www.ijrream.in Impact Factor: 2.9463

INTERNATIONAL JOURNAL OF RESEARCH REVIEW IN ENGINEERING AND MANAGEMENT (IJRREM)

Online Voting System using Gmail Verification

Prof. K. Poovazhaki, R. Sarankumar, K. Sakthivel, S. Karthick, B. Anbarasan

Department of Computer Science & Engineering

Bharathidasan Engineering College

ABSTRACT:

Advanced security methods are necessary to introduce effective online voting in the whole world further research is needed to improve security guarantees for future elections, to ensure the confidentiality of votes and enable the verification of their integrity and validity. In this paper, we propose online voting system using Gmail verification, which addresses these challenges. It eliminates all hardwired restrictions on the possible assignments of points to different candidates according to the voters' personal preferences. In order to protect the confidentiality of the votes, each cast ballot is encrypted using the using Homomorphic encryption before submission. Furthermore, during voting the system ensures that proofs are generated and stored for each element in the cast ballot. These proofs can then be used to verify the correctness and the eligibility of each ballot before counting without decrypting and accessing the content of the ballot. This validates the votes in the counting process and at the same time maintains confidentiality. The security and performance analyses included in this paper demonstrate that our method has achieved significant improvements in comparison with the previous systems. The outcomes of our experiments also show that our proposed protocols are feasible for practical implementations.

Key words - Election system, confidentiality, verification, security

1. INTRODUCTION:

"ONLINE VOTING SYSTEM" is an online voting technique. It is based on the other online services like "ONLINE RESERVATION SYSTEM". In this system people who have citizenship of INDIA and whose age is above 18 years of any sex can give his\her vote online without going to any polling booth. There is a DATABASE which is maintained by the ELECTION COMMISION OF INDIA in which all the names of voter with complete information is stored.

1. 1 Problem in Existing Systems

The existing system is manual and the paper based voting which is voted on paper and counted manually. The electronic tabulation brings new kind of voting system in which the electronic cards with all candidates symbol is marked manually and this can be counted electronically. The electronic voting systems are now different types known as the punch card, mark sense and the digital pen voting systems. The Electronic Ballot Marker makes the voter easier to vote by providing the selections on the display to vote present on the electronic machine.

The direct recording electronic voting machine is one which provides the display that can be start when the voter touches the display consists of the mechanical and electro optical buttons, software that accepts the vote and possesses a image or symbol on the display. The electronic ballots are connected with the central ballot systems which directly accept and get the updated record of all ballots. The central ballot system applies the Precinct count method which calculates the all votes from the ballots present at polling centers. The results are immediate.

2. PROPOSED SYSTEM

In proposed system remote and users can exercise. In the proposed system we can get the result without manually counting. The computerized counting is simple. In the proposed system we are using homomorphic algorithm. We speak of electronic voting when casting of votes is carried out by the voter directly by electronic means, thus obtaining an end to end digital vote .The use of paper and other physical systems is optional and auxiliary.

Eligibility of Voters: Only authorized voters can submit ballots.

Multiple Voting Detection: Each voter can only vote once. Multiple voting by any one voter is detected and identified.

Privacy of Voters: All votes must be stored securely and secretly and should not reveal voting preferences of the voters.

Integrity of Ballot: No one can modify or duplicate any submitted ballot without being detected.

Correctness of Tallied Result: Only verified ballots are counted and added to the final result.

End to End Voter Verifiable: Every voter is able to verify whether their vote is posted and counted correctly.

Contributions of this Paper: We propose a new e-voting system, which is more flexible than the previous systems. It uses encryption to achieve verification of the integrity of the voting process and the validity of the ballots, at the same time maintaining confidentiality of the users. Our e-voting system is an E2E voter verifiable voting system. Each ballot is encrypted by the Homomarphic encryption algorithm and contains proofs used in verification.

The proposed protocols achieve the following.

1. The information of each encrypted ballot can be added to other ballots without decrypting any votes.
2. Each encrypted ballot can be verified without revealing voting preferences. Only verified ballots are tallied for the final result.
3. Voters can verify that their ballots are submitted correctly to the pool.
4. Everyone is able to verify the eligibility of any voter's ballot without revealing voter's privacy.
5. Each voter can verify the correctness of the final tallied result.

3. ALGORITHM

Homomarphic algorithm we can use this paper. Homomorphic encryption is a form of encryption that allows computation on cipher texts, generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext.

These systems are slow because they use large keys in order to get the necessary security. FHS start with a SHS (all SHS are noisy encryption schemes). The construction of Gentry, found a way to refresh the ciphertext in order to decrease the noise (bootstrapping)

Homomorphic encryption can be used for privacy-preserving outsourced storage and computation. Homomorphic is working process

- Homomorphic basically repeats 4 major functions to encrypt data.
- It takes 128-bit block of data and a key [layman term password] and gives a cipher text as Output. The functions are Sub Bytes Shift Rows Mix Columns Add Key
- The number of rounds performed by the algorithm strictly depends on the size of key
- The following tables give overview of No. of rounds performed with the input of varying key lengths:

Key size (in bits).....	Rounds
128	10
192	12
256	14

Analysis of Steps:

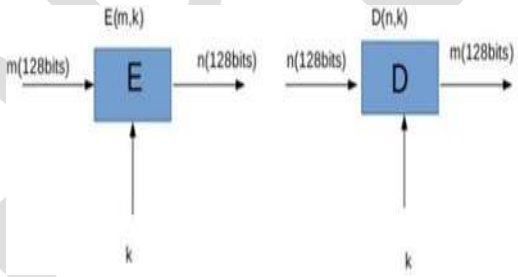
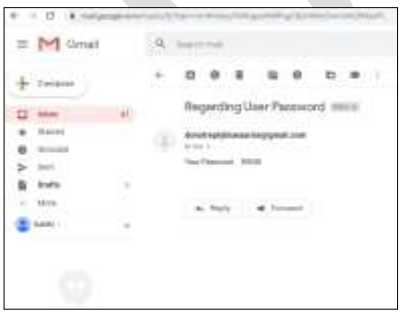


Fig. 1 Architecture



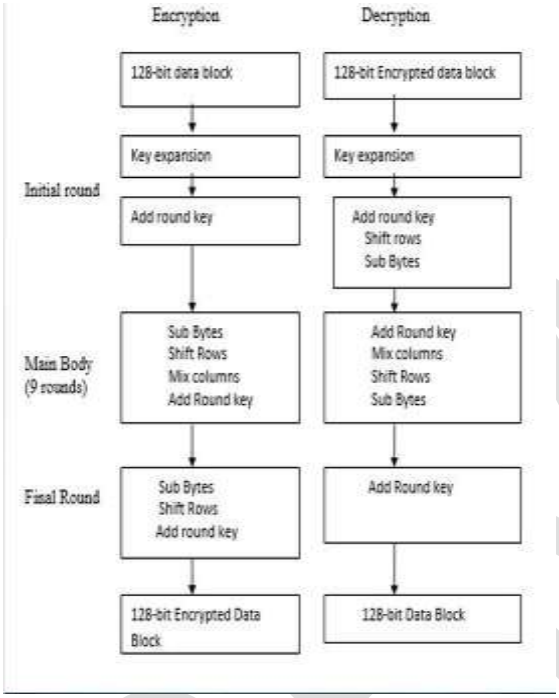


Fig.2 Screenshots

4. CONCLUSION:

This paper describes the proposed model for online voting system for India. The proposed system is much secure and efficient than the traditional voting system. Manipulation of votes and delay of results can be avoided easily. A unique AADHAAR identity is the centre point of our proposed model. It leads to the easier verification of both voters and candidates. In the proposed framework, we have tried to build a secure online voting system that is free from unauthorized access while casting votes by the voters. The server aspects of the proposed system have such distribution of authority that server does not enable to manipulate the votes. It is expected that the proposed online voting system will increase the transparency and reliability of the existing electoral system.

References:

1. Himanshu Agarwal, G. N. Pandey - Online Voting System for India Based on AADHAAR ID - Indian Institute of Information Technology.
2. Smitha B. Khairnar, P. Sanyasi Naidu, Reena Kharat - Secure Authentication for Online Voting System Pimpri Chinchwad College of Engineering, Pune.

3. Himanshu Vinod Purandre, Akash Ramswaroop Saini, Freddy Donald Pereira - Application for Online Voting System Using Android Device - St. John College of Engineering and Management, Palghar.
4. Hayam, Ketal ―The Patchwork of Internet Voting in Canada.
5. B. Rashidi, C. Fung, and E. Bertino, Android resource usage risk assessment using hidden Markov model and online learning,‘‘ Comput. Secure., vol. 65, pp. 90–107, Mar. 2017.
6. M. Gregory. (2016). Electronic Voting May be Faster but Carries Security Risks. [Online]. J. Lavelle and D. Kozaki. (2016). Electronic Voting has Advantages but Remains Vulnerable to Security, Software Problems. [Online]. Available: http://www.abc.net.au/news/2016-07- 11/electronic - voting has support-but- security-fears-remain/7587366
7. Tadayoshi Kohno, Adam Stubblefield, Aviel D.Rubin, Dan S. Wallach,“Analysis of an Electronic Voting System”, Johns Hopkins University Information Security Institute Technical Report, TR-2003-19, July 23,2003
8. Executive Summary of "Genesis and Spread of Maoist Violence and Appropriate State Strategy to Handle it", Bureau of Police Research and Development, Ministry of Home Affairs, New Delhi.
9. http://en.wikipedia.org/wiki/Electronic_ voting