 ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

Privacy Preservation in I-voting Using Homomorphic Technology

[1]Shubhangi S. Shinde, [2]Sonali Shukla, [3]D. K. Chitre
[1,2,3]Terna Engineering College, Nerul, Navi Mumbai, India

Abstract
Voting is one of the most important activities in a democratic society. In a usual voting environment voting process sometimes becomes quite difficult due to the unwillingness of certain voters to visit a polling booth to cast votes besides involving huge social and human resources. The advance of computer networks and security techniques help the implementation of electronic voting.
I-voting protocol is based on Homomorphic Technology and guarantees eligibility, unreusability, privacy, verifiability and also receipt-freeness and uncoercibility. The scheme can be implemented in a practical environment, since it does not use voting booth or untappable channel, only public channels are applied.
The proposed protocol encompasses three distinct phases - that of registration phase, voting phase and counting phase involving five parties, the voter, certification centre, authentication server, voting server and a tallying server.

Keywords
I-Voting, Homomorphic Technology, Elgamal, Multi-Authority, Threshold Sharing Key

I. Introduction

Democracy and elections have more than 2500 years of tradition. However, technology has always influenced and shaped the ways elections are held. In times past, different voting systems that are based on traditional paper ballots and mechanical devices were developed for elections.
As the computing, communicating, and cryptographic techniques progress rapidly, increasing emphasis has been placed on developing voting schemes that uses information and communications technology resources for providing more efficient voting services than conventional paper-based voting methods.
There is a need for research on secure cryptographic electronic election schemes. Internet voting system, compare to traditional paper-based elections, promise that election results will be calculated quickly with chance of less human error and also will reduce costs in a long-term period.
Internet voting has many advantages over the traditional way of voting. Some of these advantages are lesser cost, faster tabulation of results, greater accuracy, and lower risk of human and mechanical errors, it offers improved accessibility for the people with disabilities, and it provides multiple-language support for the ballots. Internet voting will increase voter convenience and voter confidence in the accuracy of election results.
A secured I-voting system should not only satisfy requirements of completeness, privacy, non-reusability, eligibility, fairness, verifiability, and robustness, but also receipt-freeness and non-coercion. The notions of receipt-freeness and coercion were introduced to deal with vote-selling and coercion in I-voting systems in. There are two threats were mentioned to address in a fair and democratic election process: voter coercion and vote buying. Internet-based voting does not introduce these problems, but it does have the potential to exacerbate them by extending the reach and data collection abilities of an attacker. In a voting system with coercers, a voting scheme must ensure that the voter should not be able to prove to a third party that he has cast a particular vote.

II. Proposed System

A. Registration Phase

Prior to the election, voters will have to prove their identity and eligibility. An electoral roll is created. The Trusted centre checks for the eligibility of each voter. The age of each person is checked and the national registration database to ensure he/she is not involved in crime before registration.
All voter information is sent to a database acting as the voters register which is kept safe by the trusted centre. Also, biometric features like fingerprint or face recognition can be very useful during registration of voters.
The voter will provide a username along with a pass code that is randomly generated by the computer to log-in during the validation phase.

B. Validation Phase

During the election, voters are authenticated before casting their vote. This is similar to manual voters verification in the traditional system of voting to ensure that the registration numbers are confirmed on the voters register.
Each voter will have to supply the pair of username and pass code. When a voter is authenticated, he can now vote for the candidate of his choice, otherwise, he will be denied access. It should be noted that only one vote per voter is allowed in this I-voting system.

C. Vote Casting Phase

Voters cast their vote. Each voters choice is directly transferred to the tallying phase. In this phase, we want to ensure anonymity, non-coercion and receipt-freeness. Anonymity ensures that each vote cannot be linked to the person that cast it. When there is receipt-freeness and no coercion, the voter will not be able to prove to the coercer the way he voted or to receive a receipt (bribe). The best way to do this is by encryption.
Modified ElGamal cryptosystem that is additive homomorphic and satisfies threshold cryptography will be used. Each voter ballot is digitally signed with EDSA (ElGamal DSA) and encrypted with the additive ElGamal scheme.
The election counter verifies the ballot, and if it passes this stage, it will accept the voter ballot because it is coming from the right source (to ensure non-repudiation of origin). The authorities monitor the voting process.

D. Tallying Phase

In this phase, all encrypted votes for all voters are decrypted and counted since each vote is sent to this phase for n-voters. At the end of the election process, there is need for audit trail where voter results are verified by the trusted centre and the whole result is made known.
The authenticator publishes the list containing the encrypted ballots and the ballot ID. The election counter publishes its version of the same list and the verifier confirms that these lists are identical to ensure fairness.

IV. Methodology Used

A. Homomorphic Technology

Voting systems using homomorphic encryption work with a communication model called bulletin board. It is a public broadcast channel with memory. All information sent to the bulletin board is readable by everyone. Every authorized user can add messages to his own area, but no one can delete any data from the board.

The central element of the homomorphic encryption is the feasibility to sum up data without decrypting them, i.e. without knowing the exact content of the data. This is a feature that is typical of the principle of homomorphism. More precisely speaking, the homomorphic encryption ensures the mathematical law that the product of encrypted data is the encryption of the sum of the data:

$Enc(v_1) *...* Enc(v_n) = Enc(v_1 +...+ v_n)$.

The method works as follows: Before the election, the talliers generate distributed asymmetric keys (e.g. Threshold cryptography). These keys are a single public encryption key and for each tallier a secret decryption key. To decrypt a message encrypted with the public key, more than at least half of the secret keys have to be used. Therefore more than half of the talliers would have to be corrupted in order to break the anonymity or manipulate the election result.

Only authenticated voters are allowed to write on the bulletin board. The voters send their votes encrypted with the public part of the distributed key to the bulletin board, together with a zero knowledge proof of correctness. After the voting phase, the talliers take all the encrypted votes from the bulletin board and form their homomorphic sum. Afterwards this sum is decrypted using the distributed parts of the key and sent to the bulletin board with proofs of correctness of the summation and the decryption. By skillful application of zero knowledge proofs, and because everybody (even external observers) can read the information on the bulletin board, everyone can verify the correctness of the results. This includes the correct summation and the completeness of votes included.

Online voting systems with homomorphic encryption secure, in particular, the casting of correctly formed votes as well as a correct counting. This is verifiable during the election, and in addition, remains verifiable after the election. However, this encryption type cannot monitor the proper execution of the election.

In order to trace the execution, an additional audit logging is necessary. Since the information on the bulletin board can be used for verification, less information is probably needed for the audit logging compared with systems that use blind signatures.

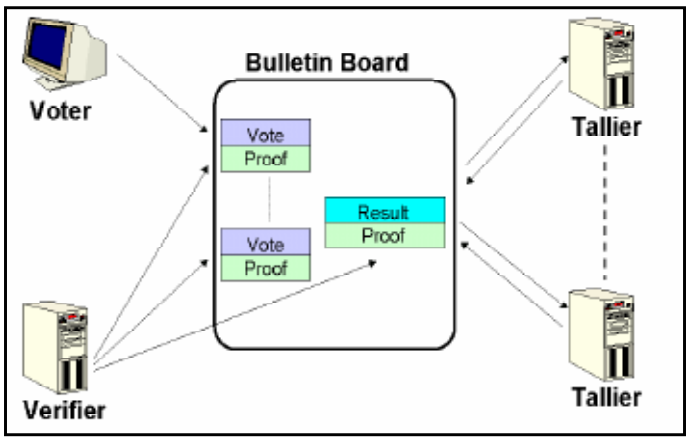

Fig. 1: Schematic View of an e-voting System Using Homomorphic Encryption

IV. Performance Evaluation

Security Analysis & Performance Measurement

1. Completeness: No fake vote and sum of valid ballots are accurately counted in the proposed I-voting scheme.
2. Privacy: In the proposed I-voting scheme, all ballots are secret (not linked to voters)
3. No vote duplication: in the proposed I-voting scheme, a voter can vote twice.
4. Eligibility: In the proposed I-voting scheme, only eligible voters can vote.
5. Fairness: No one can know the intermediate results of the voting in the proposed I-voting scheme.
6. Universal verifiability and Correctness: In the proposed I-voting scheme, the public can verify the voting system.
7. Receipt-freeness: In the proposed I-voting scheme, the voter cannot reveal his ballot to others.
8. Non-coercion: In the proposed I-voting scheme, a voter cannot be coerced into casting a particular ballot by a coercer.

V. Conclusion

Many countries have not fully implemented I-voting systems because of the associated security challenges. Any little security flaw in the design of a secure I-voting can cause a very severe electoral fraud more than the conventional voting system. In our proposed scheme, we have ensured that all the requirements to design a secure I-voting are kept in mind. The scheme ensures eligibility, completeness, privacy, efficiency, universal verifiability, no vote duplication, non-coercion and receipt-freeness. The Homomorphic Technology scheme is also practical to be used for real election.

It might be necessary for researchers to look at the implications of Homomorphic Technology scheme on the overall voting process. This scheme ensures the privacy of the voters and prevents any disruption by voters or the administrators. The implemented scheme covers most of the security requirements of the internet voting scheme including voting fairness. The problem of computer and the Internet security has taken a prominent and important place in today's research area. Since electronic election is a part of these applications, it is of supreme importance as we will consider its emerging advantages in today's modern life. This problem is open, researches in different universities and laboratories are still going on.

Different protocols are emerging by the day, each with a hint of advancement over the other. With the growing use of internet in these days, it is evident that better and more secure protocols would come to the fore and their practicality can be exploited to meet the growing security needs.

References

[1] Okediran O. O., Omidiora E. O., Olabiyisi S. O.,"A Survey of Remote Internet Voting Vulnerabilities", World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741, Vol. 1, No. 7, 297-301, 2011.

[2] Bo Meng,"A Secure Internet Voting Protocol Based on Noninteractive Deniable Authentication Protocol and Proof Protocol that Two Ciphertexts are Encryption of the Same Plaintext", Journal of Networks, Vol. 4, No. 5, JULY 2009.

[3] B. Meng, J.Q. Wang,"An efficient receiver deniable encryption scheme and its applications", Journal of Networks, Vol. 5, No. 6, pp. 683– 690, 2010.

[4] Okediran Oladotun Olusola, Omidiora Elijah Olusayo, Olabiyisi Stephen Olatunde, Ganiyu Rafiu Adesina,"A

Review of the Underlying Journal of Networks Concepts of Electronic Voting", Information and Knowledge Management, Vol. 2, No. 1, 2012.
[5] Omidiora E. O., Olabiyisi S. O., Ganiyu R. A. , Alo O. O.,"A Framework for a Multifaceted electronic voting system", International Journal of Applied Science and Technology, Vol. 1, No. 4, July 2011.
[6] Xun Yi., Eiji Okamoto,"Practical Remote End-to-End Voting Scheme", EGOVIS 2011, LNCS 6866, pp. 386–400, 2011, Springer Verlag Berlin Heidelberg 2011.
[7] Nitin jain, Saibal K. Pal, Dhananjay K. Upadhyay, "Implementation and analysis of Homomorphic encryption schemes", IJCIS, Vol. 2, No. 2, June 2012.
[8] Sadegh Jafari, Jaber Karimpour,"A new secure and practical electronic voting protocol without revealing voters identity", International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 6, pp. 2191-2199 June 2011.
[9] Adewole A. Philip, Sodiya Adesina Simon, Arowolo Oluremi. A., "A Receipt-free Multi-Authority I-voting System", International Journal of Computer Applications, Vol. 30, No. 6, September 2011.
[10] William Stalllings, Cryptography & Network Security, Fourth Edition, Pearson Education, 2006.

Ms. Shubhangi Shinde is student of ME IInd Department of Computer Engineering with Terna Engineering College Nerul Navi Mumbai. Her area of interest includes Network Security.

Mrs. Sonali Shukla is currently working with Department of Computer Engineering as Assistant Professor with Terna Engineering College Nerul Navi Mumbai. Her area of interest includes Artificial Intelligence and Databases.

Mr. D. K. Chitre has been working as Associate Professor and Head of Department in Computer Engineering Department, Terna college of Engineering, Nerul, Navi Mumbai.