iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4216

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

Homomorphic Encryption using E-Voting System

Kadlag Karan[1], Shinde Siddharth[2], Gondkar Ajit[3], Mr. Dange P. A[4]
[1, 2, 3]*Student,* [4]*Assistant Professor, Department of Computer Engineering, SSIERAS RAHATA. Rahata, India*

Abstract: ***A manual voting system can be time consuming and cumbersome and takes a lot of time. With the rapid development of Information Technology an E voting system tends to overcome all these limitations. The E-Voting system guarantees eligibility, privacy, verifiability and also receipt-freelances, no vote selling and uncoercibility. Online voting would be more convenient, relatively secure and utilize fewer resources over the traditional voting system. E-Voting System using Paillier Homomorphic Encryption Scheme which is used to provide security to the voting system and in turn help us to manipulate and transfer data in encrypted form making it impenetrable while preserving its security characteristics.This could actually be a solution for the low voter turnout at the polls which occurs due to the reluctance of voters to show up at the polls as The online voting is more reliable than the traditional system***
Keywords: Homomorphic encryption, Paillier , Cryptography .

I. INTRODUCTION

E -voting uses a range of Internet services, from transmission of data to full function online voting through connectable canals. With rapid development in the IT department an E voting system can overcome all these limitations. E voting is a fast technique and allows the voter to cast the vote from any location.

One of the main issues with this system is security. Electronic voting is an online process systems are the future of election. Each voter can cast their vote for their preferred candidates remotely through the internet. E-voting can be both advantageous and non advantageous in nature.

E-voting systems help us to reach to the remote locations can be hacked if it does not have any algorithm or protocol to protect it from the attacker. Attackers can attack on the packets of voters which are moving on the internet. Attackers can also Attack interrupt votes which are sent by voters over the internet.

A. E-Voting System Requirements

1) *Authentication:* Authorized voters should be able to vote.
2) *Unique Vote:* Voter capable only one vote.
3) *Accurate Result:* E-voting system should be able to calculate the appropriate result without human intervention.
4) *Verifiability:* Voter should be able to verify the votes anywhere during the process of voting and after the voting has completed.

Multiple countries refers to the use of computers or computerize voting equipment to cast votes in election . E-voting is an interdisciplinary subject and should studied from different domains, such as software engineering, cryptography, network security, politics, low, economics and social science. Mostly e-voting is known as a challenging topic in cryptography, because the need to achieved privacy, anonymity and vote encryption. Many e-voting systems proposed among the last decade, a lot of them based of complicated encryption schemes and other based on mix net model, blind signature model and homomorphic encryption model . Homomorphic Cryptography raised as a new solution used in electronic voting systems.

B. Cryptography

Cryptographic solutions provide methods of storing and transferring data in a secure way. Cryptographic techniques can separate into two general forms. Symmetric Encryption: In symmetric encryption there is a common key defined between sender and receiver, the same key is used for encryption purpose (,) and decryption purpose (,) process, where is the message and is the generated cipher text after encryption. cryptosystem is asymmetric algorithm for public key cryptography. Asymmetric

1) *Encryption:* In asymmetric encryption, private and public keys are generated, user can share his public key, any sender can encryption that allows computations to be carried out on cipher tex theory and modular operations, this provides a powerful property called homomorphism, and thus preserves group operations performed on cipher texts, add, multiply or both can made on two cipher text to calculate the result, which will be the same result if this operation performed on plain-text.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

C. Homomorphic Encryption

Homomorphic encryption is a form of encryption that allows computations to be carried out on cipher-text, thus generating an encrypted result which, when decrypt, matches the result of operations performed on the plain text. Homomorphic encryption is used in many modern day communication architectures. It is also used in the cloud computing environment for securing the processed data and for designing other secure homomorphic systems like secure voting system and secure information retrieval schemes. This also helps to make distributed computing secure.

whereas other systems are probably secure, but they are impractical. As a result, we have the need for a new easy to use, practical, secure and transparent online voting scheme. The Objectives of the proposed project are providing all the required services for conducting an election. Providing support to all the actors present (Organizer, Candidate, Voters).Easy and user friendly interface design. Offering the necessary functionalists for registration of eligible people to cast their votes and providing unique identification. Automated vote tally .

There are 2 types of homomorphic schemes: Partial and Fully Homomorphic schemes.

1) Partial Homomorphic schemes are those which only allow some computation to be carried out on cipher text like addition, multiplication etc.

2) Fully Homomorphic Schemes are the one in which most operations can be carried out on cipher text. First Fully Homomorphic encryption schemes was developed by Craig Gentry using lattice based cryptography.

II. LITERATURE SURVEY

Caroline Fontaine and Fabian Gland , A Survey of Homomorphic Encryption for No specialists , EURAISP Journal of Information Security

Axel, 2009 looks at the legal framework to remote electronic voting in Germany. They propose the use of a Voting Service Provider (VSP) to run and oversee the e-voting process. The VSP is supposed to be accredited to be able to offer the election services so that it operates within the law and can be held accountable and responsible of the entire process[9].

In Switzerland (Ursa Gasser and Gerlach, 2011) describes the country e-voting experiences outlining some of the benefits and challenges experienced[8].

Himanshu Agarwal and G.N.Pandey proposed aadhaar id based online voting system for Indian election is proposed for the first time in this paper. The proposed model has a greater security in the sense that voter high security password is confirmed before the vote is accepted in the main database of Election Commission of India. The additional feature of the model is that the voter can confirm if his/her vote has gone to correct candidate/party. In this model a person can also vote from outside of his/her allotted constituency or from his/her preferred location. In the proposed system the tallying of the votes will be done automatically, thus saving a huge time and enabling Election Commissioner of India to announce the result within a very short period.

This system is 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. This AADHAAR Identity number is unique for every citizen or voter of India. This AADHAAR Identity number has been introduced by government of India and this also recognized the constituency of the voter. But the registration of the voter should be completed only after the verification of all documents by the field officer. The field officer also verifies AADHAAR Identity Number from the main AADHAAR card database. After completing verification, the registration of the voter should be complete and the voter will get auto generated email which has all these information of the voter with the system generated password. The Voter can use this password for login and he/she can also change the system generated old password. Voter can also set the verification keys to ensure security. There should be restriction to use only virtual/on screen keyboard to type password or to change password. Main purpose of using virtual/on screen keyboard is to stop capturing password ,if voter changes his/her password from some public place.

III. PAILLIER CRYPTOSYSTEM

For the voting application one of the two possible additive homomorphic encryption algorithms are usually employed:

Paillier encryption or modified ElGamal encryption. Paillier encryption is inherently additive homomorphic and more frequently applied. The original ElGamal encryption scheme can be simply modified to be additive homomorphic: a message is used as an exponent in an exponentiation computation, and then the exponentiation is encrypted using the original ElGamal encryption.

A. *Related Work*

Homomorphic encryption has been used in online voting systems, for example the homomorphic property makes it possible to tally all encrypted ballots without decrypting them and accessing the content of any individual ballot. Helios is the first web-based voting system. It used ElGamal encryption to achieve open-audit voting. Helios did do not claim any cryptographic novelty apart from that fact that, assuming that there were enough auditors, even if all the authorities fully colluded to corrupt the system, they would be unable to counterfeit the election result without a high chance of being caught. Modification is that search for a logarithm must be performed in the decryption function, which becomes inefficient when the searching space is big. As the number of the voters is often large in voting applications, Paillier cryptosystem is usually preferred.

IV. METHOD

A. *Performance of The Voter Side*

On the client-side, each voter should cast a ballot and submit it to the server. In order to prevent the voting preferences of each ballot being revealed after submission, we require each voter to encrypt their cast ballots, where every element in the ballot must be encrypted. In this case, we set $P = 2n_c$, so that the total available points P is equal to twice the number of candidates n_c. For example, if there are 10 candidates ($n_c = 10$) in the election, each voter has 20 available points ($P = 2n_c = 20$) for their cast ballot. Since all elements in the cast ballot have to be encrypted, the larger the number of candidates participating, the more encryption processing time is required and the larger the submission grows.= (L(g^λ mod n*n)). total computation time and total submission size. Total computation time. We use the well-known Digital Signature Algorithm (DSA) to sign each ballot before submission. The processing time of signing is approximately equal to the time of one exponentiation.

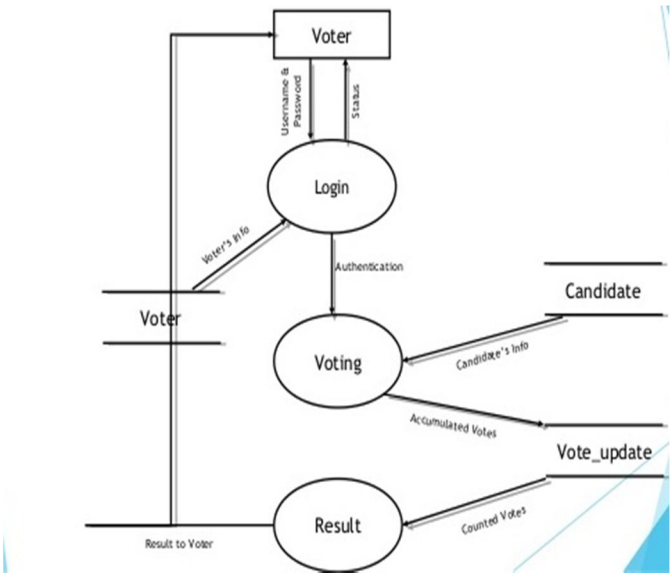
B. *Performance of The Server Side*

The performance of the server can be summarized from two aspects: verification of senders and verification of ballots. The verification of each sender is equivalent to verifying the digital signature of each submission, which does not cost much computation time. Therefore, we concentrate on the performance of ballot verification, which has two parts: the time of verifying each element of each ballot and time of verifying the total assigned points of each ballot. The total computation time on the server side. End-to-End Voter Verifiable: Every voter is able to verify whether their vote is posted and counted correctly. In order to make the system End-to-End (E2E) voter verifiable, we require each voter to generate proofs for each encrypted element of the ballot. These proofs are sent along together with the encrypted ballots. After submission, every-thing is made available publicly to all users.

V. PROPOSED MODEL

In our proposed model, we have implemented a small scale voting system through local host.We have tried to develop a website through which a voter can login securely and cast his/ her vote anonymously. Later after the voting period is finished, the administrator can login and decrypt the votes to display the final results.

The overall DFD of the system is as follows



The basic idea behind encrypting each vote is as

The above value is the plain-text which has to be encrypted as a single vote using the paillier encryption scheme.Each such cipher text is updated in the database to the variable Encrypted Sum(es).When a new cipher text(ct) is generated, this vote is updated in the database as:

es □□□es*ct□□□n^□□

After the voting phase ends, The administrator has to fetch the updated encrypted sum and perform decryption as per paillier's algorithm to get the result as follows:

The Decryption in our prototype occurs internally and is not visible to the administrator.The administrator only gets the final tally of votes per candidate.

In the proposed system the user just has to enter his/her aadhaar card number, mobile number and scan the bar code present on the Aadhaar card. It is much secure as compared to other system as it does the verification through bar code scanning and through confirmation message. As this system can be used for both government elections as well as for local election it makes the system more usable as compared to other which are just for government election.

A. Voting Step Diagram

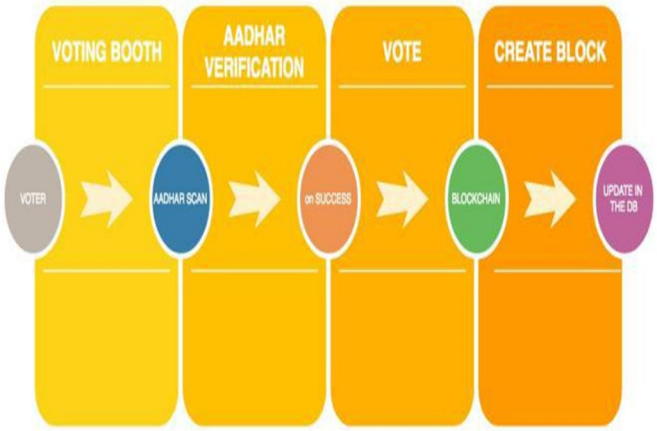
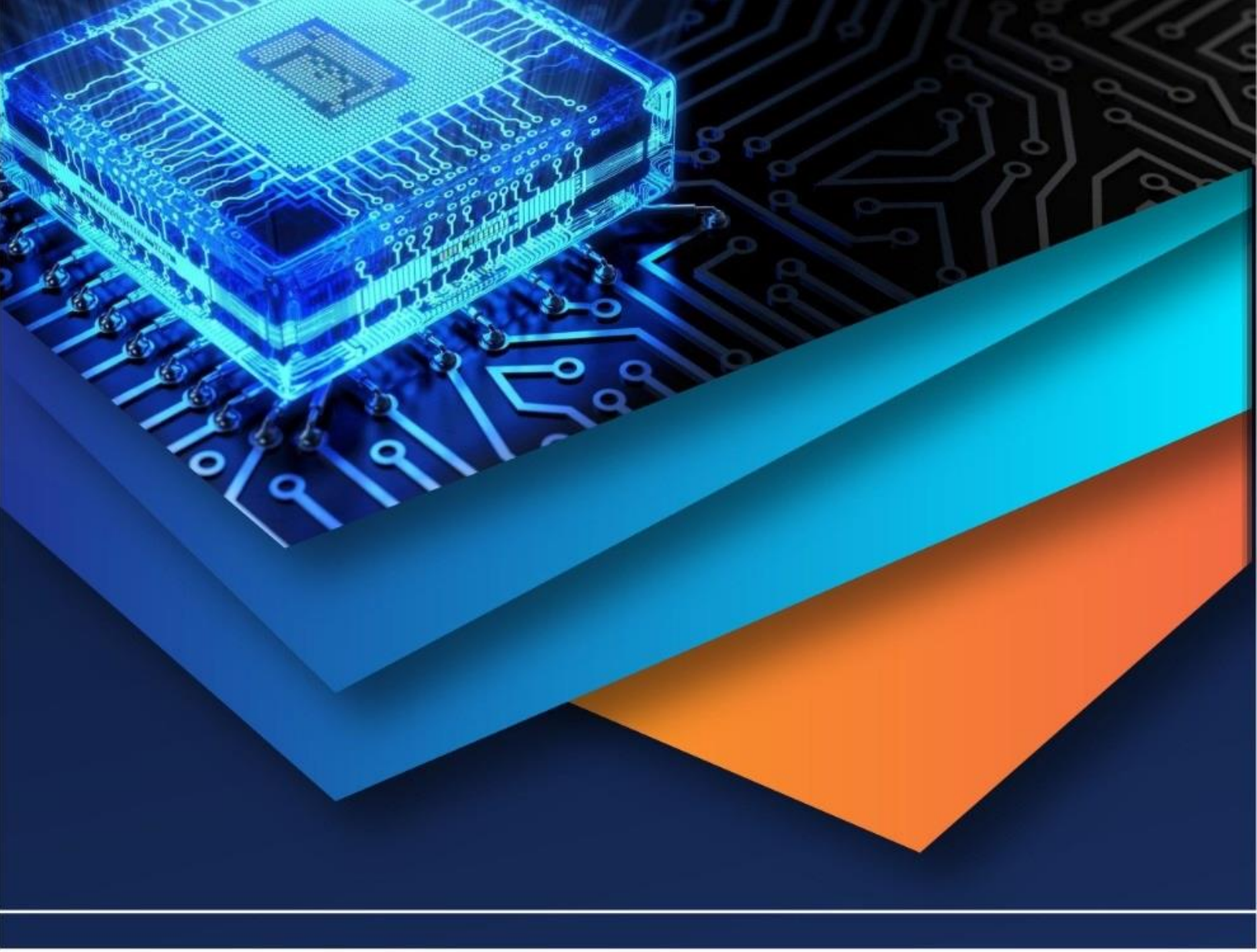


Fig: voting Step

REFERENCES

[1] A. Ara, M. Al-Rodhaan, Y. Tian, and A. Al-Dhelaan, "A secure privacy-preserving data aggregation scheme based on bilinear elgamal cryptosysytem for remote health monitoring systems," IEEE Access, vol. 5, pp. 12 601–12 617, 2017.
[2] 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.
[3] 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.
[4] X. Yi, R. Paulet, and E. Bertino, Homomorphic Encryption and Applications. New York: Sprinter, 2014.
[5] C. Expositor, A. Castigate, B. Martini, and K.-K. R. Choo, "Cloud manufacturing: Security, privacy, and forensic concerns," IEEE Cloud Computing, vol. 3, pp. 16–22, 2016.
[6] O. Has an, L. Brunei, and E. Bertino, "Preserving privacy of feedback providers in decentralized reputation systems," Computers & Security, vol. 31, pp. 816–826, 2012
[7] A. Mehmood, I. Natgunanathan, Y. Xiang, G. Hun, and S. Guo, "Protection of big data privacy," IEEE Access, vol. 4, pp. 1821–1834, 2016.R. Mendez and J. P. Vilela, "Privacy-preserving data mining: Methods, metrics, and applications," IEEE Access, vol. 5, pp. 10 562–10 582, 2017
[8] Schneier , B(1996). Applied Cryptography: protocols , algorithms and source code in C/Brut Schneir , New York , c1996



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY