that speeds up the tallying process and helps in increasing voter turnout. The security aspect of online voting is a vital significance. A robust online voting system has to address the requirements namely Authenticity, Confidentiality, Integrity, Anonymity, Accuracy, Availability, Receipt-freeness, Verifiability, Transparency and Eligibility.

The main objective of the research is to investigate on the existing mechanisms and design secure online voting framework to achieve Confidentiality, Integrity and Availability. The framework is a collection of classes, objects and their collaborations that enable large scale reuse by capturing an abstract design and the core implementation for a domain from which a range of specific applications can then be derived. Software frameworks offer reusability of both design and implementation. The primary benefits of frameworks stem from the modularity, reusability and extensibility they provide to developers. In this research, the domain framework constitutes online voting components and the service framework constitutes security components. Online voting system consists of Pre election Phase, Election Phase and Post election Phase. The Pre election phase deals with registration of the voter. The Election Phase consists of two stages Authentication and Voting stage and Post Election Phase deals with counting stage.

As a first step towards secured online voting, efforts have been taken to design online voting using Modified ElGamal encryption system to meet the security requirements namely Authenticity, Integrity, Confidentiality, Accuracy, Availability, Receipt-freeness, and Eligibility. Modified ElGamal encryption is used for communicating between the voter and the Agent. It is based on the difficulty of finding discrete logarithm in a cyclic group.

To address anonymity the Blind Signature is a type of digital signatures that allows messages to be signed without revealing its contents has been carried out. Online voting using Modified RSA Blind signature meets the security requirements namely Authenticity, Confidentiality, Anonymity, Integrity, Receipt-freeness, Accuracy, Availability and Eligibility.

A Blockchain is a peer to peer, distributed ledger that is cryptographically secure, append only, immutable and updateable via consensus. Based on the synergy between Blockchain characteristics and the voting requirements, Self organizing Blockchain enabled Security Framework has been designed. Customizable Blockchain based online voting meets the security requirements namely Authenticity, Confidentiality, Anonymity, Integrity, Accuracy, Availability, Receipt-freeness, Eligibility, Transparency and Verifiability.

The schemes are assessed using Spearman's correlation to evaluate the degree to which it meets the security requirements of online voting system. Computational complexity of the all the three schemes is carried out based on which the online voting using Customizable Blockchain has lesser computation cost than the other online voting using Modified ElGamal encryption and Modified RSA Blind signature.