Online Voting System using Homomorphic Encryption

Saksham Saproo[1,*], *Vedant* Warke[2,**], *Shreyas* Pote[3,***], and *Rashmi* Dhumal[4,****]

[1]Department of computer engineering,Ramrao Adik institute of Technology,Nerul

Abstract. An important part of a democratically fair society are elections. The conventional democratic framework becomes hard for the individuals who can't visit the polling stall for casting their votes. With quick advancement of data innovation, online Internet voting framework is all the more intriguing to use for the nations where vote casting cooperation is low and it is too helpful for people living far off from their homes. Security is a major worry for Internet voting system. The proposed framework guarantees security prerequisites for example, validation, precision, secrecy, receipt-freeness, unwavering quality, obviousness and reasonableness in the political race.

Keywords- Paillier algorithm; homomorphic encryption; E-voting

1 Introduction

Election are backbone of a democracy, so its important that it should be fair. The way to select your representative is by voting. In traditional voting system voters have to reach polling station and cast their vote, it gets difficult for elderly and for those living far from their homes or living in the remote locality. Voting through internet allows voters to give their votes to their representatives from anywhere through internet. online voting system is an application of cryptography. This promises an efficient and secure way of casting and calculating the votes.

Making an voting system on internet has many challenges to overcome. Some major issues are voting in a secured manner and accompanying many voters. There are some internet voting system that cannot work in situation with many voters. Our proposal uses Homomorphic encryption to over come these issues.

Homomorphic approach in Internet and systems administration applications, [8]security is significant worry in the present time of IT. The tremendous measure of data traded across the Internet is helpless against security dangers and assaults. Cryptography gives secure trade of scrambled information by shared key. The significant worry with this methodology is information protection as anyone with the key can get to the information. In addition, client loses command over information once it is transferred to the cloud Client must impart a key to play out any activities. We need to download and unscramble the information and afterward play out the activity. These methodologies lead to security issue and rehashed encryption decoding. So in this system we have decided to go for Homomorphic encryption.

A homomorphic encryption[10] strategy permits client to work on ciphertext. At the point when client decodes the resultant figure, it is same as though tasks are done on plaintext. In this manner, utilizing homomorphic encryption guarantees clients that their information is secure in all state: stockpiling, transmission and preparing. Assume if someone wants to sum two numbers together eg 10 and 20 which are stored in form on encrypted number as 98746 and 654421 respectively after that the result of addition 10+20=30 is also stored in encrypted number as 783356. In traditional way they have to first decrypt the two numbers than add them and show the results. Consider than same situation for a large set of database example salary record of all employees working in a firm , if we use the traditional way we have to decrypt all records related to salary of each and every employee , thus exposing data (salary)[11] for employees . But if we would use Homomorphic encryption we can easy compute salary on all employees without decrypting there data. The computation is done directly on the encrypted data using Homomorphic encryption .Homomorphic encryption can either be completely or halfway homomorphic encryption. A fully homomorphic encryption system provides both multiplication as well as addition of ciphertext. Partially homomorphic encryption supports either additive homomorphic or multiplicative homomorphic encryption. Such plan can perform predetermined number of activities. For instance partial homomorphic encryption plans can do multiple addition with one multiplication.

Pascal Paillier gave Paillier cryptosystem in 1999. This cryptosystem is an public key system. Paillier cryptosystem is an partial homomorphic encryption[3] scheme that can can perform addition operation on ciphered data. The properties of Paillier's system are:

[*]e-mail: sakshamsaproo@gmail.com
[**]e-mail: vedantwarke99@gmail.com
[***]e-mail: sap5.3.1998@gmail.com
[****]e-mail: rashmisalvi@gmail.com

1) It is a symmetric key cryptographic scheme[6], which encrypts message using public key and retrieve message back from ciphertext using corresponding private key.

2) Paillier has probabilistic nature[3]. Every time the ciphertext is encrypted using Pallier system a new cipher text is generated, due to which it is difficult to uniquely identify whether both the ciphertext are generated for same message or not.

3) It supports additive property of homomorphic cryptosystem[3].

The proposed online voting system is effective , robust and simple using paillier cryptosystem.Paillier cryptosystem is an additive homomorpic encryption system which enables to do operation on encrypted number without decrypting it. Thus using this property of homomorphic encryption the proposed system provides users with availability , confidentiality and integrity.

This paper is divided in to six sections , the brief introduction is given in section one, section 2 explains what is Homomorphic encryption and its properties with Pallier cryptosystem in brief with key generation , encryption , decryption algorithm, the proposed methodology is discussed in third section , the result and analysis is discussed in section four followed by conclusion in section five.

2 Homomorphic Encryption

R. Rivest, M. Dertouzos and Leo. Adleman presented the idea of Homomorphic cryptosystem, long after the development of RSA [1]. It enables to operate on encrypted data. Let E be an encryption function used to encrypt plaintext, x as plaintext and f() as operation to implement , So homomorphic encryption is defined as :

f(E(x1),E(x2)....E(xn)) = E(f(x1,x2....xn))
Additive Homomorphism :
Binary operation is denoted by + ,so additive homomorphic is described as
E(x2) + E(x1) = E(x2 + x1)
Pallier Cryptography supports additive homomorphic property.

2.1 Paillier Cryptosystem

One of the well known scheme for homomorphic cryptography is Paillier [4]. It was invented by Pascal Paillier in 1999. It can encrypt many bits in single operation with an constant factor of expansion and also an efficient decryption. Pallier cryptosystem is defined by four terms: key generation, encryption, decryption and homomorphic operation. [4].

2.2 Key generation

Consider q and p are two big random prime numbers which are mutually exclusive of one another ,that is[12] $\gcd(qp, (q-1)(p-1)) = 1$.
The above property is assured if both prime number are equal to each other in length. [3] Compute n=qp and $\lambda = \text{lcm}(q-1, p-1)$. Randomly select g as integer where g$\in \mathbb{Z}^*_{n^2}$ The existence of multiplicative inverse ensure that the order of g is divisible by n by the following equation: $\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod n$,[18] where function L(x)=x-$1_{\frac{}{n}}$. Note that this a$_{\frac{}{b}}$ does not mean the multiplication of a times the multiplicative inverse of b, i.e., the biggest integer value v$\geq$ 0 to satisfy the relation a$\geq$ vb. The public key (encryption) is (n,g). The private key (decryption) is (λ, μ)..
If using q,p of same length, a simpler version of the key generation steps could be to set g=n+1,$\lambda = \varphi(n)$,, where $\varphi(n) = (p-1)(q-1)$

2.3 Encryption

Let x denote a message that we want to[4] encrypted where 0$\leq$ $x < n$.
Select r randomly where , r$\in$ $Z^*_{n^2}$ and 0<r<n (i.e ensure gcd(n,r)=1)
Compute ciphertext as:
c=g$^x \cdot r^n \bmod n^2$

2.4 Decryption

Let c be the encrypted text from which plaintext need to be extracted, where c$\in$ $\mathbb{Z}^*_{n^2}$ The original message can be computed as : x=L(c$^\lambda \bmod n^2) \cdot \mu \bmod n$ decryption is one exponentiation modulo n^2."[17]

2.5 Homomorphic characteristics

The importance of Paillier algorithm is due to its homomorphic properties and it can able to generate non-deterministic encryption.[5] As function of encryption is additive, following functions are described below:

2.6 Homomorphic addition on plaintext

The multiplication of two ciphertexts will give the addition of their corresponding plain texts when deciphered[2], D(E(x$_1, r_1) \cdot E(x_2, r_2) \bmod n^2) = x_1 + x_2 \bmod n.$ [16] The product of a ciphertext with a plaintext [8][9]raising g will decrypt to the sum of the corresponding plaintexts,[13] D(E(x$_1, r_1) \cdot g^{x_2} \bmod n^2) = x_1 + x_2 \bmod n.$

2.7 Homomorphic multiplication on plaintexts

An plaintext in encrypted form when raised to the power of one another plaintext in encrypted form will give the product of the two plaintexts when decrypted, D(E(x$_2, r_2)^{x_1} \bmod n^2) = x_1 x_2 \bmod n.$)

The product of constant with plaintext in encrypted form is a decryption result of an plaintext in encrypted form is raised with a constant k.

D(E(x$_1, r_1)^k \bmod n^2) = kx_1 \bmod n.$

In any case, in the event that we are given the Paillier encryptions of two messages ,it is highly unlikely to register an encryption of the result of these messages without the utilization of private key.

3 Proposed Methodology

In today's competitive worlds most of the lot of things are created on online platform similarly in internet voting system voter can cast their votes without visiting the election booth. Online voting system utilizes homomorphic encryption to count votes. The final outcome is taken from encrypted collection of votes without decrypting them, [4]. so it remains unknown who voted whom. In this system integrity and anonymity of the voter remains hidden. The voter should have to create their own account on this portal by verified government documents. The several stages for online voting system are given below.

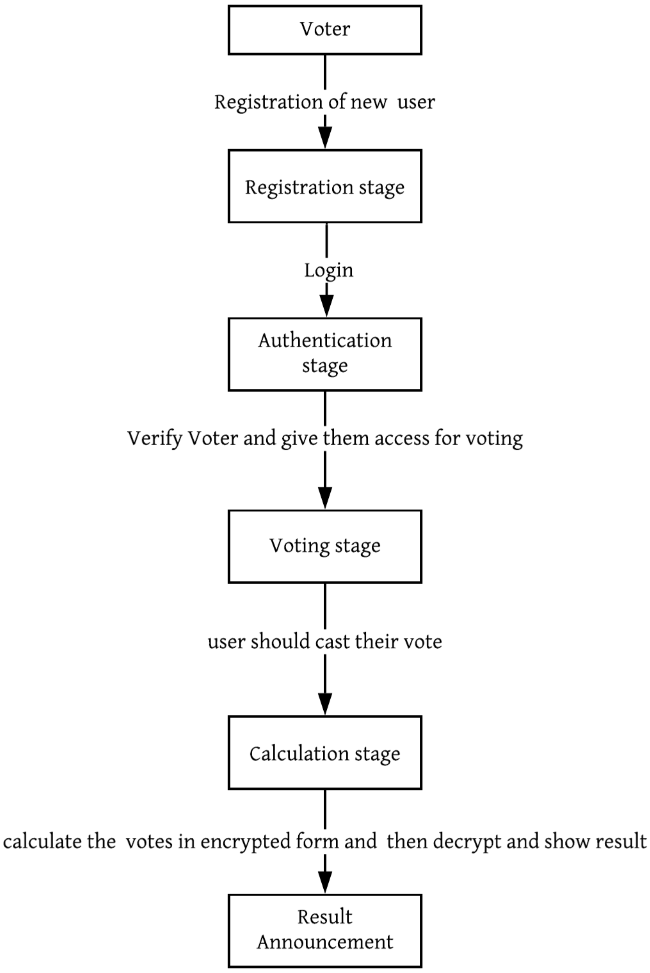

Voter
Registration of new user
Registration stage
Login
Authentication stage
Verify Voter and give them access for voting
Voting stage
user should cast their vote
Calculation stage
calculate the votes in encrypted form and then decrypt and show result
Result Announcement

Figure 1. Flow Diagram

1) Registration stage: In this stage we can add new voter in e-voting system by authenticating voter through Election authority. The eligibility of the individual voter is verified by collecting required details about them. User will enter their basic details and will add there voter id which will be crossed checked with the election commission database. After successful registration, user will able to cast a vote through e-voting system.

2) Authentication stage: This stage comes after registration stage. In this stage user will authenticate themselves using login id(which will be there voter id) and password that was set by the user in registration phase . Thus using user id and password users can get uniquely authenticated.

3) Voting stage: In this stage voter can give their vote . They can give vote to their selected candidate . The vote given by voters to their selected candidates are then encrypted using Paillier encryption. The encrypted votes are stored in database which will be then tallied in tally stage.

4) calculation stage: In this phase Votes that are stored in encrypted (using homomorphic encyption) form in database are added to get total no of votes received by the respective parties.

Consider we have two numbers 10 and 20, we have to perform the addition on encrypted numbers by using pailliar algorithm .

Table 1. Example of Encryption

10	gANjcGhlLnBhaWxsaWVyCkVuY3J5c
20	gANjcGhlLnBhaWxsaWVyCkVuY3J
10+20=30	gANjcGhlLnBhaWxsaWVyCkVuY3

In the above mentioned example it is observed that a new ciphertext is generated for a given number whenever it is encrypted, this feature helps to maintain the integrity and enhance the complexity of computation data[15]

4 Result And Analysis

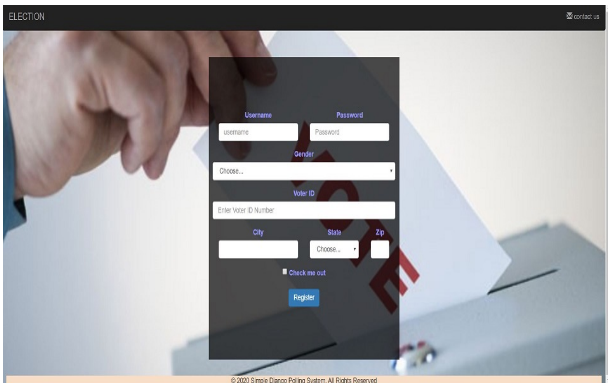
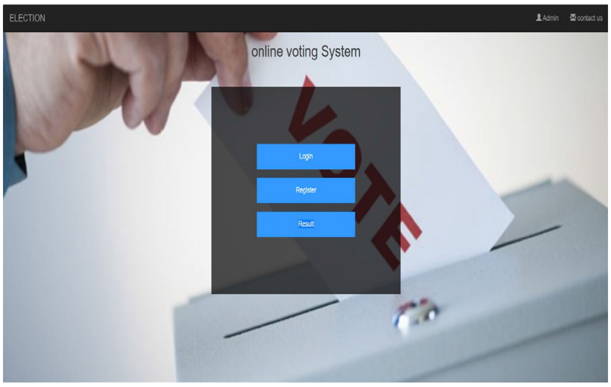


Figure 2. Registration form

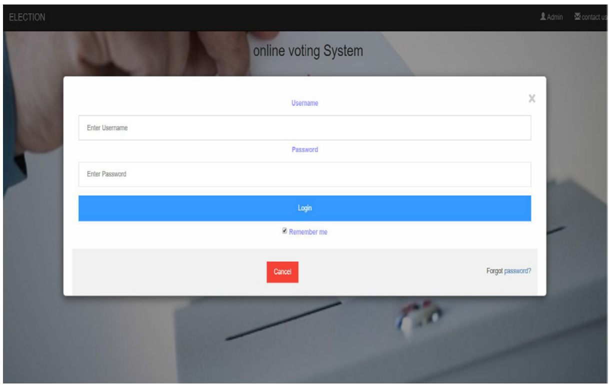
Voter will Register themselves on the portal by giving some basic details as their Fullname,password, voter id, gender, state. after fill the details user's voter id will be authenticated with government database of voter id.



online voting System

Figure 3. Home page

After successful registration stage user can login with their voterid as username and password that is set by them. Thus voters will be authenticated uniquely with the combination of voter id and password.



online voting System

Username

Enter Username

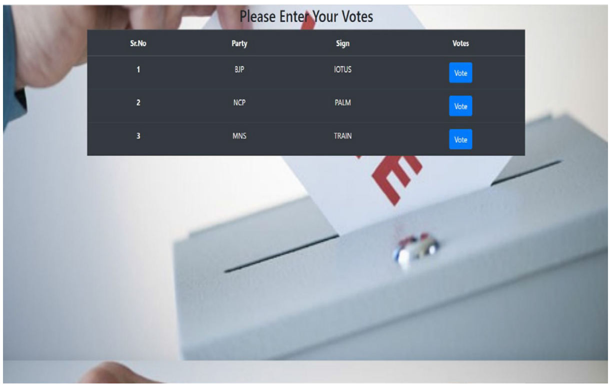
Password

Enter Password

☑ Remember me

Figure 4. Login page

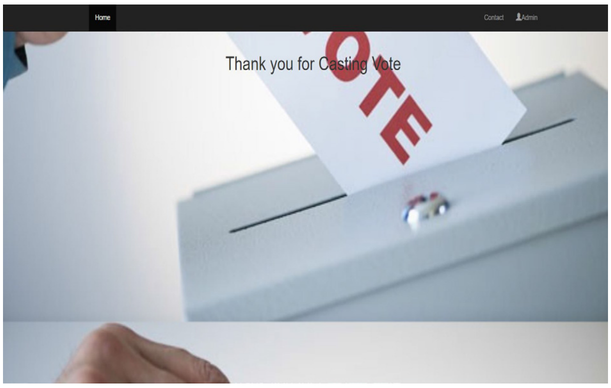
This is where voters will cast there vote to their choice of candidate. Candidates are denoted using there party symbol . Voter are needed to just tap on the button below the party symbol.



Please Enter Your Votes

Sr.No	Party	Sign	Votes
1	BJP	IOTUS	Vote
2	NCP	PALM	Vote
3	MNS	TRAIN	Vote

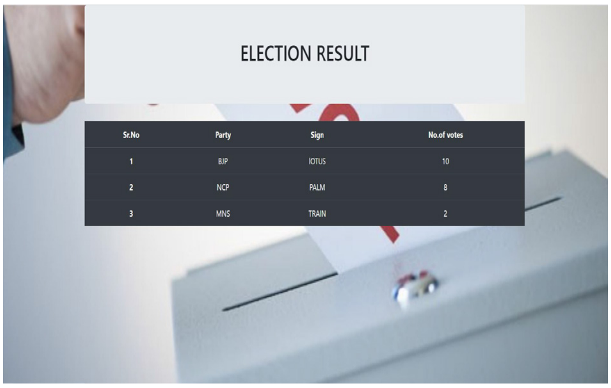
Figure 5. Voting Page



Thank you for Casting Vote

Figure 6. voting success page

After successfully casting their vote, voter's are shown a message of successfully voted and the voter are sent back to the login page and that voter cannot login again to vote. If they try to login again they will be shown a message "Already voted".



ELECTION RESULT

Sr.No	Party	Sign	No.of votes
1	BJP	IOTUS	10
2	NCP	PALM	8
3	MNS	TRAIN	2

Figure 7. Polling result

In existing system, Voter cast their votes online through e-voting system and the vote is stored in encrypted form using Paillier algorithm. The ballots are shuffled and apply the rotational method on votes for storing votes in database which increase the time and space complexity so the overall cost of the system will increases. The proposed system allows voter to cast the votes and store it in encrypted form using Paillier cryptosystem for maintaining the integrity of data. When vote casted for specific candidate, votes of that candidate stored in encrypted form and null value is in encrypted form automatically set to the remaining candidates in database. This will provide more security as the vote in encrypted form is updated in database for all candidates. The attacker as well as the admin or the employees who have access to the database will not able to distinguish between the ballots stored for the candidate is a vote cast by the voter or a null value. The final count of votes for each candidate is calculated using homomorphic addition property of Paillier cryptosystem. The proposed system is more faster and provides more security as all votes are stored in encrypted form and this will help in maintaining the three traids of the cyber security i.e. Availability , Confidentiality and Integrity of the system .

5 Conclusion

Voting through internet has attracted many people specifically people living far from their homes than traditional system of voting. From past few years a lot of researchers have started seeking interest in this field due to transparency and security concern. This research paper describes the internet voting system using Paillier algorithm and its homomorphic characteristics. This system gives a assurance of data confidentiality and data integrity in which it will uses homomorphic properties for calculation of votes in there encrypted form and then decrypting them to get only total votes thus keeping it secure. This system is equivalent to system in which votes are taken in unencrypted form and then added to get then total votes received by the party. Thus it provides us with the use fullness of traditional system plus the security and modularity of modern system.

References

[1] Salavi R.R., Math M.M., Kulkarni U.P. (2019) A Survey of Various Cryptographic Techniques: From Traditional Cryptography to Fully Homomorphic Encryption. In: Saini H., Sayal R., Govardhan A., Buyya R. (eds) Innovations in Computer Science and Engineering. Lecture Notes in Networks and Systems, vol 74. Springer, Singapore

[2] K. K. Chauhan, A. K. S. Sanger and A. Verma, "Homomorphic Encryption for Data Security in Cloud Computing," 2015 International Conference on Information Technology (ICIT), Bhubaneswar, 2015, pp. 206-209.

[3] M. Nassar, A. Erradi and Q. M. Malluhi, "Paillier's encryption: Implementation and cloud applications," 2015 International Conference on Applied Research in Computer Science and Engineering (ICAR), Beirut, 2015, pp. 1-5.

[4] Shihab, T Liji, P. (2017). Simple and secure internet voting scheme using generalized paillier cryptosystem. 551-557. 10.1109/ICICICT1.2017.8342623.

[5] M. Togan and C. Pleca, *"Comparison-based computations over fully homomorphic encrypted data,"*. in Proc. 10th International Conf. Communications, pp. 1–6, 2014

[6] C. Gentry, *"Fully homomorphic encryption using ideal lattices,"*. in Proc. the 41st Annual ACM Symp. Theory of Computing, pp. 169- 178, 2009.

[7] R. L. Rivest, L. Adleman, and M. L. Dertouzos, nations where vote casting cooperation is low and it is too helpful for people living far o *"On data banks and privacy*. homomorphisms," Foundations of secure computation, vol. 4, no. 11, pp. 169–180, 1978.

[8] C. Gentry et al. , *"Fully homomorphic encryption using ideal lattices."*. in STOC, vol. 9, 2009, pp. 169–178.

[9] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, *"(leveled) fully homomorphic encryption without bootstrapping,"*. in Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. ACM, 2012, pp. 309–325.

[10] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, *"A survey on homomorphic encryption schemes: Theory and implementation,"*. ACM Comput. Surv., vol. 51, pp. 79:1–79:35, July 2018.

[11] P. Y. Ryan, S. Schneider, and V. Teague, "End-to-end verifiability in voting systems, from theory to practice," IEEE Security and Privacy, vol. 13, no. 3, pp. 59–62, 2015.

[12] I. Damgard, M. Jurik, and J. 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.

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

[14] D. Hrestak and S. Picek, "Homomorphic encryption in the cloud," in Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014 37th International Convention on. IEEE, 2014, pp. 1400–1404.

[15] C. Ngo, "Secure voting system using paillier homomorphic encryption," Ph.D. dissertation, Texas AM University–Corpus Christi, 2014.

[16] Y. Yang, S. Zhang, J. Yang, J. Li, and Z. Li, "Targeted fully homomorphic encryption based on a double decryption algorithm for polynomials," Tsinghua science and technology, vol. 19, no. 5, pp. 478– 485, 2014.

[17] A. Snak, S. Ozkan, H. Yldrm, and S. Kiraz, "End-2-end verifiable internet voting protocol based on homomorphic encryption," International Journel Of Information Security Science, vol. 3, no. 2, pp. 165–181, 2014.

[18] A. Huszti, "A homomorphic encryption-based secure electronic voting scheme," Faculty of Informatics. University of Debrecen. Hungary, 2011.