

Secure E - Voting System Based on Paillier Cryptography

Bharati Raut, Manasi Jagtap, Sneha Ghule, Kshitija Jadhav, Prof. S. P. Aundhakar

Department of Computer Engineering, PVPIT, Pune, Maharashtra, India

ABSTRACT

In the whole world the advanced security procedures are necessary to present convincing online based casting a ballot (e-voting). Trust in the voting process is therefore an important element to any voting system. Voting over the internet is not secure enough to be trusted for government elections. Choices integrated on the paper exhaust many advantages and add to the confusion of backwoods, which causes atmosphere weakening. Then web based casting a ballot come up in countries like the US, India and Brazil showed that further examination is needed to enhance the security assures for future race, to provide the characterization of votes and enable the affirmation of their reliability and legitimacy. Here, proposed the homomorphic encryption based e-voting for casting a vote, which locate these challenges. It removes every single limitation on the possible assignments of centers to different competitors as per the voters' individual inclinations. In order to ensure the security of the votes, each cast vote is encrypt utilizing the paillier cryptosystem before counting of votes. Moreover, amid casting a ballot the framework guarantees that proofs are created and put away for every component in the cast ballot. These confirmations would then be able to be utilize to affirm the rightness and the qualification of each ballot prior to checking without unscrambling and getting to the substance of the tally. This approves the votes in the verification procedure also, in the meantime looks after classification. To enhance the security of our system we utilized OTP (SMS gateway) for login. The security and execution assessments added together show that our system has achieves critical enhancements in examination with the existing system.

Keywords : E Voting, Homomorphic Encryption, Privacy Preservation, Paillier Cryptosystem.

I. INTRODUCTION

In last two decades, various kinds of electronic voting frameworks have impressive consideration. Electronic voting deal with the election process simple and generally productive for political parties, candidates, election administration, and for voters [19]. Additionally, there are numerous problems in the electronic voting framework, such as system errors, network security, data security, However, offering online voting also makes it available to every spy, gangster, mercenary, and hacker on the planet.

Attackers could easily violate the sanctity of the secret ballot, modify votes, or even make the web application unavailable to certain voters on polling day etc. For developing countries or nations like Egypt, many voting schemes are emerging with newer strategies [18]. Consider an India as a case study a system should create with security of the voting data for direct deployment. Efficiency and cost saving provided by e-voting system. When data is on online server, security plays vary vital role due to data may get accessible for intruders. One of the main issue is cheating committed by outsiders or even the

administrator himself in manipulating the data that will be utilized or stored. We cannot simply put confidential voting data on an online server. To resolve this issue, encryption of data is to be done before sending it to the server. For encryption of data, various algorithms can be utilized, among which ElGamal, Okamoto-Uchiyama & Paillier are now-a-days most likely to be utilized [1]. Paillier algorithm is an asymmetric cryptographic algorithm. In an asymmetric cryptosystem to encrypt data, a public key is utilized and a private key is utilized to decrypt the data. The public key is shared among a number of parties that is the sender and receiver for performing encryption and decryption. The algorithm displays additional homomorphic properties. Homomorphic encryption grants computation over encrypted data for generating an encrypted result. The decrypted result and the result of operations matches as if they had performed on plaintext. This property is used to hide the vital voting data from a counting system. Here we presented an approach for secure authentication of users for e-voting which can be done from anywhere around the universe. Here homomorphic encryption is utilized for security purposes. With implementation of the Paillier algorithm, we examine the time taken by an algorithm and compare the performance of the proposed system with existing systems. Also, we go to analyse the similarities and variations of existing systems with our proposed system. In the proposed system, we will make sure that there will not be a violation of user credentials at the authentication stage, we also make sure the vote given by a voter will not be changed as their values are encrypted and as we utilize an algorithm with homomorphic property it will not be revealed at transferring on server. Also, during voting, the system assures that proofs are generated and stored for each element in the cast ballot. These proofs are then used to verify the correctness and the eligibility of each ballot before counting without decrypting and accessing the content of the ballot. This process validates the votes in the counting process and also maintains confidentiality.

The organization of this document is as follows. In Section 2 (Literature Survey), we enlisted details of all research that existed. In Section 3 (System Architecture), we present the architecture of the proposed system. In Section 4 (Result and Discussion) we discussed the experimental setup and the database / dataset used is discussed. In Section 5 (Conclusion) we discussed the conclusion and future work required to improve our system.

II. LITERATURE SURVEY

The main aim of this work is to develop an interactive voting system application [1] with which users can participate utilizing their information stored prior in a database while creating the voter ID and the information needs to be updated at a period of less than six months for exact user verification by the Independent Electoral Commission of India (IECI). Here in the system, people who have citizenship of India and whose age is above 18 years and of any sex can give their vote via online without going to any physical polling station.

On the assumption of extremely huge elections, the nature of casting a ballot framework [2] is something critical to examine. This technique consists with one downside, for example, mixnet finds ballots consolidate with a duplicate credential. It is conceivable by expanding electronic watermarking, reducing the measure of tasks in the computing section. Founded same authorized as well as duplicate watermarked ballots and elimination of duplicate watermarked ballots may decrease the amount of ballots within input of mixnet. Author has ability to use algorithm presented by Walton in JCJ technique to guarantee the integrity of ballot and especially the property of coercion protection. JCJ strategy is conceivable for all intents and all purposes if author utilizes watermarking and diminishes difficulty of computing.

Prof. S.M. Jambhulkar et al. [3] developed web based internet voting system, in that author justifies the protection to vote. For the most part security is necessary when vote transfer from casting a ballot customer to casting a ballot server. Creator solid apparatuses are the idea of number of encryption and decryption.

In paper [4], safe sensor network used to observe interaction performance by AES encryption algorithm based on plaintext size as well as value of operation per hop related to the network scale.

To achieve protection by e-voting a new e-voting system is proposed [5]. Provided security is depends on homomorphic property and blind signature method. Installed framework is utilized as casting a ballot machine and on that machine proposed framework is actualized. All guidelines of government is put away with utilization of RFID to break down voter is qualification.

E-voting [6] system is altered time-to-time related with progress of the regulative environment with arising many questions. Here presented to make examination of implemented existing vote authentication methods and their weaknesses and analysis is utilized to propose a new trustworthy and robust vote authentication method.

Recently election and voting [7] proposed to execute electronically. Web services plays vital role due to its five advantages and utilization as well as implementation of e-voting systems. Implementation of web services several big reliabilities as well as security issues. E-voting system proposed which rely on web services. The proposed system is developed on the basis of stochastic Petri nets (SPNs) and reliability and security are estimated.

Chun-Ta Li et al. [8] presented many electronic voting methods are shows that voters may confirm voting

outcomes. Unluckily, attributes of verifiability will motivate ballot buying. Author proposes an electronic voting protocol for fascinates all security needs and allows voter to take decision about cast ballot counted appropriately or not as well as not motivate to ballot purchasing.

Drew Springall, Travis Finkenauer, Zakir Durumeric et al. [9] examines the security of the Estonian I-voting system depends on a combination of in-person election observation, code review, and adversarial testing. In experimental attacks on a reproduction of the system, we demonstrate how such attackers could target the election servers or voters' clients to alter election results or undermine the legitimacy of the system.

Kausal Malladi, Srivatsan Sridharan et al. [10] proposes a robust e-voting system with Automated Teller Machine (ATM) terminals and Micro ATMs. The proposed approach ensures duplicate vote avoidance through dual-tier authentication using One Time Password (OTP) and a Random Security Question (RSQ). To further enhance the security of such a public voting mechanism, the proposed approach assigns arbitrary Candidate IDs (CIDs) to contestants. This assures voting privacy of a voter.

III. SYSTEM ARCHITECTURE

A. System Architecture

Following fig. 1 shows the proposed framework design. The system includes various modules such as user registration, user login, admin login, voting, homomorphic key generation, encryption, decryption and final vote counting on encrypted data also verification of ballot. In our work we used Paillier cryptosystem which is asymmetric homomorphic encryption algorithm.

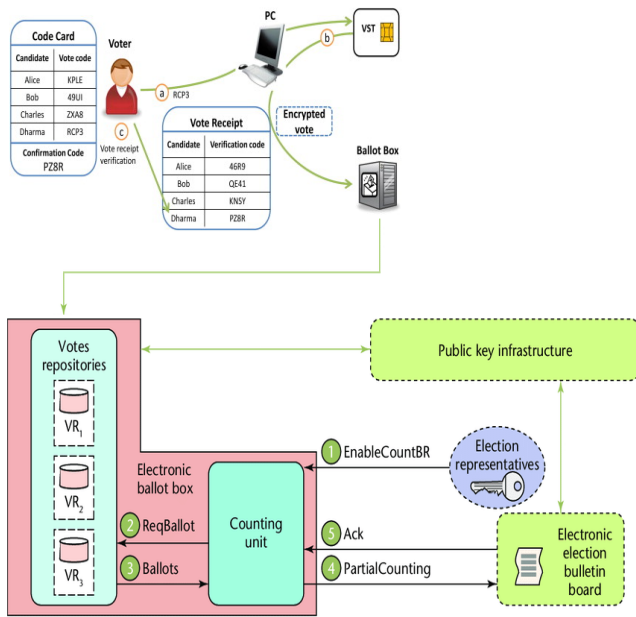


Figure 1: System Architecture

B. Asymmetric Encryption Algorithm

Asymmetric cryptography or also can be called public key cryptography is a cryptographic key that has a pair of related keys, which is public key to encode the messages, and private key to decrypt the messages. As the name implies, the public key can be put in a public place where everyone can access it, while the private key can only be accessed by its owner only. The purpose of the existence of asymmetric cryptography is to minimize the number of locks required to perform cryptographic processes. Imagine if there will be a thousand people will communicate, then if not using an asymmetric key algorithm, it would take a thousand different keys, course it is not practical. If using asymmetric cryptography, then simply store the private key that is owned by the owner alone [17].

C. Paillier Algorithm

Key Generation:

- Select two large prime numbers a and b arbitrary and independent of each other such that $\gcd(n, \Phi(n)) = 1$, where $\Phi(n)$ is Euler Function and $n=pq$.
- Calculate RSA modulus $n = pq$ and Carmichael's function is given by $\lambda = \text{lcm}(p-1, q-1)$.

- Select g called generator where $g \in \mathbb{Z}_{n^2}^*$ Select α and β randomly from a set \mathbb{Z}_n^+ then calculate $g = (\alpha n + 1) \beta^n \text{mod } n^2$.
- Compute the following modular multiplicative inverse $\mu = (L(g^\lambda \text{mod } n^2)^{-1} \text{mod } n)$. Where the function L is defined as $L(u) = (u-1)/n$.
- The public (encryption) key is $(n$ and $g)$.
- The private (decryption) key is $(\lambda$ and $\mu)$.

Encryption:

- Let mess be a message to be encrypted where $\text{mess} \in \mathbb{Z}_n$.
- Select random r where $r \in \mathbb{Z}_{n^2}^*$.
- The cipher text can be calculated as:

$$\text{cipher} = g^{\text{mess} \cdot r^n} \text{mod } n^2.$$

Decryption:

- Cipher text $c \in \mathbb{Z}_{n^2}^*$
- Original message: $\text{mess} = L(c^{\lambda} \text{mod } n^2) \cdot \mu \text{mod } n$.

IV.RESULT AND DISCUSSION

A. Dataset / Database used

The system uses user registration information as dataset and to store data, encryption key, users vote, etc. mysql database is used.

B. Experimental Setup

All the experimental cases are implemented in Java in congestion with Eclipse tools, algorithms and strategies, and the competing user behavior approach along with data encryption technique, and run in environment with System having configuration of Intel Core i5-6200U, 2.30 GHz Windows 10 (64 bit) machine with 8GB of RAM.

C. Results

Figure 2 show encryption time comparison graph, proposed system (Paillier Encryption) requires less time compare to existing system.

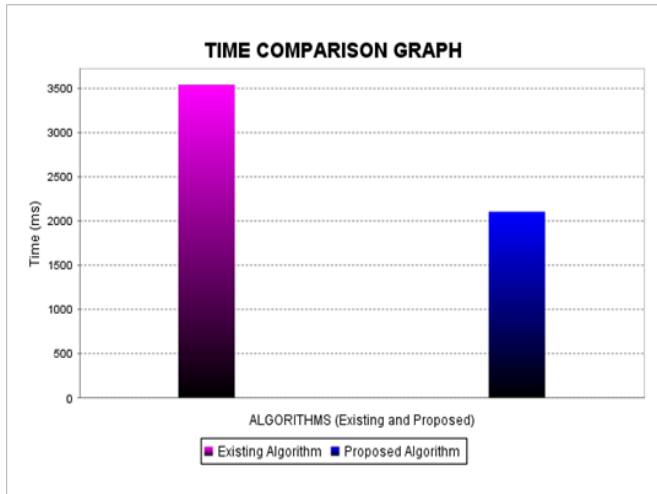


Figure 2: Time Comparison Graph

Figure 3 show encryption memory comparison graph, proposed system (Paillier Encryption) requires less memory compare to existing system.

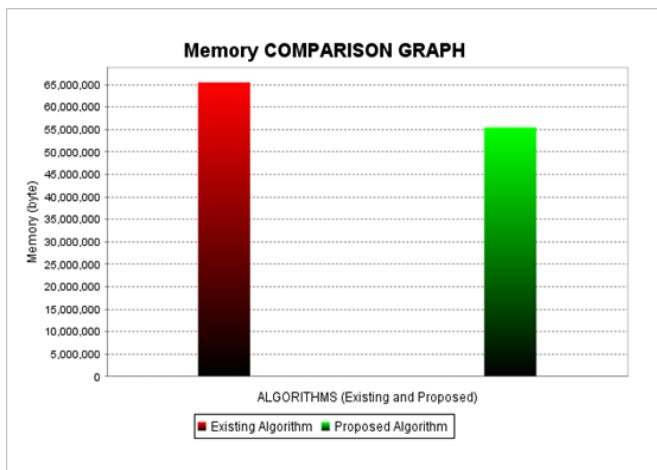


Figure 3: Memory Comparison Graph

V. CONCLUSION

Here presented new secure e-voting system for instant runoff voting. For that utilized Homomorphic encryption and blind signature. Homomorphic encryption gives confidentiality to casted ballot. The blind signature blinds the casted ballot to achieve anonymity and privacy of voter. It rejects the utilization of manual casting a ballot procedure and gives instant results in secure way. No one will forge votes on behalf of others and multiple times. This

casting a ballot technique will save time and reduces human intervention. The system is flexible and secured to be used. Limitation of proposed system is that we have to assume that at least one authority is honest, since otherwise the system is not secure. In future work, we plan to locate this issue and potentially could consider further generalizations.

VI. REFERENCES

- [1]. Amritkar, Manjusha & Dudhe, Roshani & Sawant, Komal & Phutane, Shraddha & Dadhich, Puneet. (2016). Secure Online Voting System. International Journal of Advanced Research. 4. 1648-1653. 10.21474/IJAR01/2257.
- [2]. Souheib, Y., Stephane, D., Riadh, R, "Watermarking in e-voting for large scale election", Multimedia Computing and Systems (ICMCS), 2012 International Conference on Date of Conference: 10-12 May 2012.
- [3]. Prof. S.M. Jambhulkar, Prof. Jagdish B. Chakole, Prof. Praful. R. Pardhi," A Secure Approach for Web Based Internet Voting System using Multiple Encryption", 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies.
- [4]. Hyubgun Lee, Kyoungwha Lee, Yongtae Shin, "AES Implementation and Performance Evaluation on 8-bit Microcontrollers", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6 No. 1, 2009
- [5]. Hussien, H., Aboelnaga, H., "Design of a secured e-voting system", Computer Applications Technology (ICCAT), 2013 International Conference on Date of Conference: 20-22 Jan. 2013.
- [6]. Al-Shammari, A.F.N., Weldmariam, K., Villafiorita, A., Tessaria, S., "Vote verification through open standard: A roadmap", Requirements Engineering for Electronic Voting Systems (REVOTE), 2011 International Workshop on Date of Conference: 29-29 Aug. 2011. 20
- [7]. Omidi, A., Azgomi, M.A., "An architecture for e-voting systems based on dependable web services",

- Innovations in Information Technology, 2009. IIT '09. International Conference on Date of Conference: 15-17 Dec. 2009.
- [8]. Chun-Ta Li, Dept. of Inf. Manage., Tainan Univ. of Technol., Tainan, Min-Shiang Hwang, Yan-Chi Lai "A Verifiable Electronic Voting Scheme over the Internet", Information Technology: New Generations, 2009. ITNG '09. Sixth International Conference on Date of Conference: 27-29 April 2009.
- [9]. Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, J. Alex Halderman "Security Analysis of the Estonian Internet Voting System" CCS'14, ACM 978-1-4503-2957-6/14/11. November 3-7, 2014, Scottsdale, Arizona, USA.
- [10]. Kausal Malladi, Srivatsan Sridharan, L. T. Jay Prakash "Architecting A Large-Scale Ubiquitous E-voting Solution for Conducting Government Elections" 2014 International Conference on Advances in Electronics, Computers and Communications (ICAIECC)
- [11]. X. Yang, X. Yi, S. Nepal, A. Kelarev and F. Han, "A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption," in IEEE Access, vol. 6, pp. 20506-20519, 2018. doi: 10.1109/ACCESS.2018.2817518
- [12]. A. Ara, M. Al-Rodhaan, Y. Tian, and A. Al-Dhelaan, "A secure privacy preserving data aggregation scheme based on bilinear elgamal cryptosystem for remote health monitoring systems," IEEE Access, vol. 5, pp. 12 601-12 617, 2017.
- [13]. L. Chen, M. Lim, and Z. Fan, "A public key compression scheme for fully homomorphic encryption based on quadratic parameters with correction," IEEE Access, vol. 5, pp. 17 692-17 700, 2017.
- [14]. Z. Li, C. Ma, and D. Wang, "Towards multi-hop homomorphic identity based proxy re-encryption via branching program," IEEE Access, vol. 5, pp. 16 214-16 228, 2017.
- [15]. X. Yi, R. Paulet, and E. Bertino, Homomorphic Encryption and Applications. New York: Springer, 2014.
- [16]. C. Esposito, A. Castiglione, B. Martini, and K.-K. R. Choo, "Cloud manufacturing: Security, privacy, and forensic concerns," IEEE Cloud Computing, vol. 3, pp. 16-22, 2016.
- [17]. R. Jubiya, M. Keirthis, M. Anupriya, A. Muthukumar, "IRIS Authentication Based On AES Algorithm", Volume 3, Special Issue 3, March 2014
- [18]. Ngo Cuong. 2014. Secure Voting System Using Paillier Homomorphic Encryption. Faculty of the Department of Computing Sciences Texas A&M University – Corpus Christi, Texas.
- [19]. Shifa Manaruliesya Anggriane, Surya Michrandi Nasution, Fairuz Azmi R. Nicole, "Advanced e-voting system using Paillier homomorphic encryption algorithm" in E-voting system" in IEEE Trans. ISBN 978-1-5090-1648-8, International Conference on Informatics and Computing (ICIC), 2016.
- [20]. Pranay R. Pashine, Dhiraj P. Ninave, Mahendra R. Kelapure, Sushil L. Raut, Rahul S. Rangari, Kamal O. Hajari. "A Remotely Secure E-Voting and Social Governance System Using Android Platform", International Journal of Engineering Trends and Technology (IJETT), V9(13), 671-676 March 2014. ISSN:2231-5381.

Cite this article as :

Bharati Raut, Manasi Jagtap, Sneha Ghule, Kshitija Jadhav, Prof. S. P. Aundhakar, "Secure E - Voting System Based on Paillier Cryptography", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 2, pp. 460-465, March-April 2020.

Journal URL : <http://ijsrcseit.com/CSEIT2062144>