Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 10, October 2019

E-voting system

Ms. M Rajani Shree
Faculty of Engineering and Technology
Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email Id: m.rajanishree@jainuniversity.ac.in

Abstract

The systems of e-voting are becoming popular with the widespread use of embedded devices and computers. Protection is security in such systems, the main problem should be considered. This article proposes a new method for e-voting that fulfils the protection E-voting criteria. It is based on homomorphic properties that are schemes of blind signatures. Implementation of the proposed scheme on an integrated machine that functions as a voting unit. The RFID is used in the system to store all requirements that comply with the government's law of testing qualifications for voters.

Keywords: *Blind Signature, E-voting system, Paillier cryptosystem, Security, Technology.*

I. INTRODUCTION

For democracy, one of the basic structures is elections. This is the way to gather the views of the public to form a democratic administration. The standard election method is it's pretty boring, time consuming and cumbersome[1]. Procedure for stages of planning and tallying. Overcoming these problems have been raised by the electronic voting system (EVS). As long as the planet gets more, EVS continues to expand reliably in terms of emerging technology. EVS offers a great deal of benefits than conventional methods for voting. It attempts to allow elections easily and efficiently. EVS is inexpensive because of the fact that the assets are reusable. It also doesn't need any and it offers greater geographical proximity to candidates, for broad elections, scalability[2].

Using EVS, meanwhile, must comply with such security criteria, such as authentication, voting, privacy, secrecy, honesty, etc. Many vulnerabilities in security since EVS is more fragile than traditional was discovered in the voting phase[3]. Digital data processing makes it possible for every vote manipulation, updating or copying. That is why these outcomes in a massive campaign of bribery on election day[4]. Thus many Professionals shared their adverse views on e-voting. Nonetheless, attempts are still being made to enforce EVS in countries that use conventional ballots on paper[5].

One Central adopts the proposed e-voting method facility for tabulation (CTF) gathering all secret ballots from servers of the local committee that spread between polls with stations. Each server is linked to a server at each polling station[6]. The number of embedded systems that are considered voting terminals used for the creation of voter ballots. The planned framework uses the two homomorphic cryptosystems that have been introduced using RSA-based Paillier

cryptosystem and blind signature. The method is carried out in five distinctive phases: approving, authorizing, phases of voting, authenticating, and tallying. This paper presents a new EVS which employs the Homomorphic property and RSA dependent blind signature. The paper is structured as follows; the critical safety EVS in, the specifications are defined. defines Major security instruments[7]. The specifics of the e-voting proposed the system and its various stages are described in detail in. Study of the scheme proposed from the point of view of Protection is illustrated.

II. DISCUSSION

A. ELECTRONIC VOTING SECURITY REQUIREMENT:-

First and foremost, protection and accuracy are requirements for every scheme for voting.

- Eligibility: only approved voters who meet a predetermined requirement will be able to vote.
- Uniqueness: nobody is allowed to vote more than once.
- Privacy: a vote is kept private and no one can decide. For whom someone else has elected,
- Integrity: the democratic process is secure, so that no one can without being found, change the vote of someone else. In addition, no one can replicate someone else's vote.
- Accuracy: Every voter should guarantee that his vote has been cast.

B. Authorizing phase:-

The authorization stage is the first stage of the proposed e-system for elections. When a voter arrives at the polling station, it begins with his RFID and national ID. The primary function of this process is to check the identification and qualifications of the voters. The identity of the ballot is checked by a section of the body that tests the national voter ID. That is why this aspect of the process is a process regulated by humans. Voter eligibility is verified by the passive RFID of voters. A card prepared by the government prior to election day. The Condition of the voting against each restriction is stored as a flag bit that if voters satisfy this restriction or logic zero, it is equivalent to logic one. Eh, if not. A single byte storage area is consumed by all these flags. In addition, to store the voter's name, forty bytes are needed. Since this method is proposed for any form of election, a portion is proposed for RFID memory that is reserved for the sort of option to be stored[8].

C. Voting phase:-

Voting after confirming the identity and eligibility of a voter, a process begins. The voting terminal shows an empty terminal at this point, so the qualifying elector chooses his candidate

and designs his ballot. The voting terminal subsequently stores all ballots created by voters in ML tables where the number of voters is L nominees and M is a number of voter's ballots[9].

D. Authentication phase:-

Authentication implies that it should be feasible for the to determine its origin, the receiver of a message; an intruder should be unable as someone else to masquerade. In our, blind RSA-based device signature is used for authentication[10].

E. Tallying phase:-

This stage begins with the transmission of signed votes to CTFF. That unblinds them, as shown in Equation 3. Subsequently CTF decrypts the unblended message arising from this. Owing to the Paillier cryptosystem's additive homomorphic property, the consequence of the decryption would be the addition of the prime the YES and NO Numbers of Votes

F. SECURITY ANALYSIS:-

1. Eligibility:-

This requirement is accomplished by RFID voting. The Elector until the voting terminal checks the content, he will not cast his vote. RFID of a voter. The state is planning and encrypting this data with a public key encryption algorithm. The vote through a private key, the terminal decrypts it. This part of security is the security part beyond this paper's meaning[11].

2. Uniqueness:-

It is possible to achieve this protection requirement in the step of elections. The form of election field stored in the RFID of voters that fulfils this requirement. This area consists of the option of date and flag bit that is raised every time his vote is cast by a voter. As a result, it is unlikely for people to vote again.

3. Privacy:-

This requirement requires voting to be concealed and no one can know to vote for anyone else. Using an RSA based blind signature the system given that the vote is blinded so that it is not going to be disclosed to the local committee (authority party). Furthermore, during the voting decision, the authority group does not learn the decision of the voter during subscription. The blind signature has another benefit: the blind signature voting is disassociated with voting details such that no one can recognize the vote to which a vote belongs.

4. Accuracy:-

This can be fulfilled by using the RSA-based blind signature obligation. Both votes in the voting process are blinded and then signed in the Process of Authentication. Consequently,

only the CTF counts the Votos signed. In addition, verification step satisfies this necessity by comparing local committee ballots for the one in CTF tallied.

III. CONCLUSION

A new EVS is introduced in this article. It uses Pailier for RSA-based cryptosystem and blind signature as authentication instruments. It consists of a CTF that interacts with many local committee servers spread between polling stations. Each server is linked to a collection of embedded systems. Serving as machines for elections. The device meets the critical requirements regarding protection. The cryptosystem of Pailier offers the due to its additive homomorphic secrecy requirement, Property, which makes it possible for the CTF to count the secret votes without decoding them. The RSA-based blind signature blinds the votes and voter identity to achieve privacy and accuracy requirements regarding protection. Eligibility and singularity are satisfied by the details contained in the voter's RFID.

IV. REFERENCES

[1] A. Al-Ameen and S. Talab, “The technical feasibility and security of E-Voting,” Int. Arab J. Inf. Technol., 2013.

[2] F. P. Hjalmarsson, G. K. Hreioarsson, M. Hamdaqa, and G. Hjalmtysson, “Blockchain-Based E-Voting System,” 2018, doi: 10.1109/CLOUD.2018.00151.

[3] D. Lavarino, “RANCANG BANGUN E â€“ VOTING BERBASIS WEBSITE DI UNIVERSITAS NEGERI SURABAYA,” J. Manaj. Inform., 2016.

[4] E. Aljarrah, H. Elrehail, and B. Aababneh, “E-voting in Jordan: Assessing readiness and developing a system,” Computers in Human Behavior. 2016, doi: 10.1016/j.chb.2016.05.076.

[5] B. Ondrisek, “E-voting system security optimization,” 2009, doi: 10.1109/HICSS.2009.173.

[6] K. M. Khan, J. Arshad, and M. M. Khan, “Secure digital voting system based on blockchain technology,” Int. J. Electron. Gov. Res., 2018, doi: 10.4018/IJEGR.2018010103.

[7] L. Chiang, “Trust and security in the e-voting system,” Electron. Gov., 2009, doi: 10.1504/EG.2009.027782.

[8] L. C. Schaupp and L. Carter, “E-voting: From apathy to adoption,” Journal of Enterprise Information Management. 2005, doi: 10.1108/17410390510624025.

[9] E. Smith and A. Macintosh, “E-voting: Powerful symbol of e-democracy,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), 2003, doi: 10.1007/10929179_43.

[10] J. J. Piles, J. L. Salazar, J. Ruíz, and J. M. Moreno-Jiménez, “The voting challenges in e-cognocracy,” 2006.

[11] A. Kiayias, M. Korman, and D. Walluck, “An internet voting system supporting user privacy,” 2006, doi: 10.1109/ACSAC.2006.12.