

Survey on Security for Online Voting System

Ms. Kalyani Khandar¹ Ms. Aishwarya Metkar² Mr. Dushyant Jaiswal³ Ms. Prajakta Thakre⁴
^{1,2,3,4}B.E. Student

^{1,2,3,4}Department of Computer Engineering

^{1,2,3,4}Rajiv Gandhi College of Engineering and Research, Nagpur

Abstract— The word “vote” means to choose from a list, to elect or to determine. The main goal of voting is to come up with leaders of people’s choice. Many fields came up with Online voting systems. These online voting systems have issues regarding security of vote. As we know there are many online voting systems developed earlier but they have several security issues regarding authentication, integrity and non-repudiation. Thus to avoid such issues there should be some secure approach for tackling them. We are trying to provide some with our project.

Key words: Security, Voting System

I. INTRODUCTION

Basically to vote is to elect. There are two ways to vote; one in which you have to go directly to the voting center and another is online voting. The security is not promised in online voting system, so will try to make it secure.

The main aim of this project is to provide secured voting system. The vote should be delivered without any replication or corruption. The basic objective is to protect the site or the voting system from several attacks. There are many attackers which try to make changes in the vote when it is travelling from client to server or try to detect the vote, so we try to provide security to the system from such attackers. It will also help to check whether the voter is valid voter or not.

Online voting system has been introduced in past few years in our country. It is a way in which one can vote even sitting at one’s place no need to go any voting center. This voting system is not that secured as intruders/attackers attack in many ways which does not keep this system secured. So to make the online voting system secured we are going to make use of several techniques and we will provide security to it.

II. LITERATURE SURVEY

Following are the papers which we have gone through to study the research made in the field of security of online voting system.

A. SELES: An E-Voting System for Medium Scale Online Election

Recent advances in communication networks and cryptographic techniques have made possible to consider online voting systems as a feasible alternative to conventional elections. Until today several protocols for electronic voting have been proposed, unfortunately only a few of them have been implemented in an end-to-end fully functional system. In this paper, authors have presented a secure electronic voting system for medium scale online elections (SELES). This system efficiently implements a security communication protocol offering protection against double voting and others frauds while avoiding any private voting channel. SELES accomplishes all the standard

properties of conventional voting systems, namely, accuracy, democracy, privacy, verifiability, simplicity, flexibility and double voting detection. Our system has been tested in a distributed and heterogeneous Internet network comprised by workstations, laptops and PDA nodes interacting through wired and wireless connections. Additionally, SELES has been designed to deal with communication failures, thus achieving a certain degree of robustness. [1]

B. Pair Voting: A Secure Online Voting Scheme Using Pairing-Based Cryptography and Fuzzy Extractor

With the increase in popularity of electronic voting, it has become necessary to have secure online voting mechanism. This paper presents a novel online voting scheme by using combination of biometric and password based security. The scheme uses Fuzzy Extractor to provide biometric based authentication, while secret password is used to provide password based protection of the voter. In addition, Pairing-Based Cryptography is used to provide the necessary security requirements of an online voting system. A prototype of the proposed scheme is implemented and its performance and security analysis shows that the proposed scheme is cost-effective and at the same time satisfies the security requirements of an online voting system. [2]

C. Electronic Voting Systems: Security Implications of the Administrative Workflow

With the rapid growth of the Internet, online voting appears to be a reasonable alternative to conventional elections and other opinion expressing processes. Current research focuses on designing and building "voting protocols" that can support the voting process, while implementing the security mechanisms required for preventing fraud and protecting voter's privacy. However, not much attention has been paid to the administrative part of an electronic voting system that supports the actors of the system. Possible "security gaps" in the administrative workflow may result in deteriorating the overall security level of the system, even if the voting protocol implemented by the system succeeds to fully comply with the security requirements set for voting. To this direction, this paper describes the responsibilities and privileges of the actors involved in the electronic voting process. The description of the role of each actor, together with the clear indication of what each actor is expected - and thus allowed - to do with the system, formulate an operational framework that complements the technological security features of the system and allows us to talk about "secure electronic voting systems". [3]

III. PROPOSED SYSTEM

A. Proposed Approach / Work

The project consists of online voting system in which we are providing security with different techniques. We have made a registration page in html with a table created in MySQL

connected by jsp. We are using digital signature, cryptography. We will be generating OTP i.e. one time password which will be provided to user at the time of voting to check whether the voter is valid voter or not. The casted vote will be encrypted at the client and will be decrypted at the server. In this way we will be providing security.

B. Proposed Architecture

The architecture composed of client, intruder, server and database. The user will vote at client then the vote will be travelled along through the network to the server. In between the path two types of intruders can attack: Passive intruder and Active intruder.

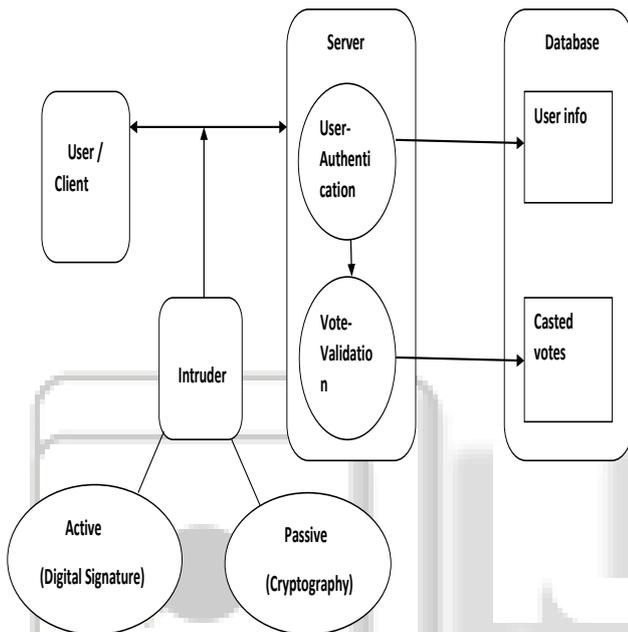


Fig. 1: Architecture of SAOVS

1) Passive Intruder

A Passive attack is one in which the intruder reads but does not modify the message stream in any way.

The passive attack can be prevented by using cryptography.

2) Active Intruder

In Active, the intruder can read the message stream as well as modifies it. The active attack can be prevented using digital signature.

After this the secured vote will be sent to server. At the server, user authentication and vote validation will be done and the vote will be saved to database. The database will ultimately save user information and casted votes.

C. Basic Steps/Scenarios

First we have to make registration page with html and have to create database table on MySQL. Then we need to connect the registration page to MySQL database with the help of JDBC so that we can store the entries from registration page to MySQL database.

After this we need to generate OTP (one time password) to detect whether the voter is valid or not. Then with the help of RSA algorithm we have to generate public and private keys to check whether the casted vote is valid or not that means whether the vote belongs to the valid voter or not.

At the end we need to apply all of the above techniques we have used and implement them on the online

voting system. Hence we get a secured online voting system which is protected from intruders.

IV. RESULT

Secure approach for online voting system project helps us to overcome the security issues in the online voting system. This voting system helps to get the fair count of votes which helps in getting clear results of election without any cheating or fraud.

REFERENCES

- [1] SELES: an e-voting system for medium scale online election
- [2] Pair Voting: A secure online voting scheme using Pairing-Based Cryptography and Fuzzy Extractor
- [3] Electronic voting systems: security implications of the administrative workflow.