International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

A Permissioned Blockchain-Based Secure Electronic Voting System Using AES Encryption, RSA Digital Signatures, and JWT Authentication

Mr.J. Sagar Babu [1], S.Lokeshwar Reddy[2], Ch.Srinithya[3], M.Sai Manikanta[4]

1Assistant Professor, Department of Computer Science and Machine Learning,
Methodist College of Engineering and Technology Abids, Hyderabad, Telangana, 500001, India.
2,3,4Student , Department of Artificial Intelligence and Data Science,
Methodist College of Engineering and Technology Abids, Hyderabad, Telangana, 500001, India.

Abstract – The growing use of digital technologies in recent years has made people want voting systems that are both safe and clear. Vote tampering, a lack of visibility in the process, and reliance on centralized control are all problems that come up with traditional voting methods. To get around these problems, this project comes up with a new electronic voting system called "VoteChain." The main idea behind VoteChain is to use blockchain technology to keep track of each vote as a block in a ledger that is spread out. This method makes it very hard to change or mess with the stored data, which makes people more confident in the voting process. We built the backend of the system with Node.js and Express, and we made a simple, easy-to-use interface for voters.To keep private information safe, each vote is encrypted with the AES algorithm, which makes sure that the data stays private. JSON Web Tokens (JWT) are used to verify users so that only people who are allowed to use the system can do so. It is designed in such a way that it can function on multiple nodes, and this helps make the system more decentralized and less controlled by a single source.The other important part of the system is the consensus mechanism. In order to ensure the data is valid, the block is validated by different nodes before being added to the blockchain.There is also the inclusion of the real-time results, and this helps the user clearly see the results of the election as the votes are being counted. This is an example of the importance and potential of using blockchain technology in the development of modern websites, as is evident in the creation of the electronic voting system.

Key Words: Blockchain, E-Voting, Cryptography, AES Encryption, JWT Authentication, Decentralization, Consensus Mechanism, Node.js

1. INTRODUCTION

Rapid technological advancements in digital technologies have led to major changes in traditional systems, including the electoral system.Electronic voting systems have emerged as an alternative to the traditional paper-based electoral system because they have the potential to provide faster results, ease the process, and reduce costs.Even though electronic voting systems have shown promise, the current state of electronic voting is faced with major challenges, including security threats, lack of transparency, data manipulation, and lack of public trust [1], [3]. Conventional centralized voting systems are at risk of various threats such as technical disruption, misuse of voting systems on the internet. Moreover, maintaining anonymity in voting while at the same time providing credibility and verifiability to the voting process is another major issueThe second important factor is the maintenance of anonymity while ensuring the verifiability and trustworthiness of the system. Although the problem has been addressed using various techniques, the solutions are found to be less efficient and reliable [11][14]. In this context, blockchain ways is being used more and more to fix the problems with current electronic systems. This technology is based on a network-based ledger system where recorded data can't be changed or deleted once it's been recorded. This keeps the system consistent and open [15], [24]. This makes sure that the votes recorded in the system are accurate by treating them as transactions in the system [4], [20]. Many systems based on blockchain technology have been proposed in recent studies to secure and make voting systems transparent. For instance, a electronic system based on a decentralized approach can be used for vote verification and counting through smart contracts, as proposed in [6], [20]. Further, voting systems based on blockchain way can be used for auditability, and hence voters and authorities can verify the voting results, providing trust in the voting system, as proposed in [9], [19]. In order to further improve the level of security in the system, advanced cryptographic techniques are used. These techniques include AES, RSA, and hybrid encryption. These techniques are used to ensure the confidentiality, authenticity of the data being used in the voting process [7], [10]. Hybrid techniques have also been found to offer better security and efficiency compared to other techniques [26]. Despite these advances, the use of blockchain electronic systems are used is faced with some challenges. Such difficulties include limited ability to cope with expansion, high computational demands, and latency, which are known to impact the efficiency of the systems, especially in larger elections [22][23]. Therefore, there is a need to create a better electronic system, which is more efficient and robust, incorporating blockchain way in addition to other sophisticated cryptographic techniques. The purpose of the research is to create a secure electronic system, which provides integrity, anonymity, transparency, and reliability in the data, while solving the performance issues in the e-voting system.

2. LITERATURE REVIEW

Another technology that has been extensively examined in recent years is blockchain technology, which has been considered a safe and decentralized technology in developing electronic voting systems. Indeed, voting systems currently in use have been facing several issues, including transparency and centralization in the voting process. As observed, many voting models have been proposed using blockchain way, ensuring data integrity and trust through decentralization.[1][3]. In addition to this, Kumar et al. [1] have also proposed an e-voting system based on blockchain technology using smart contracts, thus ensuring that the votes are secured and cannot be changed once they are stored. Kiayias et al. [2] have also proposed a complete protected voting system that enables voters to verify their votes while at the same time remaining anonymous. Liu et al. [3] have also proposed a decentralized voting system that does not require any polling authority. Some research works have been carried out towards the improvement of scalability in the blockchain way voting model. Research works [4], [5] proposed the practical implementation of the voting system using blockchain technology, which proved the usefulness of the voting system based on blockchain way. The proposed voting system using Hyperledger Fabric and Ethereum was proposed for better performance of the voting model by making use of the good technologies. Another important aspect of voting systems is privacy and security. Research works have been done on the aspect of voting systems using cryptographic protocols to make sure the anonymity of people along with the verifiability of the voting process. These works have been done in [9] and [12]. In addition to the above, researchers have also worked on the aspect of factors with regard to voting systems using blockchain technology. With regard to this aspect, researchers have worked on an efficient and scalable voting system using blockchain ways. These voting systems have been designed to handle a higher amount of transactions. With regard to the recent past, improvements have been made to lightweight blockchain technologies. Advanced forms of blockchain ways electronic systems have been proposed to enhance the security, privacy, and decentralization levels. The electronic voting system depends on the improvement of the security levels using advanced cryptographic techniques. The emergence of technologies, such as artificial intelligence, is being incorporated into the voting system, as proposed in [19]. From the above literature, it is clear that the blockchain technology, along with the use of cryptographic techniques, is an ideal platform to develop secure, transparent, and reliable electronic voting systems. However, some issues need to be addressed in the system, as in the case of VoteChain [20].

3. SYSTEM ARCHITECTURE

The permissioned system is a secure blockchain-based electronic voting system. This system will provide the necessary features for the protection the votes. The system will be composed of several functional modules, each of which will be used for a particular process during the voting system. The major function of the Authentication module, before allowing anyone into the system, is to authenticate the user. To access the system, a user will have to provide a valid voter ID and password. After authenticating the user, a JSON web token will be generated for a secure session. The voting module lets users who are logged in vote. The user can choose the candidate and vote after proving who they are. The Vochain will see if the user has already voted. Only users who meet the requirements can move on to the next step. This ensures the privacy and authenticity of the votes by using cryptographic techniques in the Encryption and Digital Signature Module.

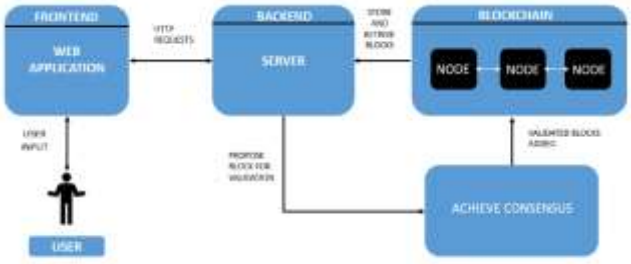

FIG-1 SYSTEM ARCHITECTURE

The Advanced Encryption Standard algorithm is used to encrypt the selected vote. This system make sures the security of the votes by keeping the data safe from being read while it is being stored or sent. In addition to that, a digital signature is created using the RSA algorithm. This algorithm validates the vote for authenticity. This watchouts that the vote comes from a valid source and has not been altered in any way. The blockchain module is responsible for storing votes safely in the form of blocks. The information in a block is stored as follows: it contains the encrypted vote, time stamp, previous hash, and current hash. The hash of a block contains information generated by a cryptographic hash function. This function is used to maintain the integrity of a block of information. The new block is linked to the previous block in such a way that a chain is formed. Once information is stored in a block in a blockchain, it cannot be altered in any way without affecting all other information in the chain. In Consensus Module,the system will make use of a simulated multi-node consensus mechanism for validating new blocks. When a new block is created, it will be sent to all remaining nodes for validation through communication using REST API. However, for a new block to be attached to the blockchain, it has to be approved by a highest count of nodes. The result processing module retrieves the encrypted votes from the blockchain using Advanced Encryption Standard to decrypt them. The results are then displayed in the form of a graph. This shows the results in a clear manner. This objective is achievable with the blockchain explorer module. The users can view the contents of the blockchain. The contents include the block index, time stamp, hash values, and the encrypted vote information. This helps in building trust among the users because they can view the information in the blockchain. The suggested system is using authentication, cryptography, blockchain, and consensus

mechanisms in such a way that it is secure, transparent, and functional.

4. IMPLEMENTATION

The proposed blockchain way electronic system is implemented through various web development and cryptographic techniques. The built voting web application is implemented in a modular fashion, where each module is implemented independently and then combined with other modules through various interfaces.
The Node.js platform was used for the development of the backend of the system. Express.js was used for handling the API requests and the logic of the system. HTML, CSS, and JavaScript were used for the interactive user interface on the frontend of the application. In order for the application to look like a multi-node blockchain network, the application was hosted on the local machine using more than one port.

JSON Web Tokens (JWT) are used for the verification of the identity of the users. After the users have logged in, their user ID and password are checked by the backend to confirm that they are correct. A token is generated and sent back after the validation is successful.
The voting functionality will be implemented by creating a protected API endpoint that will only allow users to vote after authentication. The API endpoint will then verify whether the user has already voted before accepting their vote. If the user is eligible to vote, then their vote will be accepted.The crypto module in Node.js is used for implementing cryptographic functions. The vote data will be encrypted using AES (Advanced Encryption Standard) with a predefined key for data confidentiality.The digital signature will be created using RSA, signing the encrypted vote data with a private key. The digital signature will then be verified using a public key for data authenticity and integrity.
The blockchain is implemented by using custom JavaScript classes, which define the structure of blocks and the chain itself. The blocks have attributes like index, timestamp, encrypted vote data, previous hash, and current hash. The hash is generated by a cryptographic hash function, which ensures that any change to the data will produce a different hash.
The blocks are then interlinked in the form of a hash reference, thus forming a chain of blocks, hence the term blockchain. A function is implemented for validating the integrity of the blockchain.
A simulated multi-node consensus mechanism has been implemented for validating the blocks before they are added to the blockchain. When a new block is created, it is sent to the peer nodes for validation using the REST API communication protocol. Each node will validate the block and send its approval/rejection. The block will be added to the blockchain if it is approved by a majority of the nodes. After validation, it will be broadcasted to all the nodes.
The encrypted vote information is retrieved from the blockchain. It is then decrypted using the AES algorithm. After decryption, the votes are counted for each candidate. The result is displayed on the frontend in the form of graphical charts, thus representing the result of the election.
Hence, in the above implementation, the features of authentication, cryptography, blockchain, and consensus have been used for developing an efficient voting system.

5. METHODOLOGY

The methodology used for the proposed blockchain technology-based e-voting system is based on an organized approach for the election process through the use of cryptography techniques. This proposed system is expected to provide authentication, confidentiality in the whole vote casting process.
The system will start with the initialization of the blockchain network, which will involve the creation of a genesis block with certain parameters in order to maintain consistency throughout the nodes in the network. Each node in the network will have the blockchain, and each node will be configured to interact with the other nodes in the network using REST-based API protocols. The system will be initialized with cryptographic keys in order to encrypt the data using AES or RSA algorithms.
The voting process begins with user authentication. Each user is required to enter a unique voter ID and password through the frontend interface. The backend will verify this information against the voter ID and password dataset. Once this is successful, a Jwt token is generated and sent to the backend. The JSON web token is used for session management and is required for accessing various voting processes. Any invalid authentication will be declined to prevent unauthorized access.
Upon authenticating, the voter chooses a candidate and votes. Before this vote is processed, the system checks to see if the voter has already voted in this election. This is to prevent duplicate voting. Once this is established, the vote is allowed and sent for cryptographic processing.

For confidentiality purposes, the chosen vote is encrypted using the AES encryption technique. AES encryption transforms the plain text vote into ciphertext, utilizing a predetermined encryption key and a randomly generated initialization vector. This way, even if the information is intercepted, it will not be readable unless the decryption key is available.
After this, a digital signature is created using the RSA technique, which signs the encrypted vote with a private key. This ensures that the vote comes from a legitimate source and has not been altered in any way. During the validation of the vote, the peer nodes will utilize the public key for signature verification. If signature identity fails, the vote will be not counted.
The encrypted vote and the digital signature are encapsulated in the block. The block consists of the essential attributes such as block index, timestamp, encrypted vote data, digital signature, previous block hash, and the current hash. The hash is created by using the hash function. The hash function is used in such a way that if there is any change in the block information, it will always generate a different hash value.
The newly created block has to be validated by the remaining nodes in the network. Each node in the network has to validate the block separately. The validation of the block is done by checking the block structure and the correctness of the hash and signature. This is a voting-based consensus algorithm. The block will be considered valid if it is approved by the highest of the nodes in the network. This way, no invalid data can be added to the blockchain.
After the consensus is obtained, the block is integrated into the blockchain. The updated blockchain is then sent to all the peer nodes in the network to maintain uniformity. The nodes in the network having the outdated blockchain are updated to the latest valid blockchain by the longest chain rule.

For the result generation, the system retrieves the encrypted votes from the blockchain and decrypts them using the AES algorithm. The decrypted votes are then aggregated and counted for each of the candidates. The final results are then presented in a graphical format.
During this process, a number of security features are implemented. These include authentication for preventing unauthorized access, encryption for confidentiality, and digital signatures for authenticity. In addition, the blockchain provides immutability. The consensus also helps to build trust by validating the data from multiple nodes. This provides a secure voting system. The methodology provides a smooth and secure system by integrating authentication, cryptography, blockchain, and consensus to produce a reliable electronic voting system.

6. RESULTS

The built blockchain way electronic voting system has been implemented, and its results are obtained in a simulated environment with multiple nodes. In this experiment, the proposed system has been executed with multiple instances of the code running on different ports to simulate an environment with multiple nodes participating in the system. The results obtained from this experiment show that the proposed blockchain-based e-voting system can perform all the functionalities with ease. The proposed system VIII. FUTURE SCOPE authenticates users with the help of JSON Web Tokens (JWT). The proposed system prevents users from voting twice through the voting status. The encrypted votes using AES provide confidentiality since the stored votes cannot be read in their original form. Moreover, the use of digital signatures based on the RSA algorithm provides security for votes since they can be verified for authenticity. During the test, all signatures were verified successfully before accepting the block by other nodes. Integrity of the data in the blockchain was clear from the fact that all the blocks were connected to each other using cryptographic hash functions. Any attempts to modify the data in the blockchain were clear because of the differences in the hashes. The consensus mechanism was also tested by simulating the communication between the nodes. In this case, it was noted that the blocks were added to the blockchain after the majority had approved them. This ensured that any invalid data was not accepted in the system. The results module was able to retrieve the encrypted votes, decrypt the votes, and provide the correct count of votes for the candidates. The graphical representation of the results made the results module more usable and provided a clear representation of the results. With regard to its performance, the system showed its efficient response time for its system processes such as login, vote submission, and result retrieval. However, in the future, with an increase in the number of nodes in the system, communication overhead in the consensus process could be one area of concern for its performance. From the experimental result, it has been shown that the proposed system can be used as a safe system for electronic voting that can eliminate the limitations of the traditional system.

7. CONCLUSION

This paper explains about a safe and correct electronic voting purpose system based on the blockchain technology. This voting system was proposed to resolve the limitations encountered in the conventional voting system, which is mostly centralized. This voting system uses the decentralized attribute of the blockchain technology for maintain all the encryption factors. The system makes use of various cryptographic methods such as AES encryption and RSA signature. The AES encryption method provides security to the system. The inclusion of JSON Web Tokens in the system for authentication purposes increases the security of the system. The system prevents unauthorized use and duplication of votes. A simulated multi-node system with a consensus mechanism was included in the system for validating the data before adding it to the blockchain. The inclusion of this mechanism increases the level of trust in the system. The results show that the system is effective in its purpose, ensuring accurate results for the votes. The proposed system can be concluded to be effective for providing an efficient system for electronic voting. Despite the proposed system providing an efficient solution for an electronic voting system, it has its own disadvantages, such as scalability and communication delays for a multi node system. The proposed system can be enhanced to make it more efficient in terms of decentralized peer-to-peer communication. In conclusion, it can be said that the builtsystem has shown how blockchain and cryptography-based methods can be employed to design an efficient, secure, and transparent electronic voting system.

8. FUTURE SCOPE

The deployed blockchain way electronic voting system is secure and transparent. However, there are several potential improvements to the proposed system in the context of scalability and applicability. The built system can be improved by implementing a decentralized peer-to-peer network through the use of WebSockets rather than the proposed REST-based communication. These consensus algorithms can make the system stronger. The system can also be improved by the addition of a database such as MongoDB for the efficient storage of voter details. This will ensure the availability of the data even if the system restarts. For security reasons, the system can be provided with various forms of biometric security. Additionally, the system can be provided with various forms of cryptography, such as zero knowledge proofs, in order to increase the privacy of the voters. The user interface can be improved by creating mobile apps and adding dashboards for the real-time monitoring of the activities. Additionally, the system can be integrated with the national identity systems.

REFERENCES

1]. A. Solankar, "Secure E-Voting System Using Visual Cryptography & Blockchain Ledger," Turkish Journal of Computer and Mathematics Education, vol. 12, no. 1S, pp. 7 12, 2021. [2]. A. Alotaibi et al., "Preventing Phishing Attack on Voting System Using Visual Cryptography," Journal of Computer and Communications, vol. 10, no. 10, pp. 149–161, 2022. [3]. S. Priya, G. Srivastava, and S. Kumar, "Secured Electronic Voting Transactions Integrated with Blockchain," 2021. [4]. S. Tanwar et al., "Implementation of Blockchain-Based E-Voting System," Multimedia Tools and Applications, vol. 83, no. 1, pp. 1449–1480, 2024. [5]. C. Toma et al., "Secure and Anonymous Voting D-App with IoT Embedded Device Using Blockchain Technology," Electronics, vol. 11, no. 12, p. 1895, 2022. [6]. B. Ali et al., "An Efficient E-Voting Algorithm and DApp Using Blockchain Technology," MIJRD, vol. 1, no. 03, pp. 60–69, 2022. [7]. K. N. Rahman et al., "Highly Secured and Effective Management of App-Based Online Voting System Using RSA Encryption and Decryption," Heliyon, vol. 10, no. 3, 2024. [8]. E. Daraghmi et al., "Decentralizing Democracy: Secure and Transparent E-Voting Systems with Blockchain Technology," Future Internet, vol. 16, no. 11, p. 388, 2024. [9]. S. Gupta et al., "Improving the End-to-End Protection in E-Voting Using Blockchain-Based Mechanism," Concurrency and Computation: Practice and Experience, 2024. of [10]. R. K. Muhammed et al., "Automated Performance Analysis E-Services by AES-Based Hybrid Cryptosystems," Advances in Science, Technology and Engineering Systems Journal, vol. 9, no. 3, pp. 84–91, 2024. [11]. K.-L. Tsai et al., "Low-Power AES Data Encryption Architecture for LoRaWAN," IEEE Access, vol. 7, pp. 146348–146357, 2019. [12]. S. Ajish and K. Anil Kumar, "Secure Mobile Internet Voting System Using Biometric Authentication and Wavelet Based AES," Journal of Information Security and Applications, vol. 61, p. 102908, 2021. [13]. B. A. Oke et al., "Securing Electronic Voting System Using Cryptographic Technique," 2019. [14].O. S. Adewale et al., "Visual Semagram: An Enhanced Technique for Confidentiality in Electronic Voting," International Journal of Computer Network and Information Security, vol. 12, no. 4, pp. 51–59, 2020. [15]. S. Latif and T. Anees, "Blockchain-Based Decentralized Electronic Voting System," IJCSNS, vol. 19, no. 12, p. 165, 2019. [16]. K. G. Houlder et al., "Secure Verifiable Internet Voting System Using Identity-Based Encryption," 2019. [17]. S. Jayanti et al., "A Novel Cryptosystem Using RSA and Classical Cipher for Secure E-Voting," Journal of Theoretical and Applied Information Technology, vol. 101, no. 4, 2023. [18]. J. Bhatti et al., "Secure Electronic Voting Machine Using Biometric Authentication and Encryption," International Journal of Performability Engineering, vol. 15, no. 10, p. 2570, 2019. [19]. R. Taş and Tanrıöver, "A Manipulation Prevention Model for Blockchain-Based E-Voting Systems," Security and Communication Networks, 2021. [20]. J. Lyu et al., "A Secure Decentralized Trustless E-Voting System Based on Smart Contract," in IEEE TrustCom/BigDataSE, 2019, pp. 570–577. [21]. "Hybrid Architectures Used in the Protection of Large Healthcare Records Based on Cloud and Blockchain Integration: A Review," Computers, 2024. [22]. "A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems," Sensors, 2022. [23]. Darwish and El-Gendy, "A New Cryptographic Voting Verifiable Scheme Based on Bit Commitment and Blind Signature," International Journal of Swarm Intelligence, 2017. [24]. M. H. Berenjestanaki et al., "Blockchain-Based E Voting Systems: A Technology Review," Electronics, 2024. [25]. N. J. Laila and S. M., "Blockchain Based Electronic Voting System," IJSRSET, 2023. [26]. Vinayachandra and K. Prasad, "Blockchain Based Cryptographic Algorithm for Data Protection in Electronic Voting System," EAI Endorsed Transactions on IoT, 2025.