Users Privacy-Preserving Using Homomorphic Encryption

Dafda Hiral Tulsibhai
Computer Engineering, Silver Oak College of Engineering and Technology-Ahmedabad, Gujarat Technological University, Gujarat, India.

Abstract **- Due to advancement of the technology in the storage of the data, field of data security becomes most crucial need of the users. As we know that encryption process provides the confidentiality as well as integrity of the data this process becomes necessary for the data storage facilities. In the e-voting system where data of the voter is very sensitive, we need to utilize this technology in the smart way. The main aim of this research is to provide security of this data with the help of the Pailler algorithm as well as to use homomorphic property in this system. With the help of the Homo-morphic property we are able to calculate the sum of the votes given by every voter and able to convert it into the encrypted form. The output value of the ciphertext which is diverse in the nature even if we encrypt same plaintext and it is much larger in the size as compared to the original plaintext.**

Electronic voting provides various kinds of properties like it ensures the privacy of the user by using confidentiality and verifiability by using the authentication mechanism. By using these properties intruders are unable to retrieve the vote of the voter from the system or from the communication channel. Authentication ensures the verifiability of the voter and identifies that voter is legitimate or not. Due to these kinds of strong properties of the algorithm e-voting system provides a numerous advantage like freeness of the receipts as well as resistance among the coercion and also autonomy of the ballot. By developing the secure protocols for the voting, we are able to achieve the properties needed for the secure communication. There are several methods was developed in the past years to ensure the confidentiality as well as authentication of the data and it can be categorized in different way based on how it achieves these properties.

However, this system or approach relies on the classical approaches of the security and based on some assumptions about the algorithm. If there is a quantum computer is efficient than it would be decrypt and compromise the data. So, we have to develop more reliable system among this threat and this work is the little stem among achieving this task.

Index Terms **- Electronic Voting, Homomorphic encryption, Additive Property, Paillier Encryption, Cryptosystem.**

I.INTRODUCTION

I studied various research papers and list out some major problems associated with the system which I try to solve in the proposed system and these problems are given below.

The total score is needed to develop the voting system. To achieve this task additive property of the algorithm is helpful but we have to find the way to secure this property using better algorithm which cannot be decodable easily [1].

Secure sum of the overall score is needed to preserve the privacy as well as trust of the system and there is a need of the encryption algorithm to achieve this task. For this purpose, we have to set up a trusted third party. [2]

Random number generation is needed to implement the trusted system and to provide the proof of zero-knowledge for the calculation of the feedback [3].

Authenticated trusted network has to be developed to achieve the confidentiality as well as we have to reduce the space needed for the computation without reducing the external dependable hardware. [4]

II. WORKFLOW

A. Key Generation: By using asymmetric key cryptography we have to generate the public and the private key to encode the data of the voter.

B. Selection of the Agent: Agent plays a vital role in securing the data of the users. For that purpose, we have to develop a trust matrix as well as have to feed trusted data. We have to select k numbers of agent as a representative of the data as well have to preserve their privacy. [5]

C. Formulation of the Feedback Share: For the formulation purpose we have to mark "k" numbers of the feedback which are offered by the agents and have to calculate overall feedback and it is represented as a "K". Agent again makes "k+1" feedback for the hidden response which generates a random key, and it is defined as a "M" which is known publicly

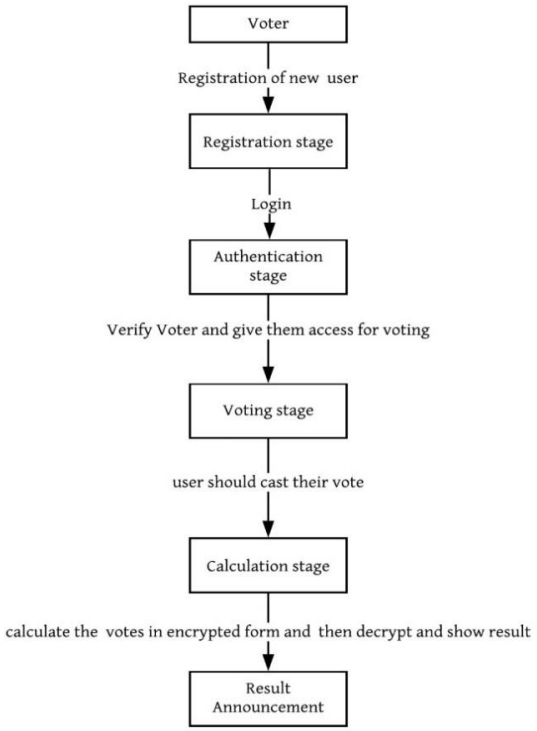

Figure 1: System Flowchart

- Encrypt the Feedback Share: We have to calculates the gradient for the all-available shares and it is comprehended by the public key of the representative. Also, we have to encrypt the kth share by using this public key so only representative can access these shares via their private key.
- Random Number Generation: In this phase random number is generated for the all the shares and we have to add "k" numbers of random number with the "k" numbers of the shares.
- Dispatchment of the Encrypted Shares. In this phase feedback provider have to provide the feedback for the entity for the source agent. Here total numbers of feedback are relied on the single agent which is trustworthy.

Summation of all Segments: When system receives the values of the feedback from the feedback provider using homomorphic property it adds all the values of the shares provided by the feedback provider. At the receiver side it decrypts the cipher text and get actual value of the feedback which is in terms of "k+1". Zero-knowledge proof is used for achieving this task.

III. MATHEMATICAL COMPUTATION FOR PROPOSED ALGORITHM

<table>
<tr><td colspan="2">The pre-processing
P= 11
Q=3
N=pxq= 11x3=33
g(p) here is primitive root of p Gf (11) = (2,6,7,8)
g= 7
Y= g^q mod p= 2</td></tr>
<tr><td>Voter1
RANDOM NUMBER = 5
K=7
E(RATING) = (RATING + r x p) mod N
= (2+5x11) mod 33</td><td>Voter2
RANDOM NUMBER =5
K=11
E(RATING) = (RATING + r x p) mod N
= (3+5x11) mod 33</td></tr>
<tr><td colspan="2">E(M) = (a, b)
E(M)= (a, b)
= ($g^{\text{random number}}$ mod p, y^k Encr rating mod p)
= ($g^{\text{random number}}$ mod p, y^k Encr rating mod p)
=(7^7mod11,2^7x24mod11)
= (7^{11}mod11,2^{11}x25mod11)
= (6,3)
= (7,6)</td></tr>
<tr><td colspan="2">(6, 3) ⊕ (7, 6)
= (110,011) ⊕ (111,110)
= (001,101) = (1,5)</td></tr>
<tr><td colspan="2">a=1
b=5
Message= b(a) mod p
=5/1 mod 11= 5
5 is decoded i.e., 2+3 = 5</td></tr>
</table>

IV. IMPLEMATATION

A. INTRODUCTION

To encrypt the data of the client and to convert it into the ciphertext form we have to apply the homomorphic encryption. Homomorphic encryption provides security of the client's data in all the phases like

extraction, transmission and in the preparing of the data. Let's take an example to understand this process. For example, if you have a plaintext data like 12 and 24 which are stored in the form of ciphertext like 8585 and 6554 respectively and the addition of the original plaintext which is 12+24= 36 is also stored in the encrypted form let's say as 5445. Now if we go through the traditional way in which system have to decrypt all the plain text then it becomes time consuming process as well as it takes large computational space for the system. On the other hand, homomorphic encryption process provides a way to decrypt the data in such a manner that system has to decrypt only homomorphic sum of the data which take small amount of computational time as well as less storage space. The flow of the system is given below which includes all the necessary steps needed for developing the system.

B. METHODOLOGY

In this section I described the methodologies implemented in my research where collection of votes from the different voters is encrypted and system generates the encrypted outcome. By using encryption process system is able to maintain the confidentiality of the voters. Integrity is achieved using signing as well as verification algorithms. Voters are able to create their account by using third party verification. I listed some stages used in the voting system which are given below.

- Registration Phase: In this phase new voters are able to register itself by authenticating their self via election authority. The eligibility of the voter is verified by using the signing process provided by the system by collecting necessary details of the voter. All the details are verified using the trusted third-party mechanism. After the registration process users are able to cast their votes.
- Authentication Phase: To provide authentication voters have to login in the system using their unique id and password and these parameters are verified by the system. Authentication mechanism uses various algorithms to verify the user and allows to login into the system if the parameters provided by the voters are legitimate.
- Voting Phase: By using this mechanism voters are able to cast their votes to the appropriate candidates. Then after votes are encrypted using the Pailler encryption mechanism and encrypted votes are stored in the database. After storing the data is feed to the Tally stage for the further process.
- Calculation Phase: Using additive property of the homomorphic encryption votes are added to get the total numbers of the votes received by the particular party.
- Homomorphic Encryption: In this system I used homomorphic encryption to encrypt the data. It uses homomorphic property which allows to perform computation on the encrypted data without decrypting it which ultimately reduce the time and space complexity of an algorithm as well as it provides confidentiality from the external users.
- We can describe the homomorphic encryption as: f(E(x1), E(x2) .... E(xn)) = E (f (x1, x2. xn))
- Here E denotes the encryption process, F denotes the operation perform on data while X denotes the plaintext to be encrypted.
- Pailler Cryptosystem: Pailler provides an encryption as well as decryption process on a data in an efficient manner. It takes multiple bits in a single operation as well as uses a constant factor of the expansion to perform efficient decryption. Pailler system is again divided into four phases which are: key generation, encryption process, decryption process and the homomorphic operations on the data.
- Key generation: Two large prime numbers are selected which are mutually exclusive in nature and key is calculated as $x=L(c\lambda \bmod n2) \cdot \mu \bmod n$ where L is a key generation algorithm.
- Homomorphic addition on plaintext: By using this property multiplication of the two different ciphertext gives the addition of their corresponding plaintext when we decrypt the ciphertext and this process is given by

$D(E(x1, r1) \cdot E(x2, r2) \bmod n2) = x1 + x2 \bmod n$

C. PROPOSED SYSTEM

The proposed online voting systems designed to provide high security with minimum cost with paperless work in the process of voting. Paillier's encryption technique is used to encrypt the casted votes before storing it in the webserver. The most

valuable feature of Homomorphic encryption discussed earlier performs the operations on stored data to find out final result of voting without even decrypting those data.
This way we can prevent a user from knowing whatever information being stored on the web server providing very high security as well as minimizing the cost by designing a user-friendly web interface for casting votes.

The Proposed Model Flow:
Voter Registration and validation phase: The voter registers themselves for voting purpose and administrator verifies the voter and gives access permission for voting. Then, sharing pass code and public key phase: With help of a key generation algorithm public and private keys are generated.and Whenever voter goes for voting, the whole process goes through various phases of homomorphic encryption process. Administrator finally checks the total votes against each of the candidates and declare the results. It is a client server-based voting system which has one administrator who can control the whole system. Administrator is the one who has the privilege to add the candidates, to whom one can vote, generate password for user and calculate the result. A user/voter needs to register before voting. Administrator verifies his/her authenticity then only provides a password through choosing a secure channel. After getting the password the voter now can login to the actual voting system and can vote for any candidate of his/her choise.

D. RESULT
The casted votes are stored in the encrypted form using pailler algorithm. System applies rotational methods to shuffle the ballots and stores it into the database which increase the computation time and the space complexity. Proposed system allows the database to store votes in the encrypted format which saves time as well as space of the system as well as provides integrity of the data. Because data are stored in the encrypted from if admin or the intruder have access of the database, they are not able to distinguish the casted votes stored in the database. By using homomorphic property of the Pailler system final calculation of the vote is calculated. The proposed system is much more reliable and faster than the traditional cryptographic techniques. By using this system, we are able to preserve the confidentiality, integrity as well as authentication of the voters.
Result of the Voting Process after all computations is as follows:
Votes for Candidate #1 = 5
Votes for Candidate #2 = 3
Votes for Candidate #3 = 2
Votes for Candidate #4 = 2
Votes for Candidate #5 = 2
Now this algorithm can be strengthened using the paillier cryptosystem technique. All the casted votes could first be encrypted and stored on the database and then they could be added homomorphically to produce the encrypted result. The decryption and further computation of the result would then finally give the winner of the election process.

VII. CONCLUSION

By studying the current research work and finding the problems in the current research work we are able to improve the structure of the algorithm which is able to increase the accuracy as well as improve the security of the voting system. In this paper we proposed a secure voting scheme applicable to web platform using Paillier's Algorithm of Homomorphic Cryptosystem. We discuss the model with the prospective of computation over cipher text and computing the voting results with the help of their Homomorphism properties. It is observed that the propose model works efficiently in a web-based model for casting votes and a cloud-based web server for storing voted information in encrypted form.

REFERENCES

[1] M. S. Kristian Gjøsteen, "A Roadmap to Fully Homomorphic Elections: Stronger Security, Better Verifiability.," in International Conference on Financial Cryptography and Data Security, 2017.
[2] F. d. João Palas Nogueira, "Trust in e-Voting Systems: A Case Study.," in Mediterranean Conference on Information Systems., 2012.
[3] J. M. Jens-Matthias Bohli, "Bingo Voting: Secure and Coercion-Free Voting Using a Trusted Random Number Generator," in International Conference on E-Voting and Identity, 2007.

[4] Anon., "Authentication Mechanisms for E-Voting. In: Human-Centered System Design for Electronic Governance," Premier Reference Source, p. 16, 2013.

[5] M. R. M. Mina Ghavipour, "Trust propagation algorithm based on learning automata for inferring local trust in online social networks," Knowledge-Based Systems, vol. 143, pp. 307-316, 2018.