ONLINE VOTING SYSTEM USING AES ALGORITHM

S.M.K. Ramakrishnan¹, S.Keerthana², V. Naveen¹, M. Nizamudeen⁴

¹Assistant Professor, Department of Computer Science and Engineering, Kathir College of Engineering, Coimbatore, smkrsulur@gmail.com
²Student, Department of Computer Science and Engineering, Kathir College of Engineering, Coimbatore, keerhanasmka@gmail.com
³Student, Department of Computer Science and Engineering, Kathir College of Engineering, Coimbatore, naveenvasudevank@gmail.com
⁴Student, Department of Computer Science and Engineering, Kathir College of Engineering, Coimbatore, nizam33364@gmail.com

Abstract - Electronic polling systems promise benefits to voters like accessibility and convenience that modify them to solid their votes at any time, from any Internet-connected electronic computer anyplace within the world. However, not like ancient paper-based selection systems, associate e-polling system introduces many security risks like privacy of vote, unlikability of a citizen, citizen coercion, secrecy of partial election results, verifiability, and poll integrity. The legitimacy of a citizen is another security concern, i.e., a citizen should be identified through associate authentication mechanism that forestalls selection of unauthorized voters or vote from approved voters. Another security concern is that the manipulation of votes by associate infected (e.g., virus, malware, so on) selection device. A malware-hosted device may build unauthorized build to the voter’s selection selections. Many e-voting systems have been proposed however, to date, all these schemes either fail to supply all the desired security properties or aren’t much possible on light-weight computing devices. During this paper, we tend to gift a secure and verifiable polling system, Online Voting System using AES Algorithm, that employs well-known science primitives to supply vote and voter’s privacy, and poll integrity, confirms the identity of voters through a multifactor authentication theme, permits vote inside the allowed polling amount, prevents double selection, and achieves verifiability and uncoercibility within the presence of untrusted selection device.

Index Terms- Authentication, efficiency, electronic polling, malware, security, verifiability.

I. INTRODUCTION

A poll is a measurement tool that enables citizens to express their opinions on various issues ranging from public policies (e.g., health care, immigration, education, etc.) to public affairs (e.g., election campaign, approval of a political party, etc.) and private businesses (brand management, consumer-focused marketing, etc.) by giving their nod of approval or rejection. With a few questions with multiple answers, a poll conducting authority can obtain hundreds or thousands of opinions of potential stakeholders to point it in the right direction. For example, in the United States, the Agriculture department carries out online polls occasionally to find out the opinions of citizens on local issues. Similarly, before national elections, various research organizations carry out opinion polling to gauge voting intentions. Traditionally, polls were conducted face-to-face, which required a citizen’s physical presence. With the rise and popularity of the Internet and mobile phones, polls could be conducted remotely. In recent years, a trend towards electronic and Internet polls can be observed. For example, SurveyMonkey is a public-opinion poll that enables people across the world to give their feedback on anything, e.g., a recent SurveyMonkey online poll was conducted in which over 2 million people participated to
either approve or disapprove the job of the United State’s president. Internet-based polls involve many components including user’s registration and authentication, poll setup, polling (selected options chosen by the user are sent from the user’s connected device across the Internet to the relevant polling authorities), tabulation, result publication, auditing, and validation. Since the Internet-based polls involve three different environments (the poll user’s computing device such as a smartphone, a tablet, a desktop PC, etc., the Internet, and the polling system), a security attack on any part of the system can lead to an incorrect poll result. These three different environments and the information shared between them are vulnerable to various attacks, which must be prevented by the poll conducting administration or authority to provide similar to electronic voting (e-voting) systems, Internet-based polls are threatened by exactly the same security attacks, such as unauthenticated voting (a non-eligible voter may cast his/her votes), double voting (an eligible voter may cast multiple votes using his/her polling credentials), voter coercion (a voter is put under pressure or is threatened by a coercer to vote in a particular manner), vote buying (a voter is offered monetary benefits by a vote buyer to vote in a particular way or abstain from voting), vote modification by a voting device that is either controlled by a malicious program (e.g., malware, virus, etc.) or a hacker, who may cause unauthorized and potentially undetected alterations to voter’s selected voting choices, theft/forgery of voter’s identity (an attacker with access to credentials of an authenticated voter could cast votes using the identities of a legitimate voter), a coalition of malicious participants to alter or eliminate any voter’s vote, or cast fake ballots on the behalf of authenticated voter, and disclosure of partial vote tally before the end of the voting period. In scientific community, little attention has been paid to develop-polling systems, i.e., low-risk or small-level public opinion systems, where reasonable level of security, privacy and functionality should be provided to the end user. Instead, considerable amount of research work can be found related to design and implementation of secure, verifiable and practical remote voting systems for national-level or big elections.

II. CHALLENGES IDENTIFIED

The process of collecting data and entering this data into the database takes too much time and is expensive to conduct, for example, time and money is spent in imprinting data capture forms, in preparing registration stations together with human resources, and there after advertising the days set for registration process including sensitizing voters on the need for registration, as well as time spent on entering this data to the database. This system is being developed for use by everyone with a simple and self-explanatory GUI. This is software that can be used by people to vote in an election. All the user must do login according to their regional languages and click on his/his favorable candidates to register his vote. It consumes time and human resources. It is difficult to track who voted and who don’t, and it consumers try to announce polling results to overcome the challenges we introduced the online voting using AES algorithm.

III. PROBLEM DEFINITIONS

E-Voting System is a web-based system that facilitates the running of elections and surveys online. Users are individuals who interact with the system. All user interaction is performed remotely through the user’s web browser. Users are provided with an online registration form before voting user should fill online form and submit personal detail with finger print. Submitted details are encrypted and then store on database. Later the user can be login using voter id and given OTP. After successful login resubmit the voter id number with finger print. These details are compared with details in database and if they match then user can be enter vote section. If conditions are not correct entry will be cancelled. Prevent voters from voting more than once for their choose candidates therefore working load reduced by the way information available at the time. It also provides the security for data stored.

IV. PROPOSED METHODOLOGY

The approach prompt is also explained by following five modules:

A. Registration Process:

The Registration module allows the users to register their details and the information of the users are stored in the Database.

B. Generating QR-Code image:

Once the Registration process is completed, the QR-Code is generated for the particular user.

C. Login Process:

The Login module allows the user to upload their generated QR-Code image and is verified with Database.

D. User Validation Process:

This module allows the user to upload the QR-Code image to visit the polling page for
casting their votes.

E. Polling Process:
This module allows the user to enter into the polling page and cast their votes. After casting the user receives the “VOTED SUCCESSFULLY” message.

![Image of System Architecture](image)

Figure 1. System Architecture

V. ENVIRONMENT OF THE PROJECT

Development of the project based on web application using JAVA and SQL, the designed system allows the user to register their personal details, and the data is stored in the database in encrypted form which is further used for counting to announced results.

VI. CONCLUSION

This paper described Online Voting System Using AES Algorithm, an electronic polling system for small to medium sized Internet-based public opinion systems that provides privacy of vote, voter’s anonymity, voter’s authentication, auditability, poll integrity, security against coalition of malicious sparties, double-voting prevention, fairness, and coercion resistance, and prevents malware-infected voting device from manipulating the authenticated voter’s voting choices. In addition, Online Voting System Using AES Algorithm provides cast-as-intended verifiability based on cryptographic primitives, which are used to design a complex voting interaction between the voting device, the polling server, the code generator and compared to the other state-of-the-art e-voting systems, Online Voting System Using AES Algorithm ensures voter’s authenticity via multifactor authentication scheme, supports multiple voting, prevents double voting through a polling tag, offers verifiability in the presence of an untrusted voting device, requires less trust assumptions on involved entities, and offers computationally feasible solution for implementation on portable communication devices. As future work, we intend to develop a working prototype of Online Voting System Using AES Algorithm, and evaluate its scalability and usability in real-world deployment. Since the polling phase of Online Voting System Using AES Algorithm Requires voter’s participation,

REFERENCES


