© 2019 IJSRSET | Volume 6 | Issue 6 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology
DOI : 10.32628/IJSRSET196643

Homomorphic Encryption Based Online Voting System

Bharati Raut, Manasi Jagtap, Sneha Ghule, Kshitija Jadhav, Prof. S. P. Aundhakar
Department of Computer Engineering, PVPIT, Pune, Maharashtra, India

ABSTRACT

Propelled security procedures are essential to present convincing online based casting a ballot (e-casting a ballot) in the entire world. Choices coordinated on paper devour lot of advantages and add to the devastation of backwoods, which prompts atmosphere weakening. Later web-based casting a ballot encounters in nations such as the United States, India and Brazil showed that further explore is expected to improve security ensures for future races, to ensure the characterization of votes and enable the affirmation of their reliability and legitimacy. In our work, homomorphic encryption-based e-voting for casting a vote is proposed, which addresses these challenges. It discards every single limitation on the possible assignments of centers to different competitors as per the voters' individual inclinations. In order to assure the security of the votes, each cast vote is encrypt utilizing the paillier cryptosystem before accommodation. 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 used to confirm 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. The security and execution assessments joined show that our system has accomplished critical enhancements in examination with the past frameworks.

Keywords : E-Casting A Ballot, Ballot Framework, Paillier Cryptosystem, Homomorphic Encryption.

I. INTRODUCTION

In the previous two decades, different sorts of electronic voting frameworks have impressive consideration. Electronic voting resolve to make the election process simple and generally productive for political parties, candidates, election administration, and for voters [19]. Likewise, there are various issues in the electronic voting framework, such as system errors, network security, data security, etc. For developing nations like Egypt, many voting schemes are evolving 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 major role because data may get accessible for intruders. One of the main problems is cheating committed by outsiders or even the administrator himself in manipulating the data that will utilized or stored. We cannot simply put confidential voting data on online server. To resolve this issues encryption of data is to be done before sending it to server. For encryption of data various algorithms can be utilized amid which Elgamel, Okamoto-uchiyama & Paillier are now-a-days most likely to be used [1]. Paillier algorithm is asymmetric cryptographic algorithm. In asymmetric cryptosystem to encrypt data, public key is used and private key is used to decrypt the data. The public key is shared between number of parties that is sender and receiver for performing encryption and decryption. The algorithm displays additive

homomorphic properties. Homomorphic encryption grants computation over encrypted data for generating encrypted result. The decrypted result and the result of operations matches as if they had performed on plaintext. This property utilized to hide the vital voting data form counting system. Here we propose an approach for secure authentication of users for e-voting which can be done from anywhere around the globe. We utilize homomorphic encryption for security purpose. With implementation of the Paillier algorithm, analysing the time taken by an algorithm and compare the performance of proposed system with existing systems. Also going to check the similarities and differences of existing systems with our system. In the proposed system, we will make sure that there will not be violation of user credentials at the authentication stage, we also make sure the vote given by voter will not be tampered as their values are encrypted and as we use algorithm with homomorphic property it will not be revealed at transferring on server. Also during voting, the system ensures that proofs are generated and stored for each element in the cast ballot. These proofs are then utilized 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 organization of this document is as follows. In Section 2 (Literature Survey), we enlisted details of all research existed. In Section 3 (System Architecture), present architecture of proposed system. In section 4 (Result and Discussion) discussed experimental setup and database / dataset used is discussed. In section 5 (Conclusion) discussed conclusion and future work required to improve our system.

II. LITERATURE SURVEY

Nature of casting a ballot framework [2] is something imperative to examination the on the premise of extremely huge elections. This technique comprises with one downside, for example, mixnet addresses ballots incorporating with a duplicate credential. It is conceivable by expanding electronic watermarking reducing the measure of tasks in 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 purposes if author use watermarking and mitigates difficulty of computing.

Prof. S.M. Jambhulkar et al. proposed web based internet voting system [4], in that author justifies the protection to vote. For the most part security is required 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.

A new e-voting system is proposed [14] to accomplish protection by e-voting. Provided security is relying on homomorphic property and blind signature method. Installed framework is used 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.

In this paper [6], safe sensor network to observe interaction performance by AES encryption algorithm on the basis of plaintext size as well as value of operation per hop related to the network scale.

E-voting [7] system is altered time-to-time related with progress of the regulative environment with arising many questions. This paper is presented to make analysis of implemented existing vote authentication methods and their weaknesses and

analysis is used to propose a new trustworthy and robust vote authentication method.

Chun-Ta Li et al. introduced [9] 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.

Election and voting [11] is recently proposed to execute electronically. Web services plays important role due to its 5 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 is based on web services. The proposed system is developed on the basis of stochastic Petri nets (SPNs) and reliability and security are calculated.

Kausal Malladi, Srivatsan Sridharan et al. [13] proposes a robust e-voting system using 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 ensures voting privacy of a voter.

Drew Springall, Travis Finkenauer, Zakir Durumeric et al. [16] analyze the security of the Estonian I-voting system based 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.

III. 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.

A. 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].

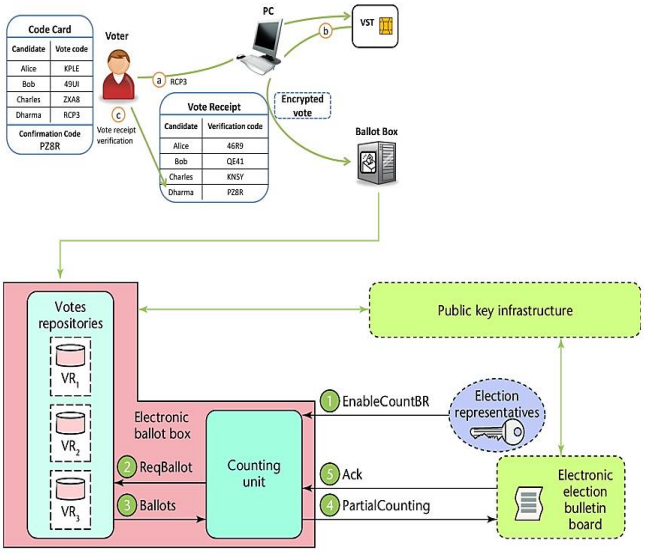

Figure 1 : System Architecture

B. Paillier Algorithm

Key Generation:

- Select two large prime numbers a and b arbitrary and independent of each other such that gcd(n, Φ (n)) = 1, where Φ (n) is Euler Function and n=pq.
- Calculate RSA modulus n = pq and Carmichael's function is given by λ = lcm (p-1, q-1).
- Select g called generator where $g \in \mathbb{Z}^*_{n2}$ Select α and β randomly from a set $\mathbb{Z}_n^*$ then calculate g = $(\alpha n + 1)\, \beta^n \bmod n^2$.
- Compute the following modular multiplicative inverse $\mu = (L\ (g^\lambda \bmod n^2)^{-1} \bmod n$. 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 (λ and μ).

Encryption:

- Let mess be a message to be encrypted where mess ∈ $\mathbb{Z}_n$.
- Select random r where r ∈ $\mathbb{Z}^*_{n2}$.
- The cipher text can be calculated as:

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

Decryption:

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

V. CONCLUSION

New secure e-voting system for instant runoff voting is presented. Homomorphic encryption and blind signature are used. Homomorphic encryption provides 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 our 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 address this issue and potentially could consider further generalizations.

VI. REFERENCES

[1]. 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

[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]. 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.

[4]. 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.

[5]. 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.

[6]. Hyubgun Lee, Kyounghwa 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

[7]. AI-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

[8]. 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.

[9]. Chun-Ta Li, Dept. of Inf. Manage., Tianan 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.

[10]. X. Yi, R. Paulet, and E. Bertino, Homomorphic Encryption and Applications. New York: Springer, 2014.

[11]. 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.

[12]. 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.

[13]. 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 (ICAECC)

[14]. 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.

[15]. R. Jubiya, M. Keirthi, M. Anupriya, A. Muthukumar, "IRIS Authentication Based On AES Algorithm", Volume 3, Special Issue 3, March 2014

[16]. 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.

[17]. Ngo Cuong. 2014. Secure Voting System Using Paillier Homomorphic Encryption. Faculty of the Department of Computing Sciences Texas A&M University – Corpus Christi, Texas.

[18]. Shifa Manaruliesya Anggriane,Surya Michrandi Nasution, Fairuz AzmiR. 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.

[19]. 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, "Homomorphic Encryption Based Online Voting System", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 6 Issue 6, pp. 159-163, November-December 2019. Journal URL : http://ijsrset.com/IJSRSET196643