A Survey on-Confidentiality Preserving in Instant Runoff Voting Method

Shital Chattar
Pimpri Chinchwad College of Engineering

Reena Kharat
Pimpri Chinchwad College of Engineering

ABSTRACT
The E-voting promises the chance of convenient, straightforward and economical. Recently in cryptography some modifications guaranty to allow us to run difficult algorithms within the encrypted domain. During this state of matter, Majority technique may be a new scheme for a brand new electoral system. This system is with lots of mark able advantages, means a lot of concerned tallying method than first-past-the-post selection. To protect voter's privacy, a method must be done b solely manipulating encrypted knowledge by Instant-runoff selection (IRV). Generally IRV referred to as hierarchic order selection, permits voters to rank their preferences for a specific workplace among multiple candidates. Though the precise strategies of vote calculations will vary, within the finish the system is determined to make sure that the winner has the support of a majority of voters. This scheme will effectively ensure confidentiality and integrity of ballot in instant runoff voting method.

Keywords
Online voting, encryption, decryption, ballot, Instant runoff

1. INTRODUCTION
Elections permit the individuals to decide on their representatives and categorical their preferences for the way they're going to be ruled. Basically, the integrity of the election method is key to the integrity of democracy itself. The election system should be sufficiently strong to resist a range of fraudulent behaviors associated should be sufficiently clear and graspable that voters and candidates can settle for the result of an election.An electoral systemcould be aset of rules that determineshoweverelections area unit conductedand the waytheirresultsareaunitdetermined.Electrolsystemaccommodte ssets of rules that describes all aspects of theballot process. When electionhappens, who is allowed to vote, whowillstand as a candidate, how ballotsarea unit marked andforged, how the ballots area unit counted.

Types of electrol systems are **plurity voting: Plurality** voting is system within which the candidates with the best number of votes can win, with no demand to get a majority of votes. **Majority voting**: It could be a system within which the candidate got to receive a majority of votes to be electoral**. Proportional voting:** It is electoral system within which division in associate degree electro rate are reflected proportionately within the electoral body.E-voting Electronic pick is once an elector casts a ballot through a digital system rather than on paper. Instant - runoff pick (IRV) may be a voting technique utilized in single-seat elections with quite two candidates rather than pick just for one candidate. Voters in IRV elections will rank the candidates so as of preference. Ballots area unit at the start counted for each elector's prime selection, losing candidates area unit eliminated, and ballots for losing candidates area unit decentralized till one candidate is having majority votes. Once the sector is reduced to two, it's become an associate "instant runoff" that enables a comparison of the highest two candidates head-to-head. IRV has the result of avoiding split votes once multiple candidates earn support from similar voters.

2. LITERATURE SURVEY
A. Yang, Xuechao,[1] propose a secure verifiable Ranked choice online voting system based on homomorphic Encryption. Elections conducted on paper consume a many resources and contribute to the destruction of forests, which leads to climate deterioration. Recent on-line voting experiences in countries, like the United States, India, and Brazil, incontestable that additional analysis required to enhance security guarantees for future elections, to ensure the confidentiality of votes and modify the verification of their integrity and validity. In this paper, we tend to plan a ranked selection online voting system, which addresses these challenges. It eliminates all hardwired restrictions on the possible assignments of points to completely different candidates according to the voter's personal preferences. In order to protect the confidentiality of the votes, every cast ballot is encrypted using the exponential ElGamal cryptosystem before submission. During voting system ensures that proofs are generated and hold on for every part within the cast ballot. These proofs can then be wont to verify the correctness and additionally the eligibility of every ballot before counting while not decrypting and accessing the content of the ballot. This validates the votes within the counting method and at the same time maintains confidentiality. The security and performance analyses included during this paper demonstrate our technique has achieved significant improvements compared with the previous systems. The outcomes of our paper additionally show that our proposed protocols are possible for practical implementations. The fundamental plan of our voting system is to encrypt every ballot using the common public key of the distributed ElGamal cryptosystem. Since the exponential ElGamal satisfies the additive homomorphic property, the encrypted ballots can be directly tallied. This procedure is additionally called homomorphic tallying. Finally, the tallied result will decrypted by collaboration of all authorities. In this paper e-voting system consists of the following stages: initialisation,registration, ballot casting, verification of voters, verification of ballots, tallying and result revealing.[1]

B. Vanstone,Scott A.[2] propose a Elliptic curve cryptosystem due to strong, fast public key cryptography for securing constrained environment.Elliptic Curve Cryptography has been a recent analysis area within the field of Cryptography [2]. It provides higher level of security with lesser key size compared to other cryptologic techniques. The new technique has been proposed throughout this paper wherever the classic technique of mapping the characters to affine points in the elliptic curve has been removed [11]. The corresponding ASCII values of the plain text are paired up. The paired values function input for the Elliptic curve cryptography. This new technique ignores the expensive operation of mapping and conjointly the need to share the common look up table between the sender and conjointly the receiver [10].

C. Aditya, Riza propose [3] a secure e voting for preferential election. E-voting systems will greatly progress the potency, and doubtless, the transparency of national elections. However, the protection of such systems is an area of on-going analysis. The literature for secure e-voting is predominantly involved with1-out-of-m selection strategies, wherever m is the variety of candidates running for the elections. This paper presents a case study of crypto logical protocols for secure e-voting systems that use advantageous selection strategies. The size of the electronic vote for a advantageous electoral system is inherently larger than a 1-out-of-m electoral system, once the amount of candidates, m, increases. In advantageous electoral system, the dimensions of the vote is a minimum of log2 (m!) bits. Thus the selection systems using some typeofhomomorphi c coding tend to be inefficient or impractical selection systems that use mix-networks,on theopposite hand, don't need a special kind fortheelectronicvote.The procedure complexness i sn't adversely affectedby the amount of candidates.

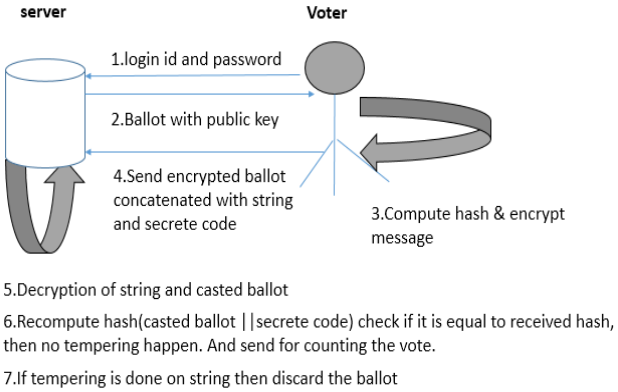
D. Peng, Kun [4] propose evoting using multiplicative homomorphic encryption. In the security world, Cryptography is one the most mentioned topics. The aim of this project is to develop a small scale secure on-line E-Voting paradigm system utilizing the Homo-morphic encoding Technique of the Paillier Cryptosystem [6] internet services in an attempt to and possible solutions to any improve existing legal system. The E-Voting system guarantees eligibility, privacy, and verifiability and additionally receipt freeness, no vote commercialism and uncoercibility. On-line option would be a lot of convenient, comparatively secure and utilize fewer resources over the standard voting system. The protocol permits a voter to forged his/her ballot anonymously, by exchanging untraceable however authentic messages. To be able to access e-voting system from a private, business or perhaps a library computer is also a lot of convenient for several individuals to vote. One amongst the primary options of this technique is its pertinence to figure on cloud in-frastructure, whereas preserving its security characteristics. This might really be a solution for the low vote at the polls that happens because of the reluctance of voters to indicate up at the polls as they're terrified of large crowd [8].

E. Keller, Jason, and Joe Kilian [5] propose a linked-list approach to cryptographically secure elections using instant runoff voting. Number of ways have been planned to conduct cryptographically secure elections. Most of those protocols specialize in 1-out-of-n voting schemes. Few protocols are devised for discriminatory voting system, within which voters provide an inventory of rankings of the candidates, and many of these treat ballots as if they were ballots in a 1-out-of-n option theme. We have a tendency to propose a linked-list-based theme that gives improved privacy over current schemes, hiding citizen preferences that should not be disclosed. For big lists of candidates we have a tendency to reach improved straight line performance.

3. PROPOSED METHODOLOGY

In the proposed system, user first register for election voting, on the basis of registration system will generate secret code and save it in database, Generated secret code and Ballet sequence is used for encryption with hash code, that hash code used to identify tempering votes in the system at the time of decryption.

A. Architecture



4. RESULT AND DISCUSSIONS

Instant runoff pick system uses stratified selection ballots to simulate a standard runoff in a single round of pick. Voters rank candidates in order of preference. They are usually given the choice to the rank as several or as few candidates as they would like. Indicating support for the lesser choice never counts your higher selection. Each elector has a one vote. That vote is counted at the start for the voter's first selection. If there are quite two candidates who receive votes, the lowest candidate with the fewest votes is eliminated. Quite one candidate may be eliminated at the similar time if their combined vote is a smaller amount than the whole of the alternative remaining candidate. Ballots enumeration for the eliminated candidate is additional to the totals of the candidate stratified next on every ballot. This method of eliminating lowest candidates and adding ballots solid for those candidates to the totals of the next-ranked selection thereon ballot continues till two candidates stay. The candidate with a bulk of votes during this final round is said the winner.

5. CONCLUSIONS

The planned Instant Runoff vote technique is preventing the privacy of voter and confidentiality of vote casted using ECC(Elliptic curve cryptography)and SHA-256 .This IRV system can be used anytime and from anywhere by the employees. It excludes the use of manual voting process. Employees can keep themselves updated with all things going on in the organization. No one can cast votes on behalf of others and multiple times. This voting method will Saves time and reduces human intervention. It will makes employees happy as their opinions are considered for the matters in organization.Admin can get instant result. The system is flexible and secured to be used.

6. REFERENCES

[1] Yang, Xuechao, et al. "A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption." IEEE Access 6 (2018): 20506-20519.

[2] Vanstone, Scott A. "Elliptic curve cryptosystem—the answer to strong, fast public-key cryptography for securing constrained environments." *Information Security Technical Report* 2.2 (1997): 78-87.

[3] Aditya, Riza, et al. "Secure e-voting for preferential elections." *International Conference on Electronic Government*. Springer, Berlin, Heidelberg, 2003.

[4] Peng, Kun, et al. "Multiplicative homomorphic e-voting." *International Conference on Cryptology in India*. Springer, Berlin, Heidelberg, 2004.

[5] Keller, Jason, and Joe Kilian. "A linked-list approach to cryptographically secure elections using instant runoff voting." *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, Berlin, Heidelberg, 2008.

[6] Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 223238. Springer, Heidelberg (1999).

[7] W. Lu, A. L. Varna, and M. Wu, ‘‘Confidentiality-preserving image search: comparativestudy between homomorphic encryption and distance-preserving randomization,’’ IEEE Access, vol. 2, pp. 125–141, 2014

[8] Parmar, Payal V., et al. "Survey of various homomorphic encryption algorithms and schemes." *International Journal of Computer Applications* 91.8 (2014)..

[9] Ahmad, Tohari, Jiankun Hu, and Song Han. "An efficient mobile voting system security scheme based on elliptic curve cryptography." *Network and System Security, 2009. NSS'09. Third International Conference on*. IEEE, 2009.

[10] Vanstone, Scott A. "Elliptic curve cryptosystem—the answer to strong, fast public-key cryptography for securing constrained environments." *Information Security Technical Report* 2.2 (1997): 78-87.

[11] M. Hirt and K. Sako, ``Effcient receipt-free voting basedonhomomorphic encryption," in *Advances in Cryptology_EUROCRYPT*. Bruges, Belgium: Springer, 2000, pp. 539_556. [Online]. Available: