Implementation of Homomorphic Encryption in Online Voting System using Paillier Algorithm

Subin Joseph
Department of Computer Applications
Amal Jyothi College of Engineering, Kanjirappally, India
Subinjoseph@mca.ajce.in

Sr. Mercy Joseph
Department. of Computer Applications
Amal Jyothi College of Engineering, Kanjirappally, India
elsinchakkalackal@amaljyothi.ac.in

***Abstract*— This paper is delivered to improve the online voting process by enhancing security using homomorphic encryption. Elections are confidential activities that have many chances for malpractice like tampering with the digital ballot by hacking etc. It makes our system weak and worthless. It can be overcome by encrypting the data by homomorphic encryption. We know that homomorphic encryption is dealing with numbers, that is we can perform operations on encrypted data without decrypting it. This extension will make our system more secure. That is no one is going to see the results or lead before publishing the result including the admin.**

Keywords: Paillier Cryptosystem, Encryption, PHE, AES

I.INTRODUCTION

Voting is the supreme right of the citizens of a democratic nation and provides the opportunity to elect representatives for a certain period. That is, elections are the soul of a democratic country. As we know, to vote, we have to go to the polling booth to cast our vote. This is very difficult for elderly people or people who study or work abroad to cast their vote. This situation requires an online system for voting. It is a big challenge to design an online voting system when we analyze the system from the view of security. As we know it is impossible to ensure 100% security for anything in the cyber world. But we can improve or enhance the security to an extent by providing frequent updates etc. Our implementation in the system by homomorphic encryption will make the system more secure as compared to the existing system.

The depicted Strategy (Homomorphic Encryption), allows the individual to work on cipher text. That is the result will not differ from the result which is generated with plaintext. Eg : consider two numbers 54 and 34 both are encrypted as 54=f203a0bec0018b8a9b4c5d54 and 34= f6135c6fb78eeacda7459745 respectively (hexadecimal) .The result 54+34=88 is also stored in an encrypted form like e570a55b1bcc7e0a. That is we can compute a large set of data by working with the cipher text by not exposing the values to anyone. It improves the confidentiality of the data. Paillier encryption technique is applied here (Partial Homomorphic encryption) Symmetric key cryptosystem.

The scheme is a cryptographic scheme that encrypts the message using a public key and decrypts it by the corresponding private key. The property of additive homomorphism performs addition operations on encrypted cipher text. That is the core concept of the implementation proposed in the system.

A. *Nature of Paillier Cryptosystem*

The nature is probabilistic. That is every time the ciphertext is encrypting again and again and a new encryption code is generated. It makes it difficult to realize whether both the ciphertext are generated for the same message or not. The proposed methodology is additive homomorphic encryption which is robust by the paillier algorithm. It allows us to operate on encrypted data and also provides confidentiality, integrity, and availability.

II.HOMOMORPHIC ENCRYPTION-PAILLIER ALGORITHM

The idea of homomorphic encryption is proposed by R. Rivest, M.Dertouzosand,Leo.Adleman after the development of the RSA. Consider an encryption function 'H' which encrypts a plaintext P and f () be an operation. That is homomorphic encryption is defined as

$$f(H(x1), H(x2) \ldots.H(xn)) =H(f(x1,x2\ldots.xn))$$

This phenomenon is called additive homomorphism That is + implies the binary addition operation Therefore, an additive homomorphism is described as

$$H(x2)+H(x1)=H(x2+x1)\ x$$

That is paillier algorithm depicts additive homomorphic property. It’s a well-known member of homomorphic cryptography, which is implemented by Pascal Paillier in 1999. It encrypts multiple bits in a single operation with a constant factor of expansion and also efficient decryption.

The cryptosystem is defined by four terms which are key generation, Encryption, Decryption, and operations.

○ *Key Generation*

Consider x and y are two big random prime numbers that are mutually exclusive, that is $\gcd (XY, (x-1)(y-1))=1$

This property is assured if both numbers are equal to each other in length. Calculate $n=xy$ and $\lambda=\mathrm{lcm}(x-1,y-1)$ Select f randomly as an integer where f belongs to $Z*N^2$. The existence of multiplicative inverse ensures that the order of f is divisible by n by the following equation $\mu=(L(g^\lambda \mathrm{mod} n^2))^{-1}$ where function $L(x)=x-1/n$. The public key (encryption) is (n,f). The private key (decryption) is(λ,μ).

If using x,y of the same length, a simpler version of the key generation steps could be to set $f=n+1$, $\lambda=\varphi(n)$, where $\varphi(n)= (x-1)(y-1)$

- *Encryption*

  Let a message is denoted by x which we won't want to encrypt where $0 \le x < n$. Consider r where r is randomly selected where, r ϵ *Z*^**n*2 and 0 < r < n gcd (n, r) =1)
  Calculate cipher text as follows
  c=g^x·r^n mod) n^2

- *Decryption*

  Let a cipher text is denoted by c which is encrypted by the public key which is needed to extract as a plaintext where c ϵ *Z*^**n*2. The exact message can be calculated as x=L (c^ λ, mod n^2)

- *Characteristics*

  A homomorphic algorithm is important due to its homomorphic nature and it can generate non-deterministic encryption. That is the algorithm is additive

- *Addition process in paillier algorithm*

  While performing an addition operation using the paillier algorithm there performs the multiplication of the ciphertext which gives the sum of the plain text when the result is decrypted

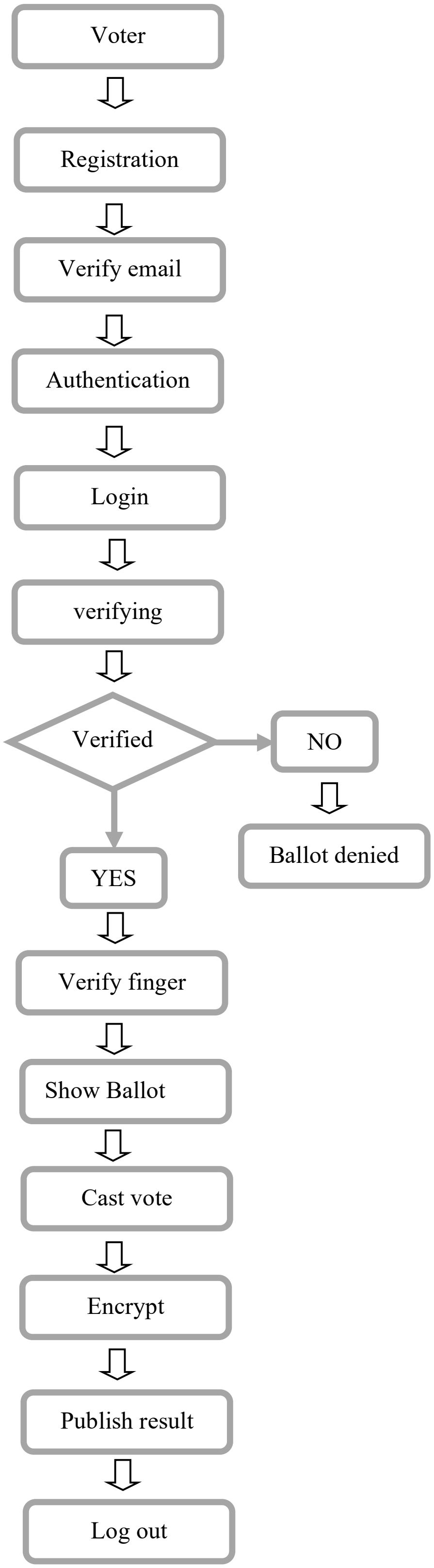
III.PROPOSED METHODOLOGY

The proposed system is an online voting system. The voter can cast their vote without visiting the polling booth. As we know security is a major concern while designing a solution for confidential problems like designing an online voting system. Data security of all the users is important which is achieved using the AES encryption technique in the existing system.

Homomorphic encryption in the proposed system using for counting votes and storing them in the database. That is the final count is taken from the database only while publishing the result. So there is not even a clue about who voted to whom and the vote count will also be encrypted.

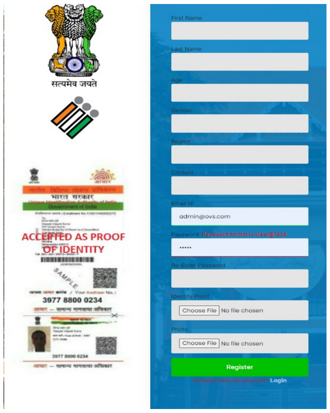
In this system, the integrity and anonymity of the users are hidden. Self-registration of users is allowed in the system and govt officials can verify the proof submitted by the users at the time of registration according to the genuineness of the proof the govt officials can accept or reject the registration. methodology

Email verification is also required at the time of registration. Users enter the dashboard after getting verified by themselves using email. The voter or candidate can participate in the election only after successful verification by the election authority. Data entered at the time of registration is also kept encrypted using Advanced Encryption Standard (AES). This ensures the data security of the voter and candidate and all other users. It also resists SQL injection and other forms of attacks on the database which steal sensitive information like password contacts etc. AES is a powerful standard that is widely used for encryption all around the world



- *Registration:*

Self-registration can be done by the voter. After successful registration admin can approve or reject the application. Email verification is also done during registration. Registration data is kept encrypted using Advanced Encryption Standard(AES).



First Name

Last Name

Age

Gender

Region

Contact

Email id: admin@ovs.com

Password **Password format is:User@1234**: •••••

Re-Enter Password

Identity Proof: Choose File No file chosen

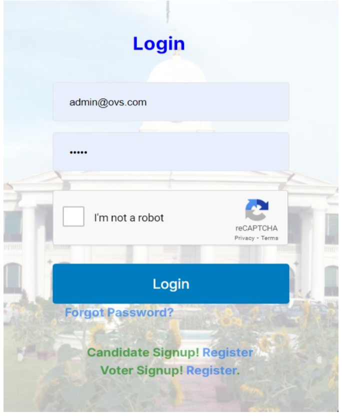
Photo: Choose File No file chosen

Register

Already have an account? Login

- *Login*

After a successful registration user can log in to their dashboard with credentials.



Login

admin@ovs.com

•••••

□ I'm not a robot

Login

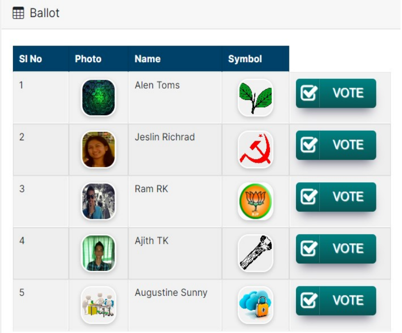
Forgot Password?

Candidate Signup! Register

Voter Signup! Register.

- *Verification*

It implies the verification that the corresponding voter is approved or not by the admin. If approved system initiates the finger verification session and shows the ballot.



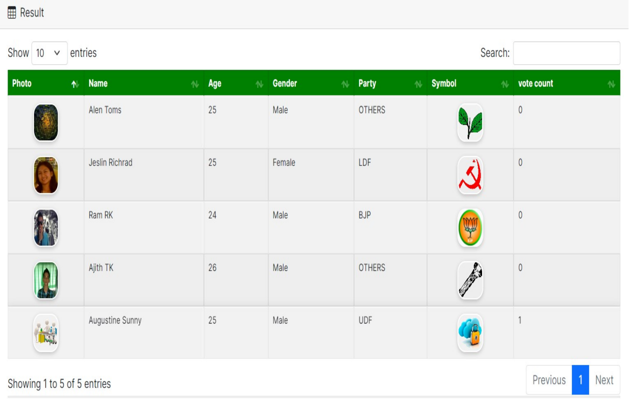
Ballot

Sl No	Photo	Name	Symbol	
1		Alen Toms		☑ VOTE
2		Jeslin Richrad		☑ VOTE
3		Ram RK		☑ VOTE
4		Ajith TK		☑ VOTE
5		Augustine Sunny		☑ VOTE

- *Publishing Result*

After the election the administrator can publish the result then all the users will be able to view the result and generate a PDF of the result.

In the proposed system the vote count is encrypted using Paillier Algorithm. That's why we are maintaining the integrity of data. Due to the partial homomorphic nature of the paillier algorithm vote data is more secure as compared to the existing system. Since we perform calculations of votes on encrypted data the votes remain a secret for all until the result is published. The person who has control over the database like an admin or an intruder can't distinguish the votes gained by each candidate.



Result

Show 10 entries   Search:

Photo	Name	Age	Gender	Party	Symbol	vote count
	Alen Toms	25	Male	OTHERS		0
	Jeslin Richrad	25	Female	LDF		0
	Ram RK	24	Male	BJP		0
	Ajith TK	26	Male	OTHERS		0
	Augustine Sunny	25	Male	UDF		1

Showing 1 to 5 of 5 entries   Previous 1 Next

IV.CONCLUSION

An online voting system is an excellent solution and it will enhance democracy and ensures maximum participation in the election process. It is a comfortable solution for voters who were working or studying abroad and voters who are not able to visit the polling station.

Security is a major concern since the system needs high security. There are many chances to alter the system by a hacker or an external agency to change results for someone's interest or steal the user's data. The proposed system protects users' data by using Advanced Encryption Standards (AES) and keeps securing votes using homomorphic encryption. Only the final count of votes is decrypted and all the calculation processes are done using encrypted vote counts. It is impossible to identify who voted for whom. That is, it provides anonymity for voters. The implemented model provides ensures data confidentiality and integrity of the data since it is a combination of two encryption techniques. It provides all the functionalities of the existing system plus encryption of vote counts and vote calculation using cipher texts. The main aim of the proposed implementation is to provide security to the existing model.

As we know we can't ensure 100% security for anything in the cyber world since intruders are everywhere. So, we can only maintain the security of the system by providing updates. The system must be kept updated with new security techniques.

I.References

[1] Mercy Joseph, Gobi Mohan,"Design a hybrid Optimization and Homomorphic Encryption for Securing Data in a Cloud Environment",International Journal of Computer Networks and Applications (IJCNA),9(4), PP: 385-398, 2022,DOI: 10.22247/ijcna/2022/214502.

[3]I. Damgard,M.Jurik,andJ.B.Nielsen, “A generalization of paillier’s public key system with applications to electronic voting,”International Journal of Information security,vol.9,no.6,pp.371–385 ,2010.

[2]Amal Joy, & Sr. Mercy Joseph. (2022). Secure Cloud Data Processing with Fully Homomorphic Encryption.Proceedings of National Conference on Emerging Computer Applications 2022(NCECA 2022), 196–199. https://doi.org/10.5281/zenodo.6365059

[4]P. Paillier, Public-Key Cryptosystems Based on Composite Degree Residuality Classes.Berlin, Heidelberg: Springer Berlin Heidelberg,1999, pp. 223–238.