RESEARCH ARTICLE OPEN ACCESS

A SECURE VERIFIABLE INTERNET VOTING SYSTEM USING IDENTITY BASED ENCRYPTION AND DECRYPTION

Kevin Gabriel Houlder [1], Nithishwar P [2], Santhosh G [3], Venkatesh E [4]

[1][2][3][4] UG Scholar, Department of Information Technology
SRM Valliammai Engineering College
Chennai - India

ABSTRACT

To ensure 100% voting automation came into play. But this automated system have been approved only on some developed countries since security have not been ensured to a large extent. Our main aim of the proposed system is to develop a compatible voting machine with high security . The proposed system is mainly designed for our country. It has three phases. First the details of the persons who are above 18years are extracted from aadhar card database since it had become mandatory in present scenario. Automatically a new voter id with necessary details will be created and an intimation will be given to the persons to ensure more security, finger prints and face recognition of the voter is used as the main authentication resource. Since the finger pattern as well as face of each human being is different, the voter can be easily authenticated. As soon as they cast their vote, their voter id and other details will be erased automatically and the Aadhar card details which they used will be tracked and will be locked to access. This is done to preserve the security, people cast their vote the results will be updated automatically and on the same day of election, the results will also be published

Keywords: Aadhar Card, Finger Print, Face Recognisation, Encryption, Decryption, End to End Verification.

I. INTRODUCTION

The main objective of the democracy is "vote" by which the people can elect the candidates for forming an efficient government to satisfy their needs and requests such that their standard living can be improved. In developing countries like "INDIA" the election commission follows manual voting mechanism which is done by electronic voting machine. This machine is placed in the poll booth centre and is monitored by higher officials. due to some illegal activities the polling centre are misused and people's vote to right has been denied.This seldom occurs in rural areas as well as in urban cities because the educated people are not interested in casting their votes to candidates who represent their respective areas.To ensure 100% voting automation came into play. But this automated system have been approved only on some developed countries since security have not been ensured to a large extent.

1.1 OBJECTIVE

To study the electronic voting protocols from the security perspective. First the details of the persons who are above 18years are extracted from Aadhar card database since it has became mandatory in present scenario. To ensure more security, finger prints and face recognition of the voter is used as the main authentication resource.

People cast their vote the results will be updated automatically and on the same day of election, the results will also be published

1.2 BENEFITS

Travelling cost for voting will be reduced. This system is very useful to people who are physically challenged. Manual work done by the peoples in poll booth will be reduced. By avoiding travelling pollution will be minimized. The people who are in foreign countries (NRI's)can also cast their vote from their respective places by this 100% vote and full pledged democracy can also be achieved. It will be more useful for physically challenged voters

1.3 CHALLENGES

The main challenges is, the voters should know how to handle this proposed system and hardware equipment is mandatory, sometimes trust can be broken.

II. LITERATURE SURVEY

The following works explain the system used in various fields using online voting system

Mahender Kumar , Satish Chand, and C. P. Katti "A Secure End-to-End Verifiable Internet-Voting System Using Identity-Based Blind Signature- 2020 IEEE

The end-to-end (E2E) verification enables a voter to check if his ballot is recorded as he intended and the public to check if the system has correctly counted all of the recorded ballots. Several E2E voting systems have been discussed in the last decade in terms of analyzing the e-voting system and formalizing its security requirements. This article presents an E2E verifiable internet voting system that provides mobility to a voter and allows him to cast his vote secretly in public computer with the benefit of early voting. The system provides a digital witness to a voter that enables him to check whether his vote is recorded as he meant and the public to check if all the recorded ballots are counted correctly. The privacy of the proposed system is achieved under the elliptic curve discrete logarithm and gap Diffie–Hellman assumptions

SHIYAO GAO,IEEE 2019 "An Anti-Quantum E-Voting Protocol in Blockchain with Audit Function". this scheme has the ability to audit voters operating incorrectly and resist quantum attacks by adopting the certificateless and code-based cryptography. After performance analysis, our scheme is suitable for the small-scale election and has some advantages in security and efficiency when the number of voters is small

Mohammad Hamdaqa, Gísli Hjálmtýsson , Science Reykjavik University, Iceland 2018 IEEE. "Blockchain-Based E-Voting System", Building a secure electronic voting system that offers the fairness and privacy of current voting schemes, while providing the transparency and flexibility offered by electronic systems has been a challenge for a long time. In this work-in-progress paper, we evaluate an application of blockchain as a service to implement distributed electronic voting systems. The paper proposes a novel electronic voting system based on blockchain that addresses some of the limitations in existing systems

Xuechao Yang, 2018 IEEE "A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption"The security and performance analyses included in this paper demonstrate that our method has achieved significant improvements in comparison with the previous systems. The outcomes of our experiments also show that our proposed protocols are feasible for practical implementations.

Dr. Z.A. Usmani Computer Engineering Department M. H. Saboo Siddik College of Engineering Mumbai, India.2017 IEEE conference on innovation of Information Technology "Multi propose platform independent on online voting system" The voting system is the backbone of every democracy and organization. The voting system has experienced many efficient changes in the past few decades. There are various voting techniques used such as Paper Ballot Voting System, E-Voting System also known as Electronic Voting System, Internet Voting System, SMS and Miss Calls Voting System.

III. MODULE DESCRIPTION

LIST OF MODULES:

- **IDENTIFICATION OF VOTERS**
- **PROCESS OF VOTING**
- **FINALISING OF RESULTS**

IDENTIFICATION OF VOTERS

The system starts with a initial face of identifying where voters aadhar card details along with their face and fingerprint is identified. If his/her vote is valid (above 18) will be allowed to vote. If verification is done successfully and voters will be allowed to cast their vote.

PROCESS OF VOTING

After the verification is done successfully and voter can vote to their respective candidate by selecting them. After voting is done and voter vote will be converted to an encrypted form and decryption will be done only if the election commissioner identities are verified.

FINALISING OF RESULTS

The verification of the election commissioner is done after that decryption takes place and result will be finalized and announced to the public

IV. SYSTEM DESIGN

The front end is designed with php and backend is designed with python. The biometric verification and registration are done by MatLab.

4.1ARCHITECTURAL DESIGN

The architectural diagram of online voting system depicts with a voter who can vote their respective candidate through three faces identifying; process and finalising. The voter registration details will be stored and its managed by EC, the details of all the voters will be maintained in pollbooks. After verification is done, voter can vote for their candidates and voting is done successfully the result will be announced by EC (after encryption and decryption is done). The proposed system can be used for both central and state election. The system starts with an initial face of identifying where voters aadharcard details along with their face and fingerprint will be recognized before identification the web page will be displayed and divided into two sides. One is for physically challenged and another one is for normal peoples. If a voter

selects for a physically challenged means on that its categorized into blind and without hands. For blind voter he/she can be identified by using his/her fingerprint and trusted person face and fingerprint recognition. For without hand voter he/she will be identified by using face recognition and trusted person face and fingerprint recognition and for normal person identification can be done by verifying his/her face and fingerprint and voters will be provided with three trials after that he/she should answer the questions which is being asked on their registration time and if verification is done successfully, the voter will be accessed to the next step(process), where voter can vote for their respective leaders. In this stage encryption process will takes place after voting. Finally the vote will be decrypted when Election Commissioner opens for a result announcement. Before this process Election Commissioner will be identified with his/her face and fingerprint. If he/she fails to identity within 3 trials, code will be send from central cyber hub to Election commissioner mail id after that should answer the questions which is being asked on their registration time

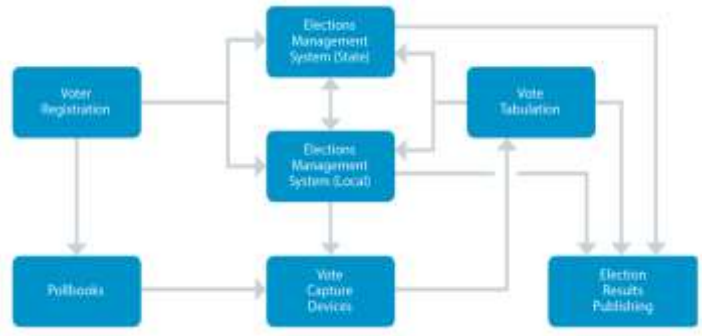

Fig -1: Architecture Diagram

V. ALGORITHM

5.1ADVANCED ENCRYPTION STANDARDS

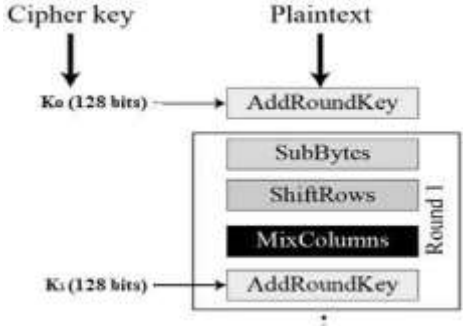

Fig -2: AES Diagram

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involves huffling bits around (permutations). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

5.2 TRIPLE DES

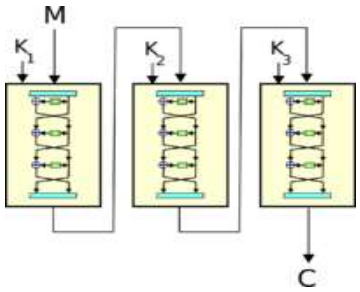

Fig -3: Triple Des Diagram

Encrypt the plaintext blocks using single DES with key K_1.Now decrypt the output of step 1 using single DES with key K_2.Finally, encrypt the output of step 2 using single DES with key K_3.The output of step 3 is the ciphertext. Decryption of a ciphertext is a reverse process. User first decrypt using K_3, then encrypt with K_2, and finally decrypt with K_1.

VI. SECURITY ANALYSIS OF OUR SCHEME

Theorem 1 (Unforgeability)

Based on the hard of CDHP, our e-voting scheme is unforgeable in the random oracle model.

Proof. Setup: The Adversary A is given the system parameters param = {G1, G2, G, Ci , PK1i , H1, H2, Ppub, g, e, f} generated by the Simulator S.

Random Oracle: The Simulator S receives the hash request from the Adversary A, then S queries the hash function H2 and returns the hash value to A as a response.

Joining Oracle J O: The Adversary A gets a set U = {PK1, PK2, ...,PKn} of all the voters' public keys through n queries.

Corruption Oracle CO: On input a public key PKi ∈ PK that is output from J O, and the Simulator S checks whether it corresponds to the set U. If it is, S stops immediately, otherwise, S outputs the corresponding private key.

Signing Oracle SO: On input a ballot, a set U and the signature voter's public key, then S simulates the following process:

(1) Choose a random index k ∈ {1, 2, ..., n}.

(2) The Simulator S selects random numbers ri ∈ Z ∗ q , i = 1, 2, ..., n, aj ∈ Z ∗ q , j = 1, 2, ..., n, j 6= k and computes Tj = ajG, Pi = ri (G + qi), Si = riPK2i , U = xk Pn i=1 Pi . Then S

computes the hash value hj = H2 (Ballot||f (Tj)||f (U)||det(A)) by using Random Oracle.

(3) S selects the random number ak ∈ Z ∗ q and computes Tk = akQk − Pn j (Tj + hjPK2j). Then S computes the hash value hk = H2 (Ballot||f (Tk)||f (U)||det(A)) by Random Oracle.

(4) Compute Z = hkxkPpub + hkSK2k + akdk and get the final signed ballot

σ = (Ballot, T1, T2, ..., Tn, S1, S2, ..., Sn, U, Z, A).

(5) Adversary A can adaptively query the SO. We prove the unforgeability of our scheme through contradiction. Assume that the Adversary A can forge a valid signed ballot

σ = (Ballot0, T0 1 , T0 2 , ..., T0 n , S0 1 , S0 2 , ..., S0 n , U0 , Z0 , A0) that was not obtained through the SO. According to the forking lemma for ring signature , the Adversary A can forge another valid signed ballot

σ = (Ballot0 , T0 1 , T0 2 , ..., T0 n , S0 1 , S0 2 , ..., S0 n , U0 , Z00 , A0) with non-negligible probability. The two forged signed ballots have the same randomness for the same content of ballot and the ring user group U formed by the voters.

Ppub, Pn i=1 Ti+h 0 iPK2 0 i = e G, Z0 e Ppub, Pn i=1 Ti+h 00 i PK2 0 i = e G, Z00According to the above formulas, we get e G, Z0 − Z 00 = e Ppub, Pn i=1(h 0 i − h 00 i)PK2 0

By using the forking lemma for ring signature, there are indexes i and j, which satisfy h 0 i − h 00 i = 0 and h 0 j − h 00 j 6= 0, i 6= j. Thus e G, Z0 − Z 00= e Ppub,(h 0 j − h 00 j)PK2 0 j

The probability of PK2 0 j = PK2k is 1 |U | , so there is (1) e G, Z 0 − Z 00 = e Ppub,(h 0 j − h 00 j)a(G + q) = e G, sa(h 0 j − h 00 j)(G + q) Thus (2) Z 0 − Z 00 = sa(h 0 j − h 00 j)(G + q) = saG(h 0 j − h 00 j) + saq(h 0 j − h 00 j) saG = (Z 0 − Z 00 − saq(h 0 j − h 00 j))(h 0 j − h 00 j) −1

Based on the computational difficulty of CDHP, the probability that the Adversary A wins the game is negligible.

Theorem 2 (Conditional Anonymity).

Our e-voting scheme is conditional anonymity. Proof. We prove the conditional anonymity of our scheme from the following two points.

(1) In this e-voting system, the anonymous is realized by using the ring signature technology to hide the identities of voters. When voters sign the Ballot, they first compute Si = riPK2i through the public key addresses of all voters. P

(2) Secondly, when computing Tk = akQk − n j (Tj + hjPK2j), their public key addresses are also required. Si and Tk will be the part of the signed ballot (Ballot)Sig k .

Therefore, the signer's public key address can be hidden in all of the authenticated voters, and anyone, including the regulator, cannot judge the determined signer from signature σ.

Only when the audit is required, the regulator revokes their anonymity through cooperating with every voter.

Theorem 3 (Verifiability)

Our e-voting scheme is verifiability. Proof. Verifiability includes personal verifiability and universal verifiability. In terms of personal verifiability, all of the voters can check and count the transaction data on the chain to verify whether their ballots are counted.

In terms of universal verifiability, because the distributed ledgers in the blockchain are public, anyone interested in the election results is able to get a copy of the ledgers, verifying whether the digital signature is correct, count the election results, and compare with the official results to ensure the verifiability of the electronic voting scheme.

The correctness of the digital signature is verified as follows: Verifier Knows (Ballot)Sigk = (Ballot, T1, T2, ..., Tn, S1, S2, ..., Sn, U, Z, A), then computes hi = H2 (Ballot||f (Ti)||f (U)||det(A)) and verifies the validity of bilinear pairings e (Ppub, Pn i=1 Ti+hiPK2i) = e (G, Z).

(3) e Ppub, Xn i=1 (Ti + hiPK2i) ! = esG, Tk + hkPK2k + Xn j=1 (Tj + hjPK2j) = e sG, akQk − Xn j (Tj + hjPK2j) + hkPK2k + Xn j=1 (Tj + hjPK2j) = e (G, s(akQk + hkPK2k)) = e (G, akdk + hkxk (Ppub + dk)) = e (G, Z)

Theorem 4 (Auditable)

Our e-voting scheme is auditable. Proof. Since the traceable ring signature technology is employed in our e-voting scheme, When the consensus of voting cannot be reached, the anonymity of voter is revoked through a round of interaction with them and find the signer corresponding to the ballot. The correctness of the anonymity revocation of the voter is verified as follows: a. The regulator verifies the validity of bilinear pairings e (Si , G + Qi) = e (Pi , PK2i).

(4) e (Si , G + Qi) = e (riPK2i , G + Qi) = e (rixi (G + Qi), G + Qi) = e (ri (G + Qi), xi (G + Qi)) = e (Pi , PK2i) b. The regulator verifies the validity of bilinear pairings e (U, G + Qi) = e (V, PK2i). (5) e (U, G + Qi) = e xk Xn i=1 Pi , G + Qi ! = e Xn i=1 Pi,xk (G + Qi) ! = e (V, PK2i)

Theorem 5 (Resistance to attacks).

Our e-voting protocol is able to defend against the replay attack, the man-in the-middle attack, the counterfeiting attack, the modification attack and quantum attack. Proof. The details of the defense against the above attacks are as follows.

(1) Replay attack: In the process of generating signed ballots, the voters are required to choose random numbers ri ∈ Z ∗ q , i = 1, 2, ..., n, aj ∈ Z ∗ q , j = 1, 2, ..., n, j 6= k, ak ∈ Z ∗ q . Therefore, it is possible to detect the replay of the signed ballot and conclude that our scheme can resist the replay attack.

(2) Man-in-the-middle attack: In the preparation phase, the generation of the key pair PK2i , SK2i that the voter uses to sign the ballot is based on CDHP. Any adversary cannot get the private key through the public values or parameters.

(3) Counterfeiting attack: Based on the proof of Theorem 1, any adversary is not capable of forging a signed ballot (Ballot)Sigk = (Ballot, T1, T2, ..., Tn, S1, S2, ..., Sn, U, Z, A) without the voter's private key.

(4) Modification attack: In our scheme, the voters sign the ballot and record the signed ballot on the blockchain. If the adversary tampers with the ballot, it can be found by verifying its digital signature,it is impossible for an attacker to tamper with the recorded transaction, since every block of the chain contains the hash values of all transactions. The modification attack is successful if the attacker can modify the recorded ballots in each block. However, this probability is negligible due to the anti-collision of the hash function.

(5) Quantum attack: In our protocol, the regulator generates and distributes the P SK for each voter. The algorithm is a cryptographic algorithm based on the code, and its security is reduced to the syndrome decoding (SD) problem of coding theory. This is an NP-complete problem, which is difficult to solve even in front of quantum computers with powerful computing power. So, our e-voting scheme is able to resist the quantum attack.

VII. CONCLUSION

Democracy can only be achieved by voting to obtain that democracy 100% of voting is needed this can be achieved by our proposed system with an advanced security. The voters details will be maintained confidentially and the voting result will be published in favour of public not in favour of any officials. The system will be easily accessed to all of the peoples. Apart from poll booth voting, online voting accuracy will be more effective and efficient. In this paper, a blockchain e-voting protocol with audit function is introduced. We adopt to resist the quantum attacks. In our scheme, the KGC in certificateless cryptosystem is introduced as a regulator. It not only realized the anonymous of voters but also provided the feature of the audit by combining with the traceable ring signature algorithm, to maintain the fairness

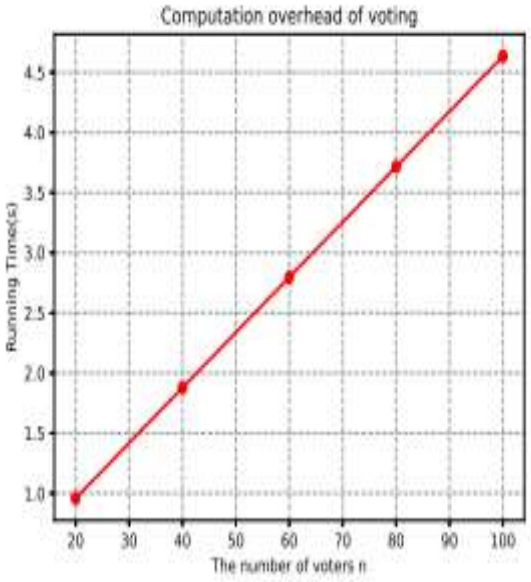

Fig-4: Computation Overhead Of Voting

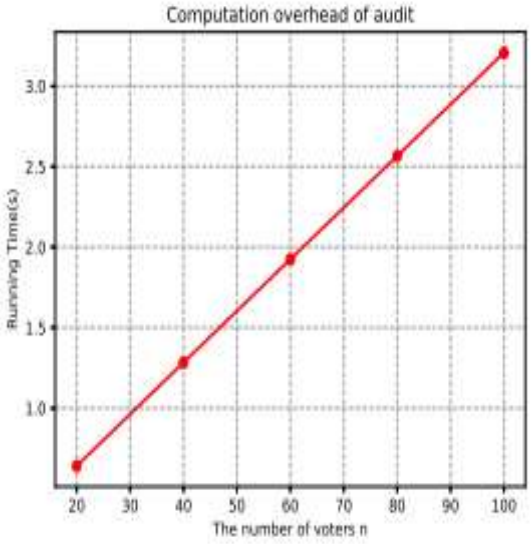

Fig-5: Computation overhead of Audit

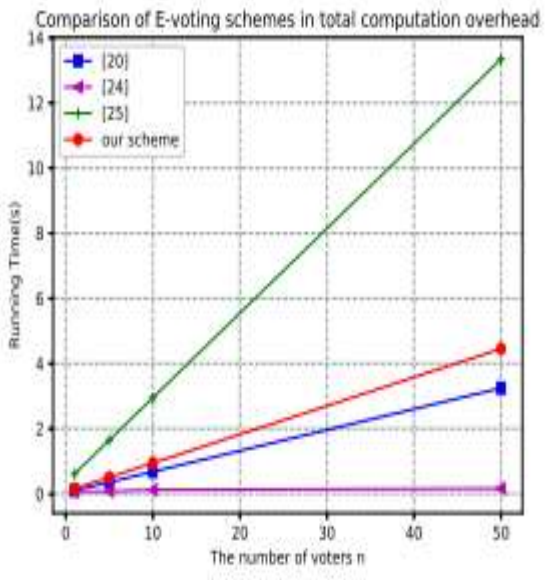

Fig-6: Comparison of E voting Schemes in Total Computation Overhead

VIII. FUTURE WORK

In future, we can widely develop this system with higher security and we will add some additional features to protect vote of voters and the system will be developed in mobile for easy access to the peoples with all features available in laptop and computer

REFERENCES

[1] TechCrunch, (2018). Liquid democracy uses blockchain to fix politics, and now you can vote for it. Available at: https://techcrunch.com/2018/ 02/24/liquid-democracy-uses-blockchain/

[2] Ajit Kulkarni, (2018), "How To Choose Between Public And Permissioned Blockchain For Your Project", Chronicled, 2018.

[3] "What Are Smart Contracts? A Beginner's Guide to Smart Contracts", Blockgeeks, 2016. Available at: https://blockgeeks.com/guides/ smart-contracts/

[4] Salanfe, Setup your own private Proof-of-Authority Ethereum network with Geth, Hacker Noon, 2018. Available at: https://tinyurl.com/ y7g362kd.

[5] Geth.ethereum.org. (2018). Go Ethereum. Available at: https://geth. ethereum.org/

[6] Vitalik Buterin. (2015). Ethereum White Paper Available at: https: //github.com/ethereum/wiki/wiki/White-Paper.

[7] Ethdocs.org. (2018). What is Ethereum? — Ethereum Homestead 0.1 documentation. [online] Available at: http://ethdocs.org/en/latest/ introduction/what-is-ethereum.html

[8] Agora (2017). Agora: Bringing our voting systems into the 21st century Available at: https://agora.vote/Agora_Whitepaper_v0.1.pdf

[9] Patrick McCorry, Siamak F. Shahandashti and Feng Hao. (2017). A Smart Contract for Boardroom Voting with Maximum Voter Privacy Available at: https://eprint.iacr.org/2017/110.pdf.

[10] Jonathan Alexander, Steven Landers and Ben Howerton (2018). Netvote: A Decentralized Voting Network Available at: https://netvote. io/wp-content/uploads/2018/02/Netvote-White-Paper-v7.pdf

[11] Jelurida, "Jelurida", 2017. Available at: https://www.jelurida.com/sites/ default/files/JeluridaWhitepaper.pdf

[12] Sos.ca.gov. (2007). Top-to-Bottom Review | California Secretary of State. Available at: http://www.sos.ca.gov/elections/voting-systems/oversight/ top-bottom-review/. [12] D. Chaum, P. Y. A. Ryan, and S. Schneider, "A practical voter-verifiable election scheme," in Proc. Eur. Symp. Res. Comput. Secur., 2005, pp. 118–139.

[13] S. Popoveniuc and B. Hosp, "An introduction to PunchScan," in Towards Trustworthy Elections, vol. 6000, New York, NY, USA: Springer, 2010, pp. 242–259.

[14] K. Gjøsteen, "The Norwegian internet voting protocol," in Proc. Int. Conf. E-Voting Identity, 2011, pp. 1–18.

[15] B. Adida, "Helios: Web-based open-audit voting," in Proc. USENIX Secur. Symp., 2008, vol. 17, pp. 335–348.

[16] E. Hubbers, B. Jacobs, and W. Pieters, "RIES-internet voting in action," in Proc. 29th Annu. Int. Comput. Softw. Appl. Conf., 2005, vol. 1, pp. 417–424.

[17] D. Chaum et al., "Scantegrity II: End-to-end verifiability for optical scan election systems using invisible ink confirmation codes," in Proc. USENIX/ACCURATE Electron. Voting Workshop, 2008, vol. 8, pp. 1–13.

[18] N. Chondros et al., "D-DEMOS: A distributed, end-to-end verifiable, internet voting system," in Proc. IEEE 36th Int. Conf. Distrib. Comput. Syst., 2016, pp. 711–720.

[19] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," SIAM J. Comput., vol. 38, no. 1, pp. 97–139, 2008.

[20] A. Boldyreva, "Threshold signatures, multisignatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme," in Proc. Int. Workshop Public Key Cryptography, 2003, pp. 31–46.

[21] J. C. Choon and J. H. Cheon, "An identity-based signature from gap DiffieHellman groups," in Proc. Int. Workshop Public Key Cryptography, 2003, pp. 18–30.

[22] M. Kumar and S. Chand, "ESKI-IBE: Efficient and secure key issuing identity-based encryption with cloud privacy centers," Multimed. Tool Appl., vol. 78, pp. 19753–19786, 2019.

[23] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," in Proc. Int. Conf. Theory Appl. Cryptology Inf. Secur., 2001, pp. 514–532.

[24] F. Zagórski, R. T. Carback, D. Chaum, J. Clark, A. Essex, and P. L. Vora, "Remotegrity: Design and use of an end-to-end verifiable remote voting system," in Proc. Int. Conf. Appl. Cryptography Netw. Secur., 2013, pp. 441–457.
[25] V. Cortier and B. Smyth, "Attacking and fixing Helios: An analysis of ballot secrecy," J. Comput. Secur., vol. 21, no. 1, pp. 89–148, 2013.
[26] R. Joaquim, P. Ferreira, and C. Ribeiro, "EVIV: An end-to-end verifiable Internet voting system," Comput Secur., vol. 32, pp. 170–191, 2013.
[27] B. Yu et al., "Platform-independent secure blockchain-based voting system," in Proc. Int. Conf. Inf. Security, 2018, pp. 369–386.
[28] X. Yang, X. Yi, S. Nepal, and F. Han, "Decentralized voting: A self-tallying voting system using a smart contract on the Ethereum blockchain," in Proc. Int. Conf. Web Inf. Syst. Eng., 2018, pp. 18–35.
[29] J. Li, X. Wang, Z. Huang, L. Wang, and Y. Xiang, "Multi-level multi-secret sharing scheme for decentralized e-voting in
cloud computing," J. Parallel Distrib. Comput., vol. 130, pp. 91–97, 2019.
[30] S. Dzieduszycka-Suinat et al., "The future of voting: End-to-end verifiable internet voting-specification and feasibility study," US Vote Found., Arlington, VA, USA, 2015. [31] D. A. Gritzalis, "Principles and requirements for a secure e-voting system," Comput. Secur., vol. 21, no. 6, pp. 539–556, 2002.
[32] M. Kumar, C. P. Katti, and P. C. Saxena, "An untraceable identitybased blind signature scheme without pairing for E-cash payment system," in Proc. Int. Conf. Ubiquitous Commun. Netw. Comput., 2017, pp. 67–78.
[33] B. Lynn, "The Stanford pairing based crypto library," Privacy preservation scheme for multicast communications in smart buildings of the smart grid vol. 324, 2013.
[34] Y.-F. Chung and Z.-Y. Wu, "Approach to designing bribery-free and coercion-free electronic voting scheme," J. Syst. Softw., vol. 82, no. 12, pp. 2081–2090, 2009. '
[35] C.-T. Li, M.-S. Hwang, and Y.-C. Lai, "A verifiable electronic voting scheme over the internet," in Proc. 6th Int. Conf. Inf. Technol., New Gener., 2009, pp. 449–454.
[36] Z.-Y. Wu, J.-C. Wu, S.-C. Lin, and C. Wang, "An electronic voting mechanism for fighting bribery and coercion," J. Netw. Comput. Appl., vol. 40, pp. 139–150, 2014.

AUTHORS

KEVIN GABRIEL HOULDER pursuing BTech Information Technology in Srm Valliammai Engineering College ,Tamil Nadu,India. His research interests focus on AES and Triple Des, electronic voting and information security

NITHISHWAR P,pursuing BTech Information Technology in Srm Valliammai Engineering College Tamil Nadu,India. His present research interests include attribute-based cryptography, cloud computing, and symmetric algorithm

SANTHOSH G, pursuing BTech Information Technology in Srm Valliammai Engineering College Tamil Nadu,India. His research interests include security and privacy in Internet of Thing.

VENKATESH E, pursuing BTech Information Technology in Srm Valliammai Engineering College Tamil Nadu,India. His present research interests include Triple DES, user authentication and information security