E-Voting using Homomorphic Encryption Scheme

Tannishk Sharma
Student
Department of information technology,
BVCOE Delhi

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. E voting is fast and helps us to cast our vote from any location. One of the main concern of then E-Voting System is security. In this paper we propose an 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. Here We use the Paillier Encryption Homomorphic property that allows us to add the votes in encrypted form. The online voting is more reliable than the traditional system and is able to save to save the time

Keywords
Homomorphic encryption, Paillier Algorithm, E-voting, Cryptography

1. INTRODUCTION
Electronic voting is an online process in which tasks to cast and count votes is done by using electronic means. E -voting uses a range of Internet services, from transmission of data to full function online voting through connectable canals. E-voting system may consist of optical fibers, computers. It can include transmission of data using optical fibers, coaxial cables and satellites. E-voting can be both advantageous and non advantageous in nature. E-voting systems help us to reach to the remote locations. People can vote from any place they want over the internet. People can open the website and cast their vote at any place and anytime they want. The disadvantages of E-voting is that they are vulnerable to hacking. If proper encryption scheme is not implemented, then hackers can catch and change the vote information easily.

E-Voting System Requirements [15]:

1. Authentication: Only authorized voters should be able to vote.
2. Unique vote: No voter should be able to cast their vote more then once.
3. Accurate Result: E-voting system should be able to calculate the appropriate result without human intervention.
4. Verifiability: It should be able to verify the votes anywhere during the process of voting and after the voting has completed.

Encryption is a way to encode messages or data with a key in such a way that only authorized parties can read it. Tradition Encryption techniques were able to protect the data only within transmission but data needs to be decrypted when some operation needs to be carried out on this data. If the computer on which our computation needs to be performed has been compromised, then this will lead to loss of data. To overcome this problem, concept of homomorphic encryption was proposed according to which operations can be performed on cipher text without knowledge of your key or password, thus generating an encrypting result which when decrypted produces the same result if the same set of operations were performed on plain text.

2. RELATED WORK
In [1] We study the various properties and limitations of different homomorphic schemes and how to select a scheme based on a particular use

In [2] We study the various properties, types of Homomorphic encryption and a somewhat homomorphic encryption scheme when applied to lattices.

In [3] We study the the various properties of the Paillier cryptosystem, how does the Paillier cryptosystem works and how it can be applied to solve the real world problems

In [4] We study the tallying part of the election process using Paillier Algorithm which gives us the ability to add data in encrypted form.

In [5] We study various encryption algorithms like RSA, ELGAMAL, Paillier Algorithm and how it can be used to implement an e-voting system

In [15] We study a voting protocol which should be observed to achieve universal verifiability and protects voter's privacy

2.1.Homomorphic encryption
Homomorphic encrypti**on** is a form of encryption that allows computations to be carried out on cipher text, thus generating an encrypted result which, when decrypted, 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.

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

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

2.2.Paillier cryptosystem
Paillier cryptosystem is asymmetric algorithm for public key cryptography. An important feature of the Paillier

cryptosystem is homomorphic property.

Let m be the plain text to be encrypted. Then select random number x where r,n belongs to Z then we get cipher text c = $g^m x^N \text{mod } N^2$.

2.3 Homomorphic Addition

The product of two cipher texts will decrypt to the sum of their corresponding plaintexts,

$$D(E(m_1, r_1) \cdot E(m_2, r_2) \text{mod} n^2) = m_1 + m_2 \text{mod} n.$$

$$D(E(m_1, r_1) \cdot g^{m_2} \text{mod} n^2) = m_1 + m_2 \text{mod} n.$$

The product of a cipher text with a plaintext raising g will decrypt to the sum of the corresponding plaintexts,

2.4 Homomorphic multiplication

A cipher text raised to the power of another plaintext will decrypt to the product of the two plaintexts

Paillier Cryptosystem can be used in various practical

$$D(E(m_2, r_2)^{m_1} \text{mod} n^2) = m_1 m_2 \text{mod} n.$$

$$D(E(m_1, r_1)^{m_2} \text{mod} n^2) = m_1 m_2 \text{mod} n,$$

applications like it can be used in cloud environment to implement secured electronic voting and electronic cashing and mail server etc.

2.5 Paillier Algorithm

Paillier is one of the most widely used cryptography scheme. It has wide range of applications like bank security systems, in the area related to cloud computing etc. We are going to use the above stated system for implementing an E Voting System.

Step 1:

Process of Key Generation takes place by using following steps:

1. Generate two large prime numbers a and b randomly which are independent of each other such that gcd(a*b,(a-1)*(b-1)) = 1 . GCD is the greatest common divisor of two or more integers which is the largest positive integer that divides the number without a remainder.
2. Compute n = ab and k(n)=lcm(p-1,q-1) where k(n) being Carmichael function .
3. Select a generator g such that g belongs to Z_{n2}
4. Calculate the follow Modular Multiplicative inverse $u = (L(g^k \text{mod } n^2))^{-1} \text{ mod } n$ where L(u) = (u-1)/u

So Pair of Key Generated: the public key is (n,g) and the private key is (k,u)

Step 2: Encryption Process

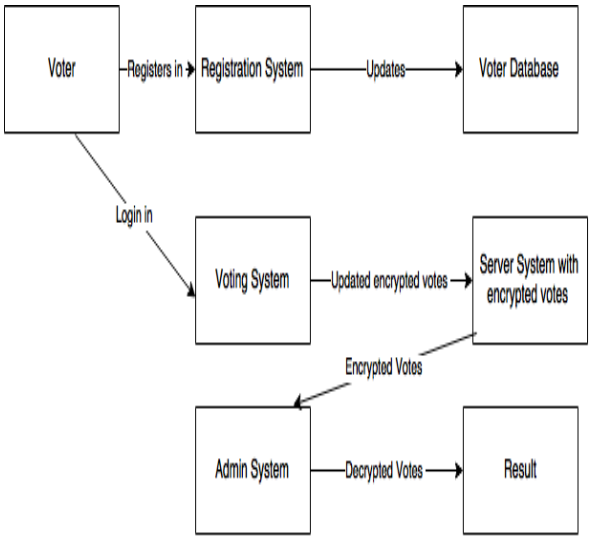
1. The message m is a message need to be encrypted where m belongs to Z
2. Choose a random number r
3. Compute cipher text $c = g^m * r^n \text{ mod } n^2$

Step 3: Decryption Process

1. Cipher text c will be decrypted to get message m as follows by using private key (k,u) :- $m = L(c^k \text{ mod } n^2) * k \text{ mod } n$

3. PROPOSED MODEL

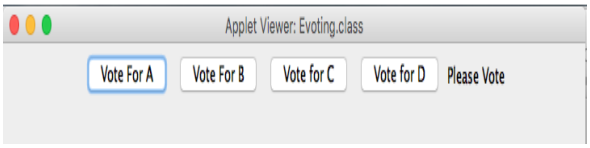
Basic E-Voting system should consists of three types of systems that is ,client system, server system and the registration system. Each system is connected to the common database. The registration system allows the user to register itself so that it can cast a vote. Client system allows it to cast a vote and server system is used to keep tract of the different votes casted. Client system consists of 2 types of systems: voter system and admin system. Voter System is the system where user casts his/her vote and Admin System is the system where we can verify the number of votes casted and display the final result



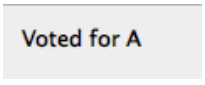
Initially Values of Different Candidates at the Server System is:

```
A:null
B:null
C:null
D:null
```

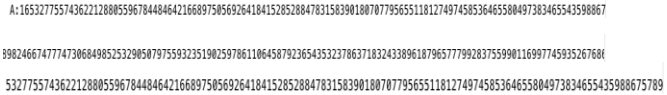
Voter registers at the registration system where he enters all his required details and is given a unique voter id. Using this unique voter id and password entered by him logins at the client side The following screen is displayed to ask the user for its candidate choice

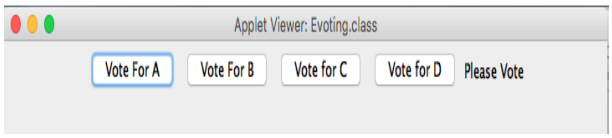


Let's suppose that a given user voted for Candidate A then at client system a message is displayed as shown:



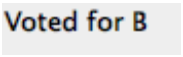
At Server System the number of votes are saved at the server in encrypted form. number of votes for candidate A is displayed as shown:



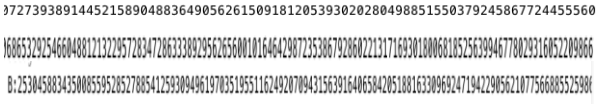


Now a new user login at the client system At the Client System following message is displayed:

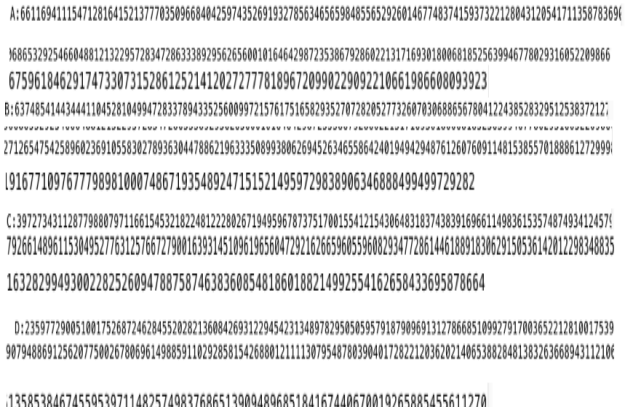
Suppose voter votes for B and following message is displayed: -



At Server System the Number of votes for Candidate B is saved at the server in encrypted form as shown: -



This process continues for 10 voters in which they vote for their candidates respectively. After 10 votes have been casted number of votes for different candidates are saved on the server system in the encrypted form as shown: -



When It is decrypted by the administrator at the admin system

```
A:1
B:5
C:3
D:1
```

we get: -

4. FUTURE WORK AND CONCLUSION

Many places have not fully implemented E-Voting system because of the associated security challenges and flaws. Our proposed scheme successfully implemented a secure E – Voting System based on Paillier Encryption. This process ensures that votes can be transferred securely over the internet and counted correctly. This scheme ensures eligibility, completeness, privacy, efficiency, universal verifiability, no vote duplication, non-coercion and receipt-freeness. The above E voting system implemented is simple and can be extended to run on different platforms such as web browsers and on Android / IOS Devices. Users should be able to download the plugin for their web browser or application for their hand held devices and cast their votes. This Project can be extended to help voters cast their vote over the internet. It is the cheapest, quickest and secure way to vote as compared to tradition voting scheme. One doesn't need to be present at the voting booth to cast their vote. One can vote from any location. All in all, it has met the requirements of an E-voting system.

5. REFERENCES

[1] Caroline Fontaine and Fabien Galand , A Survey of Homomorphic Encryption for No specialists , EURAISP Journal of Information Security

[2] Craig Gentry , A Fully Homomorphic Encryption Scheme

[3] Michael O'Keeffe , The Paillier Cryptosystem

[4] Sansar Choinyambuu , Homomorphic Tallying with Paillier Cryptosystem

[5] Coung Ngo , Secure Voting System Using Homomorphic Encryption

[6] E-Voting Simulator based on the Paillier Cryptosystem, Andreas Steffen, HSR Hochschule für Technik Rapperswil

[7] Schneier , B(1996). Applied Cryptography: protocols , algorithms and source code in C/Brue Schneir , New York , c1996

[8] Paillier Cryptosystem , Wikipedia

[9] Lecture Notes 15 : Voting, Homomorphic Encryption Ron Rivest

[10] Xun Yi., and Eiji Okamoto, "Practical Remote End-to-End Voting Scheme", EGOVIS 2011, LNCS 6866, pp. 386–400, 2011, Springer Verlag Berlin Heidelberg 2011

[11] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI, "Homomorphic Encryption Applied to the Cloud Computing Security " WCE 2012, July 4 - 6, 2012, London, U.K.

[12] N. P. Smart and F. Vercauteren. Fully homomorphic simd operations. IACR Cryptology ePrint Archive, 2011:133,2011.

[13] William Stalllings, Cryptography & Network Security, Fourth Edition, Pearson Education, 2006.

[14] Ryan, P. Y. A. (2007). The computer ate my vote. Retrieved from http://www.dagstuhl.de/Materials/Files/07/07091/07091.RyanPeter.Paper.pdf

[15] A. Acquisti, "Receipt-Free Homomorphic Elections and Write-in Voter Verified Ballots", Technical Report 2004/105, CMU-ISRI-04- 116 (2004).