International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

Evaluating the Security Impact of Face Recognition and IoT-Enabled Blockchain on Electronic Voting Machines

[1]ESLAVATH NIKHIL,[2]SARAMPELLI RAVIVARMA,[3]GURADI HARIKA,[4]GALUGU SASIDHAR,[5]Mrs. A.Lakshmi Devi,

[1,2,3,4] Student,Department of EEE,Narsimha Reddy Engineering College,Misammaguda(V), Kompally-500100, Telangana State,India.

[5]Professor,Department of EEE,Narsimha Reddy Engineering College,Misammaguda(V), Kompally-500100, Telangana State,India.

Abstract—

Persistent privacy and security concerns have hindered the broad use and success of electronic voting. Enhancing the security of voting transactions and the validity of voter data, this study provides a strong architecture that blends sophisticated hashing and encryption methods with blockchain technology. False votes and EVM manipulation are two election problems plaguing India, the biggest democracy in the world. A biometric voting system that uses fingerprint authentication to confirm a voter's identity is proposed as a solution to these problems. Following the idea of "Single voter, Single authenticated vote," this approach guarantees that every voter casts a single authenticated vote. The Unique Identification Authority of India (UIDAI) may assist with the maintenance of the proposed biometric voting machine prototype and its interface with the Aadhar database. This development has the potential to greatly improve the device's suitability for use in national elections, opening up new possibilities for its implementation. Improvements in efficiency, security, and transparency were realized via the use of blockchain technology with this biometric voting method. Integrity, transparency, security, and efficiency in the election process are all bolstered by the suggested structure.

Keywords— Electronic Voting Machine (EVM), Secure Voting, Internet of Things (IoT), Ethereum-based Blockchain, Unique Identification Authority of India (UIDAI). I.

INTRODUCTION

The purpose of institutions like the "Election Commission" in parliamentary democracies is to make voting more trustworthy. It is the responsibility of these bodies to draft the laws and regulations that will allow for the holding of elections. They create strong voting systems, outline voting districts, and plan thorough election procedures. Making ensuring elections are open, free, and fair is the main goal, since it will increase people's faith in democracy. Since the inception of voting systems, the concept of secret voting has had significant importance. It is critical to maintain and strengthen public faith in voting [1, 2] in light of the growing confidence in democratic institutions. The voting process has been corrupted on several occasions in recent history. Problems like unfairness and lack of openness have surfaced, as has the fact that governments have not been formed in a way that reflects the true will of the people. A number of countries have voiced serious concerns over these issues; they include Brazil, Bangladesh, Pakistan, India, and Nigeria. Although these problems are multi-faceted and present many administrative, logistical, and technological challenges, blockchain technology has recently emerged as a game-changing tool for updating

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

voting systems [3]. Its distributed, unchangeable, and publicly available ledger is one of its defining characteristics; these three things also make it well-suited to election procedures: I. Permanentness A secure blockchain is updated with each new block, which is linked to the preceding block, forming an immutable chain of data.

Once data is saved on the blockchain, this feature ensures that it cannot be altered or tampered with. For fair and transparent elections, the immutability of blockchain technology is crucial [5, 6]. B. Achievability The blockchain ledger is decentralized because it is spread and duplicated across many different places. By removing a potential weak link, this redundancy makes the system more resilient and ensures that all of its resources are always available. Furthermore, third-party verification is possible because to the ledger's public accessibility. Voters are given more confidence in the voting process and more transparency when all nodes in the blockchain network work together to establish a consensus version of the ledger. Section C: Spreading the Vote A distributed consensus mechanism is what makes blockchain work; it chooses which node gets to contribute the next block of transactions. A new transaction can't be added to the network unless at least 51% of the active nodes agree that it's genuine. The integrity and safety of the election data are preserved by use of this kind of consensus mechanism, which blocks illegal entries and records only legal transactions. Blockchain is able to accomplish these features by use of complex cryptographic algorithms, which provide an extremely high degree of security compared to more conventional methods of recording information. Because of these characteristics, many experts believe that blockchain technology might be a powerful tool in creating a modern, secure, and transparent voting process. To abolish traditional election processes and increase public trust in democratic institutions, the authors advocate for blockchain-based voting systems [7], [8], [9].

LITURATURE REVIEW

The authors Zeeshan A. S. et al. [12] offer an FPGA-based live-face authorization system for electronic voting. In order to improve the overall security of electronic voting systems, the authors stress the need of strong face recognition. Integrating FPGA technology to strengthen electronic voting security is the main emphasis of the suggested technique. The author was successful in improving the accuracy of facial recognition. To increase the security of electronic voting machines, it was necessary to integrate FPGA technology into its real-time processing capabilities, which presented difficulties due to hardware complexity and possible scalability issues. The use of blockchain technology for a decentralized online voting mechanism is the primary emphasis of Lalitha V. et al. [13]. Decentralization and immutability are two of blockchain's most appealing qualities, since they promote openness and honesty. The technique incorporates blockchain technology to enhance the security and transparency of the voting process. Contributions to the use of blockchain technology in online voting have positive effects, such as increased transparency and security. In their pursuit of perfection, the authors encountered obstacles including scalability and network problems.

A Raspberry Pi-powered electronic voting kiosk with multi-mode authentication is proposed by M. G. Gurubasavanna et al. [14]. With the aim of providing individuals with an easy and efficient voting experience, reliability and usability are given top priority here. To increase trustworthiness and accessibility, the suggested approach uses Raspberry Pi and multimodal authentication. One good thing that came out of contributing to using Raspberry Pi in electronic voting was how much easier and more reliable it is. In spite of all these improvements, the article does mention some possible drawbacks, such as a reliance on certain devices and problems with user adoption. The dependable use of Raspberry Pi technology, which stresses democratic openness, is suggested by Patchava V. et al. [15]. The use of Raspberry Pi as voting infrastructure is one of the key characteristics. A user-friendly and trustworthy voting system is envisioned in the paper via the use of a touch screen interface and the integration of Aadhar ID. Improved accessibility and dependability are some of the good outcomes, and contributions to affordable solutions via the use of Raspberry Pi are also noteworthy. Problems with scalability and

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

device dependence, however, could prevent broad use, as the authors warn. A VNC server-based EVM system is proposed by N. N. Nagamma et al. [16] with the goal of providing remote accessibility. One important aspect is the ability to securely access electronic voting machines (EVMs) remotely via the use of video conferencing server technology. To improve accessibility and security, the system incorporates a VNC server. The deployment of VNC servers has the ability to reduce costs while simultaneously improving accessibility and security. Despite praising the possible advantages, the writers discuss worries about the scalability and security of the network.

PROPOSED FRAMEWORK OF VOTING SYSTEM

An electronic voting machine (EVM) that incorporates blockchain technology was developed and implemented using the secured voting technique. The voting process is meticulously designed with three main components to ensure the security, integrity, and transparency of the election. Each of the three distinct phases—pre-voting, voting, and post-voting—contributes to the overall safety and credibility of the electoral process. Figure 1 shows the procedures involved in the voting process, and Figure 2 shows the total voting process. Below is an explanation of each phase's many stages.

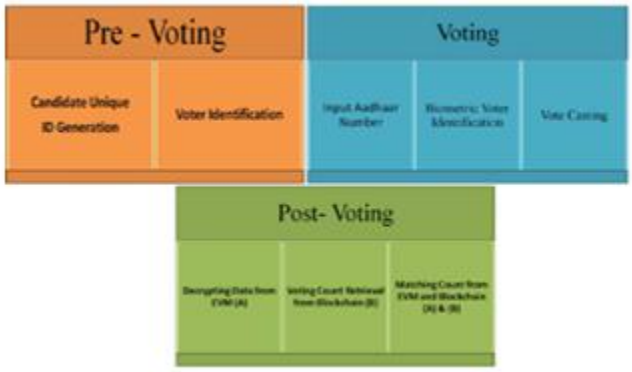

Fig. 1. Processes involved in complete voting system

Election Day A safe and open voting system can't be established without first completing the pre-voting portion of the election process. During this stage, we take numerous important precautions to guarantee that the information we get from candidates is genuine and unadulterated. 1) AES Algorithm for Standard Candidate Unique ID Generation a) Registering as a Candidate: It is essential for candidates to register with the Election Commission of India in order to take part in the election process. As part of this procedure, applicants must provide a number of pieces of identity and credentials for evaluation. For the purpose of checking candidates' legitimacy and making sure everyone is following the rules, the Election Commission looks over these papers very closely. b) Creating an Individual Encrypted Identifier: A applicant ID (CID) is created for every applicant when their papers have been successfully verified. To guarantee the privacy and security of candidates' information, this CID is created using an advanced algorithm that encrypts it using the Advanced Encryption Standard (AES). First Step: BEGIN Secondly, gather Candidate Cn's biometric picture, In Step 3: Locate the Face area in the image, Fn Fourth, calculate and encode (Fn)Hold on to SaltCn Step 5: Verify the Candidate's Aadhar Number, abbreviated as An Step 6: Get the Bn, or birth year, from the Aadhar database using the hash function concatenated with ACn.Seventh Step: Hn (BCN) + Salt (Cn)

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

Use AES encryption with (Hn + Private Key)Eighth Step: CIDs Nineth Step: Get CIDn Back Lastly, halt To start the identification process, the algorithm takes a picture of the candidate's biometric (In) features, which are like a digital fingerprint. This picture is the main input for the algorithm. Following this, the algorithm uses image processing methods to determine which part of the biometric picture corresponds to the face, referred to as (Fn). The program then encodes the detected face area and calculates and saves a salt value, SaltCn.

The salt value adds an extra degree of protection to the encryption process, guaranteeing that the produced Candidate ID (CID) is both unique and created at random. The next step is for the algorithm to get the candidate's Aadhar number (An) and birth year (YYYY) from the database. The creation of the one-of-a-kind encrypted ID relies heavily on these bits of data. By merging the Aadhar number and birth year with a hashing function, the method calculates a hash value, Hn, using the recovered Aadhar number and birth year in addition to the calculated salt value. While protecting the privacy and security of the data, this hash value encompasses all the necessary information for identifying candidates. At last, the technique uses the AES algorithm and a private key to encrypt the calculated hash value, Hn. Protecting the Candidate ID (CID) from prying eyes and accidental changes, this encryption procedure keeps it private and unchangeable. To provide a trustworthy and unchangeable record of candidate identities, the encrypted Candidate ID (CID) is thereafter safely saved in the database of the Election Commission. Ensuring the integrity and security of the candidate identification process, the private key used for encryption is kept secret until the results are announced. The Pre-Voting phase establishes a strong basis for the next phases of the voting process by using an all-inclusive technique for creating distinct encrypted IDs; this promotes honesty, openness, and faith in the electoral system. b) Protecting Individual Candidate IDs: To ensure that the encrypted Candidate IDs (CID) cannot be accessed or altered by unauthorized parties, they are maintained securely in the database of the Election Commission. The encryption process's private key is kept secret until the results are announced. Each Candidate ID is generated using the same private key, guaranteeing dependability and consistency in the identifying process.

This thorough procedure for registering candidates and creating unique IDs is implemented during the Pre-Voting phase. It lays a strong foundation for the next phases of the voting process and helps ensure the electoral system is secure and honest. The procedure for authenticating voters (a) Aadhaar Card The process of verifying a voter's eligibility includes comparing their voter IDs with their Aadhaar card numbers, which are encrypted using SHA in a one-way fashion. Protecting sensitive voter information from unwanted access or alteration is the goal of this encryption method. The local database of the EVM uses RSA encryption methods and strict access limits to safely store the encrypted Aadhaar numbers. b) Securely Storing Aadhaar Numbers: Ensuring the safety and privacy of voter data relies on the secure storage of Aadhaar numbers. To ensure the security of encrypted Aadhaar numbers, the EVM employs robust access restrictions and state-of-the-art encryption techniques to keep them locally in the database. The election system safeguards voter data from any security breaches by using strong encryption methods and executing stringent security procedures. Data security is an important part of maintaining the credibility and transparency of our democratic system, as it helps to safeguard voter information and inspire faith in the electoral process. c) LBPH Algorithm for Biometric Information Retrieval and Model Training: A vital part of voter authentication is retrieving biometric data from the UIDAI database. The LBPH method relies on this biometric to develop face recognition models that are essential for voter identification. To improve the safety and efficiency of the voting process, the LBPH algorithm analyzes patterns in biometric data to help in voter recognition. Ensuring frictionless voter access while protecting system integrity, the algorithm enhances recognition accuracy via repeated refinement during training. The electoral system improves the precision and dependability of voter identification by making use of cutting-edge machine learning methods, This boosts confidence in the voting process among the general population. d) Message Recipient's Anonymous Identity The Message of the Digest Algorithm Ensuring accurate identification while anonymizing voter identities is made possible by the digest algorithm. The technique ensures that important voter information is protected from any security breaches by creating unique message digests for each Aadhaar number, protecting voter privacy and confidentiality.

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

By promising voters that their information would be kept private and anonymous, this initiative boosts faith in the voting process. B. Voting In order to have a safe and smooth election, the following procedures must be followed throughout the voting phase. Step 1: Enter Aadhaar Number Before being compared with the current database, voters encrypt their Aadhaar card numbers. When it is found in the current database, biometric verification is started if the voter hasn't cast their ballot yet; otherwise, they are instantly excluded from voting. Identifying Voters Through Biometrics For more accurate face identification, voters may use an integrated camera to record their biometric information. Local Binary Pattern Histogram (LBPH) authentication is used to confirm the voter's identity. 3) Casting votes and adding them to the blockchain To guarantee that only verified voters may cast their votes in a safe environment, the process for activating the electronic voting machine (EVM) is conditional on successful authentication. Using a method similar to a blockchain, the EVM records and stores vote transactions. It employs encryption to provide secrecy and uses a special storage technique, which is detailed below, to make it impossible to modify any transaction. To further ensure the security of voting transaction data, it is further kept on a blockchain that is built on the Ethereum platform. In order to record vote transactions and transmit transaction data to other modules that keep copies of transactions in the Ethereum-based blockchain, the following Secure Chain Based Voting algorithm operates under an EVM machine.

Step 1: START

Step 2: EVM Machine initiate

Step 3: Repeat Step 4 to Step 10 for each voters in particular booth area

Step 4: IF Voter- NOT authenticated based Biometric verification:

Step 5: THEN: Wait for Authentication

Step 6: ELSE: Activate EVM machine for accepting vote

Step 7: LET Voter-N cast their vote to Candidate-P, denoted by Vn-Cp

Step 8: LET Tnp =Time-Stamp at which transaction Vn-Cp is occurred

Step 9: LET HN-1= Previous transaction Hash

Step 10: HN = Compute HASH (Vn-Cp, Tnp, HN-1)

Step 11: En-p = Encrypt (Vn-Cp)

Step 12: Store in EVM database (En-p, HN)

Step 13: Send Transaction Vn-Cp to Blockchain

Step 14: PRINT "Vote given to candidate-P"

Step 15: STOP

Blockchain technology You may build a solid basis for your electronic voting system using Ganache for local server deployment, Solidity for coding, and Remix as the integrated development environment (IDE). The blockchain is built on Ethereum. Since smart contracts automate key steps in the voting process and guarantee transparency,

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

Ethereum is a good fit for this application. The abundance of information, tools, and community support available in Ethereum's mature ecosystem further simplifies the process of creating, testing, and deploying blockchain applications. Incorporating Ethereum's decentralized architecture into your voting system will mitigate the dangers of centralized control and significantly increase the difficulty of manipulating votes. To submit the vote tally of verified voters to the Ethereum blockchain, see the Solidity code for the SubmitVote function in Figure 2 [10].

Fig. 2. SubmitVote solidity function C. Post-Voting (Result Calculation)

In order to accurately determine election results, the following stages are included in the post-voting phase. 1) EVM Data Decryption Here, the Electronic Voting Machine's (EVM) safe Chain Based Voting algorithm is used to decode the encrypted voting data, allowing for the safe extraction of candidate-wise vote tallies. Below is a thorough description of the method. a) Extracting Encrypted Data: The EVM securely stores the encrypted voting data, which is retrieved for decryption. b) RSA Decryption: The data is decrypted using the Rivest Shamir-Adleman (RSA) technique, which is well-known for its strong encryption and decryption capabilities. Only the election commission has the private key that can be used to decode the data. c) Vote Count Extraction: A key component of subsequent result computation is the extraction of individual candidate-wise vote counts from the encrypted data, which is done upon successful decryption. 2) Using Blockchain to Retrieve Vote Counts Here, we extract the voting tally from the blockchain, which guarantees the security of the result calculation process and the transparency of the vote transactions. Following is a detailed description of the process. Voting tallies saved safely in the blockchain's distributed ledger may be retrieved by establishing an access to the blockchain. By taking use of the cryptographic protections and inherent immutability of the blockchain, the obtained vote counts are double-checked to make sure they are accurate and complete.A more trustworthy and accountable election process is possible because to the blockchain's immutability, which makes vote tallies available to authorized parties. 3) The Count of Matches between EVM and Blockchain Critical verification occurs in the last stage of result computation, which is to compare the vote counts acquired from the EVM with those retrieved from the blockchain. The integrity of the whole election result is guaranteed by this painstaking comparison, which certifies the correctness and consistency of the vote data. Here is how everything happens.
Data Comparison: To make sure everything is in sync, we compare the vote tally from the encrypted EVM data with the one from the blockchain. The immutability of the blockchain ensures that the recorded vote tally is accurate, which allows for trustworthy comparisons. b) Confirmation of Authenticity: When the electronic voting machine (EVM) and the blockchain are able to match the vote tallies, it shows that the election results are genuine, which gives stakeholders and the public faith in the process. To build a strong voting system that can safeguard voters'

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

privacy and guarantee the accuracy of election results, this all-encompassing approach combines cryptographic methods, biometric identification, and blockchain technology.

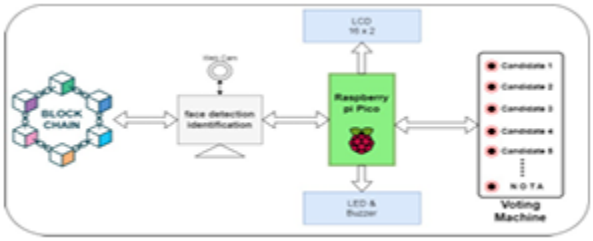

Fig. 3. Voating process block level representation

RESULTS AND DISCUSSION

Distributed Ledger Technology for Elections The following are the main criteria used to assess nine different voting systems that use blockchain technology: 1) Using Smart Contracts: Privacy in Transactions: Analyzes safeguards to prevent unauthorized access to voter records and to keep voters' identities secret throughout the voting process. Reviewing techniques to verify voter IDs is part of voter authentication, which aims to ensure that only eligible participants are able to cast ballots. 3) Hardware Security: Assesses the physical security, including tamper-proofing and encryption, of voting system hardware. 4) Tamper Resistance: Evaluates the system's ability to prevent manipulation or tampering in order to ensure the integrity of the election. Decentralization, which examines the system's control structure to lessen the need for centralized authority and increase openness and safety, is the fifth factor. 6) Efficiency: Weighs the advantages of the system, such as safety and availability, against the expenses of setting it up and keeping it running. Reviewing data encryption technologies, such as SHA-256 or AES-256, that are used to safeguard voter data and transactions, falls under the seventh category.

TABLE I. SECURITY PARAMETER ANALYSIS

Paper	A	B	C	D	E	F	G	H
1	Yes	High	Manual	High	Yes	Yes	Medium	SHA-256
2	Yes	High	Automatic	Medium	Yes	Yes	High	AES-256
3	Yes	High	Automatic	Low	Yes	Yes	Medium	RSA
4	Yes	High	Automatic	High	Yes	No	High	AES-

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

								256
5	No	Low	Manual	Medium	No	No	Low	-
6	Yes	High	Automatic	Medium	Yes	Yes	Medium	SHA-256
7	Yes	High	Automatic	High	No	Yes	High	AES-256
8	No	Low	Manual	Medium	No	Yes	Medium	SHA-256
9	Yes	High	Automatic	Medium	Yes	Yes	Medium	AES-256
Proposed System	Yes	High	Automatic	High	Yes	Yes	High	AES-256, SHA-256, Custom

A: Smart Contract Utilization, B: Transaction Privacy, C: Voter Authentication, D: Hardware Security, E: Tamper Resistance, F: Decentralization, G: Cost-effectiveness, H: Data Encryption Technique (Algorithm)

Assessment of Work Performance Using the Ganache blockchain server and Raspberry pi Pico hardware, the suggested solution for electronic voting machines (EVMs) was put into action and tested. After being built in the Remix IDE and delivered to the Ganache server, the smart contract controlling the voting process was thoroughly tested. We concentrated on critical performance indicators, such as gas consumption, cost analysis, and storage capacity for voting data, to assess the system's functioning and reliability. Because the computing resources needed to execute smart contract tasks are closely correlated with gas consumption, it is a significant statistic for measuring the performance of blockchain-based applications. We figured out how much gas was used by important processes in our suggested system: First Class for Votes Cast for Candidates The intricacy and cryptographic processes needed in voting for certain candidates caused the gas consumption to vary. We ran simulations of the voting process in several election situations to learn more about gas use. The gas usage for casting votes grew in a linear fashion with the number of votes cast, as we saw. The amount of gas used for every vote is shown in Figure 3. The system's capacity to keep gas costs in check and maintain a steady consumption pattern regardless of changes in voter participation is a testament to its scalability and its appropriateness for large-scale elections. In order to assess how well the proposed voting method worked, we looked at the gas consumption that came with deploying contracts to the Ganache server (Block 1) and conducting vote operations on the blockchain (Table 2 and Figure 3).

TABLE II. GAS CONSUMPTION ANALYSIS

Block	Action	Gas Used
Block 0	Genesis Block	0
Block 1	Contract Deployment	1,100,983
Block 2	Vote Transaction 1	67,056
Block 3	Vote Transaction 2	52,092
Block 4	Vote Transaction 3	52,056
Block 5	Vote Transaction 4	37,092
Block 6-11	Vote Transaction 5-10	40,634
Block 12- 21	Average (Vote Transaction 11 -20)	37,297
Block 22-31	Average (Vote Transaction 21 -30)	34,972

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

Results and Analysis 1) Deploying the Contract: The gas usage for deploying the contract is 1,100,983 units, which is the highest recorded (see table). Part Two. Because the contract code is performed during deployment, it is intended to be sophisticated and large in size. Gas usage for individual vote transactions ranges from 32,784 units at the lowest to 67,056 units at the greatest. Transactions may be conducted in a variety of states and situations, which explains the difference in gas use. 3) The Efficiency of the Suggested method: The suggested voting method demonstrates its efficiency by distributing gas usage reasonably across the various processes. As the number of votes rises, the gas consumption goes down a little, which means the system can manage more votes without using more resources. 4) System Comparison: The suggested technique shows reduced gas usage, especially during the vote transaction phase, in comparison to current blockchain-based voting systems. This effectiveness is due to the fact that the suggested system makes use of efficient algorithms and a secure storage mechanism. A graph showing gas usage for various blocks-wide activities is below:

Fig. 4. Gas Consumption Across Different Blocks

Vote transactions exhibit a somewhat constant gas consumption trend after the contract deployment phase, when the graph displays a rise. As the number of voters grows, the system's capacity to expand effectively depends on this stability.

CONCLUSION

In order to solve important problems with election procedures, this study introduces an Internet of Things (IoT) enabled electronic voting system that uses blockchain technology and sophisticated cryptography techniques. Our technology outperforms the current state of the art by guaranteeing efficiency, transparency, and security throughout the whole voting process. Widespread adoption is possible because to the suggested biometric identification and encryption systems, which increase voter confidence and decrease election fraud. With this development, we are taking a giant leap forward in protecting and enhancing democracy, which will ultimately lead to more trustworthy elections on all levels.

REFERENCES

[1]. O. Jaisinghani, P. Ramteke, “EVM Based and E- Voting System Using Block Chain Mechanism: A Review,” Science, Technology And Development Journal, vol. 10 I.8, pp. 127-132, Augest 2021.

[2]. O. Jaisinghani, P. Ramteke, B. Dhak "Ensuring Trustworthy Elections Using IoT-Enabled Blockchain EVM Voting Mechanism with Aadhaar Card- Based Face Verification," in: Dev, A., Sharma, A., Agrawal, S.S., Rani, R. (eds) Artificial Intelligence and Speech Technology. AIST 2023. Communications in Computer and Information Science, vol 2268. https://doi.org/10.1007/978-3-031-75167-7_10. Springer, Cham.

[3]. A. C. S. Sheela and R. G. Franklin, ''E-voting system using homomorphic encryption technique,'' J. Phys., Conf. Ser., vol. 1770, no. 1, Mar. 2021, Art. no. 012011.

[4]. A. M. Jagtap, V. Kesarkar and A. Supekar, "Electronic Voting System using Biometrics, Raspberry Pi and TFT module," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 10.1109/ICOEI.2019.8862671. 2019, pp. 977-982, doi:

[5]. M. Volkamer, O. Spycher, and E. Dubuis, "Measures to establish trust in Internet voting," in Proc. 5th Int. Conf. Theory Pract. Electron. Governance, 2011, pp. 1–6.

[6]. S. Chaudhary et al., "Blockchain-Based Secure Voting Mechanism Underlying 5G Network: A Smart Contract Approach," in IEEE Access, vol. 11, pp. 10.1109/ACCESS.2023.3297492. 76537-76550, 2023, doi:

[7]. K. Kapadiya, U. Patel, R. Gupta, M. D. Alshehri, S. Tanwar, G. Sharma, and P. N. Bokoro, ''Blockchain and AI-empowered healthcare insurance fraud detection: An analysis, architecture, and future prospects,'' IEEE Access, vol. 10, pp. 79606–79627, 2022.

[8]. A. Jangada, N. Dadlani, S. Raina, V. Sooraj, and A. R. Buchade, ''Decentralized voting system using blockchain,'' in Proc. IEEE Int. Conf. Blockchain Distrib. Syst. Secur. (ICBDS), Sep. 2022, pp. 1–5.

[9]. V. S, R. R, R. P, M. S. S, P. R and J. S, "IoT Based Secured Smart Voting System Using Diffie Hellman Algorithm," 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2023, pp. 48 53, doi: 10.1109/ICACCS57279.2023.10113082.

[10]. M. J. H. Faruk, M. Islam, F. Alam, H. Shahriar, and A. Rahman, ''Bie vote: A biometric identification enabled blockchain-based secure and transparent voting framework,'' in Proc. 4th Int. Conf. Blockchain Comput. Appl. (BCCA), Sep. 2022, pp. 253–258.

[11]. F. D. Giraldo, M. C. Barbosa, and C. E. Gamboa, ''Electronic voting using blockchain and smart contracts: Proof of concept,'' IEEE Latin Amer. Trans., vol. 18, no. 10, pp. 1743–1751, Oct. 2020.

[12]. Z. A. Soomro, T. Din Memon, F. Naz and A. Ali, "FPGA Based Real Time Face Authorization System for Electronic Voting System," 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, 2020, pp. 1 6, doi: 10.1109/iCoMET48670.2020.9073880.

[13]. V. Lalitha, S. Samundeswari, R. Roobinee and L. S. Swetha, "Decentralized Online Voting System using Blockchain," 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2022, pp. 1387-1391, doi: 10.1109/ICAAIC53929.2022.9792791.

[14]. M. G. Gurubasavanna, S. Ulla Shariff, R. Mamatha and N. Sathisha, "Multimode authentication based Electronic voting Kiosk using Raspberry Pi," 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on, Palladam, India, 2018, pp. 528-535, doi: 10.1109/I-SMAC.2018.8653726.

[15]. P. Vamsikrishna, S. D. Kumar, D. Bommisetty and A. Tyagi, "Raspberry Pi voting system, a reliable technology for transparency in democracy," 2016 IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT), Pune, India, 2016, 10.1109/ICAECCT.2016.7942629. pp. 443-449, doi:

[16]. N. N. Nagamma, T. Narmada, M. V. Lakshmaiah, V. Ramesh and G. Pakardin, "VNC server based EVM system," 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, India, 2017, pp. 802-805, doi: 10.1109/ICECDS.