iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.53179

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Decentralized Voting System Using Blockchain

Atharva Raskar[1], Mayur Pansare[2], Vishal Chumbalkar[3], Tushar Kamble[4], Mrs. Manisha Desai[5]
[1, 2, 3, 4]*U.G. Student, Department of Computer Engineering, RMD Sinhgad School of Engineering, Maharashtra, India*
[5]*Project Guide, Department of Computer Engineer, RMD Sinhgad School of Engineering, Maharashtra, India*

Abstract: ***India is the world's huge democracy and has the greatest population. The necessity for more advanced technology is brought on by security flaws in the current voting system. Although there are difficulties in creating a safe electronic voting system, there are advantages such as ease and cost savings. There are problems that need to be solved, like user authentication and faulty equipment. In order to increase security and transparency, the suggested solution calls for building a secure voting system that makes use of blockchain technology. The dependability and integrity of the Indian election process would increase as a result of this, which would guarantee the users' legitimacy and safeguard against manipulation or fraud.***
Keywords**: *Blockchain, Data Security, Voting System, Voter ID, Vote.***

I. INTRODUCTION

Democracies rely heavily on voting, but younger generations in particular are becoming least active voters. E-voting has been suggested as a solution to this issue as a means of enticing more young people to vote. E-voting must satisfy a number of functional and security requirements, including transparency, correctness, auditability, data integrity, privacy, availability, and dispersed authority, in order to be successful. Many of these needs may be met by blockchain technology, which has recently gained popularity. A decentralised network of linked nodes called a blockchain stores every transaction in full detail on each node. Transactions are only accepted if the majority of nodes agree in order for it to operate without a central authority. Blockchain enables user anonymity and has the potential to increase e-voting's acceptability and dependability.

II. RELATED WORK

According to a research paper [1], a novel voting system that prioritizes security utilizes biometric technology based on RFID. The system incorporates a two-step verification process. Initially, an LPC 2148 chip embedded in an RFID tag holds essential verification information. In the second step, a fingerprint scanner is employed to verify the identity of the individual by cross-referencing it with the corresponding RFID tag. However, the system's expenses are considered high primarily due to the utilization of RFID technology.

In a different research proposal [3], a cutting-edge voting system is outlined, leveraging the advancements in fingerprint recognition technology. This innovative solution aims to revolutionize the voting process in India by enabling citizens to exercise their voting rights conveniently from any location within the country. By visiting the nearest voting booth, individuals can securely cast their votes, ensuring their representation in their respective residential constituencies. The primary objective is to establish a robust and secure biometric-based voting system that eliminates any apprehensions or obstacles, allowing voters to participate seamlessly in the democratic process.

A research paper [4] introduces a robust voting system designed to safeguard against unauthorized voting. The system employs biometric data for individual authentication and utilizes Aadhaar information to verify voter eligibility. To ensure a high level of security, the system heavily relies on fingerprint biometrics. By leveraging the fingerprint data stored in the Aadhaar database, the system establishes a reference point for voter authentication during the voting procedure. Through this innovative approach, the proposed system establishes a unique and reliable means of preventing unlawful voting occurrences.

In contrast, the existing electronic voting machines commonly utilized today [5] exhibit certain drawbacks, including the potential for a single individual to cast multiple votes and the automatic rejection of invalid votes. To overcome these limitations, an intelligent system has been innovated, incorporating fingerprint biometrics to effectively curb multiple voting occurrences. Moreover, this advanced system incorporates automated procedures for vote verification and validation, enhancing the overall efficiency of the voting process. By adopting these measures, the proposed system provides a straightforward solution to address the aforementioned limitations and optimize the integrity of the voting system.

A research paper [6] presents an innovative E-Voting protocol that centers around the RSA public key encryption cryptosystem. This protocol introduces a convenient and cost-effective approach, enabling voters to cast their votes effortlessly from their personal computers. The security of the system hinges on the implementation of the public key encryption protocol, renowned for its heightened reliability compared to traditional voting systems. The proposed protocol is anticipated to bolster voter trust in the system while ensuring precise and accurate vote counting.

In a different system outlined in a separate study [7], comprehensive security measures have been integrated to safeguard the transmission of votes from the client to the server, mitigating various types of potential attacks. These measures are designed to provide robust protection against both passive and active intruders, ensuring the integrity of the voting process. Notably, the system introduces an advanced approach to voter authentication, emphasizing the use of biometric data like thumb impressions or facial recognition instead of traditional usernames. By adopting this approach, the system significantly enhances security measures, fortifying the overall system against potential threats and unauthorized access.

In the context of voting systems, a research paper [8] introduces a novel concept of utilizing blockchain technology. However, due to its novelty and the criticality of voting in democratic processes, widespread acceptance of this blockchain-based voting system may require considerable time. Conversely, another model proposed in a separate study [9] is highly regarded for its exceptional security measures, making it particularly suitable for conducting large-scale elections. In this model, known as the NCVVS system, after casting a vote, the voter receives a confirmation email containing two important elements: the ballot fingerprint and the election fingerprint. These fingerprints are derived through the utilization of the SHA (256) hash function, ensuring the integrity and verifiability of the votes. By presenting this unique and secure approach, the NCVVS system establishes a promising framework for conducting major elections with utmost reliability and trustworthiness.

In another research paper [10], a solution is put forth that harnesses the power of blockchain technology to mitigate potential risks within the communication channel. By adopting a decentralized approach, the system effectively minimizes vulnerabilities and enhances security measures. Moreover, the proposed solution incorporates advanced techniques such as hashing and encryption to fortify the overall security framework. These measures ensure that sensitive information remains protected and inaccessible to unauthorized parties. Through the implementation of blockchain technology and robust security measures, the proposed system presents a unique and effective strategy for eliminating potential risks and bolstering the security of the communication channel.

Contrarily, a different approach outlined in a distinct paper [2] involves leveraging Aadhaar cards equipped with a QR code issued by UIDAI (Unique Identification Authority of India). This method entails conducting the voting process through an online platform, with the collected data securely stored on a dedicated server. To access the results, the administrator is required to authenticate themselves by providing a unique user ID and password. By adopting this approach, the system offers an alternative and efficient means of conducting elections while ensuring the security and confidentiality of the voting process. The administrator's authorized access enables them to view and analyze the results with ease and convenience.

The advent of blockchain technology [11] has opened up new possibilities for the development of innovative digital services. However, current research in this field primarily focuses on technical and legal aspects rather than fully capitalizing on this ground breaking concept to create advanced digital systems. In this particular paper, the author aims to leverage open source blockchain technology to present a design for a novel electronic voting system that can be employed in local or national elections. This blockchain-based system promises enhanced security, reliability, and anonymity, ultimately resulting in an increased participation of voters and fostering trust among the population in the electoral services. By proposing this innovative approach, the paper seeks to explore untapped potential and pave the way for transformative advancements in the realm of digital democracy.

Within the context of the article [12], a pioneering concept is put forth by the author—an autonomous and decentralized electronic voting protocol for a ranked-choice voting system known as Broad vote. This groundbreaking protocol operates without the need for a trusted entity or central authority to handle the vote tallying process. Instead, voters engage in open communication through a publicly accessible notice board, ensuring transparency and irrefutability. The protocol consists of two distinct rounds: during the first round, voters disclose their public keys, followed by the disclosure of their randomized ballots in the second round. Importantly, all voters provide Non-Interactive Zero-Knowledge (NIZK) proofs to validate their adherence to the protocol, while simultaneously safeguarding the confidentiality of their individual votes. At the conclusion of the election, anyone, including third-party observers, will be capable of independently calculating the vote count without relying on a central authority for tallying. This system encompasses robust security measures, guaranteeing the highest level of protection for each voter and instilling confidence in the security and privacy of the voting process.

In an article by Author [13], a functional, stage-independent, secure, and transparent democratic framework is proposed, capable of deployment on any blockchain platform that supports smart contract execution. The inherent transparency is provided by the underlying blockchain platform, while additional cryptographic techniques such as Paillier encryption, proof-of-data, and linkable ring signatures are employed to establish a robust security framework and protect user privacy independently from the security and privacy features of the blockchain platform. The proposed voting system's accuracy and resistance against tampering are thoroughly analyzed. Hyperledger Fabric is utilized as the platform for deploying the voting system, and a comprehensive mathematical analysis is conducted to assess the performance of the proposed distributed scheme. By presenting this innovative approach, the article offers a unique solution that combines the advantages of blockchain technology with advanced cryptographic techniques to ensure a secure and efficient voting process.

In an insightful study [14], the authors introduce a groundbreaking approach to internet voting utilizing Blockchain technology, referred to as the Open Vote Network. This protocol presents a decentralized and self-tallying system that prioritizes the utmost privacy for voters. Specifically tailored for boardroom elections, it is implemented as a smart contract on the Ethereum Blockchain. Distinguishing itself from previous Blockchain-based e-voting protocols, the Open Vote Network eliminates the need for a trusted authority to calculate the vote tally or safeguard the privacy of voters. Instead, the protocol operates in a self-tallying manner, granting each voter full control over the confidentiality of their individual vote. In fact, the only conceivable means of compromising a vote's privacy would involve a coordinated effort involving all other voters. This innovative system ensures a high level of privacy and security, paving the way for enhanced trust and integrity in the realm of internet voting.

The introduction of the Open Vote Network marks a remarkable progression in the realm of electronic voting, effectively tackling critical concerns surrounding vote manipulation and transparency. Through this innovative system, voters can place their trust in the safeguarding of their votes' security and the precise determination of election results.

Notably, political violence [15] during elections has been a persistent issue in Africa and other developing nations. However, the utilization of BEV (Blockchain-based Electronic Voting) in the electoral process brings forth numerous advantages. It ensures heightened levels of security and transparency, effectively minimizing the risk of electoral violence. Moreover, BEV holds the potential to deliver more accurate election results through meticulous mathematical computations.

A key advantage of BEV lies in its decentralized nature, eliminating the requirement for a central authority to oversee the voting process. Consequently, the costs associated with traditional voting methods witness a substantial reduction.

Additionally, BEV has the capacity to diminish expenses linked to paper-based elections while simultaneously augmenting voter participation. By capitalizing on the convenience and accessibility of digital technologies, BEV streamlines the voting process, making it more efficient and accessible to a broader spectrum of individuals.

In essence, the integration of BEV into electoral procedures possesses the transformative potential to redefine the voting landscape, enhancing its security, accuracy, and cost-effectiveness.

III. EXISTING APPROACH

Advancements in electronic voting systems have improved their efficiency, dependability, and security. The security of elections, however, can still be jeopardized by flaws in the current generation of computerized voting devices. Risks include those posed by system breakdowns, impersonation, hacking, and human mistake. Researchers and subject matter experts are developing creative answers to these problems.

These include of using blockchain technology for improved security, creating cryptographic protocols for the protection of privacy, and using cutting-edge statistical methods for precise vote counting. For electronic voting systems to be trustworthy and reliable, ongoing advances in this area are essential.

IV. PROPOSED APPROACH

With the use of a web interface and blockchain technology, we established a safe online voting platform called Smart E-voting. Before their vote is entered into the main database, voters must verify their identity with a high-security OTP and their Aadhar Card for security reasons.

Voters can verify that their votes have been cast for the right party or candidate, which is another element of the system. The method counts the votes instantly, saving a tonne of time and allowing the Indian Election Commissioner to make an announcement of the results right away. Overall, the Smart E-voting system we've suggested offers voters a safe, simple, and effective means to take part in the democratic process.

A. Flow Diagram

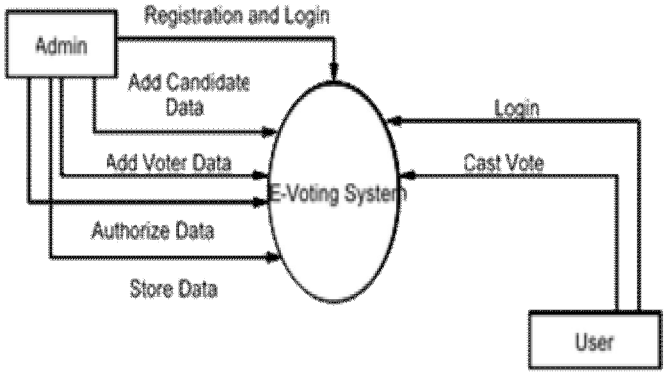


Fig.1: Block diagram of e-voting system

B. Algorithm

1) AES Algorithm for Encryption

The AES (Advanced Encryption Standard) algorithm is a symmetric algorithm used to convert plain text into cipher text for secure transmission or storage. It was developed to address the weaknesses of the DES (Data Encryption Standard) algorithm, which had a 56-bit key and 64-bit block size that were no longer secure against modern attacks. The AES algorithm uses a block size of 128 bits and keys of 128, 192, or 256 bits. It was developed by Joan Daemen and Vincent Rijmen, who called it Rijndael. To encrypt data using AES, the algorithm takes in a secret key and plain text input of the same bit size (e.g., 128-bit key and 128-bit input). The algorithm then processes the input through 10, 12, or 14 rounds, depending on the key and input size. Each round consists of four steps: substitution of the input bytes, shifting of the rows, mixing of the columns, and adding of the round key. The final round differs slightly from the previous rounds. The output of the AES algorithm is the cipher text, which is the encrypted version of the plain text input. The cipher text is also of the same size as the input, typically 128 bits for most modern applications.

Steps:

- Step1: Key Expansion: Expand the initial encryption key into a set of round keys.
- Step2: Initial Round: Add a first-round key to the input data.
- Step3: Rounds: Perform a series of substitution, permutation, and mixing operations on the data for a fixed number of rounds based on the key size.
- Step4: Final Round: Perform the final round of operations without the mixing step.
- Step5: Generate the encrypted output.

2) SHA 512

A hashing algorithm's main purpose is to ensure that it is almost impossible to find two different inputs that produce the same output, which is known as a collision. If a collision is detected, it can call into question the accuracy of the original message that was un-hashed. SHA-0 and SHA-1 have both been found to have several collisions, making them unsuitable for use in real-world scenarios. On the other hand, SHA-2 encryption has proven to be highly secure, with no collisions detected and no current technology capable of breaking it. However, given the development of quantum computers, it is possible that SHA-512 could have a security advantage in the future. It is more likely, though, that new, quantum-resistant algorithms will need to be developed to replace all SHA-2 algorithms to protect against potential collision attacks.

Steps:

- Step 1: Prepare the message by adding extra bits to make it a specific length.
- Step 2: Initialize the algorithm with predefined values.
- Step 3: Divide the message into blocks.
- Step 4: Generate a schedule of new values based on the blocks.
- Step 5: Mix and process the blocks using a series of operations.
- Step 6: Repeat the process for each block.
- Step 7: The output is the SHA-512 hash value, representing a unique and fixed-size representation of the original message.

C. System Architecture

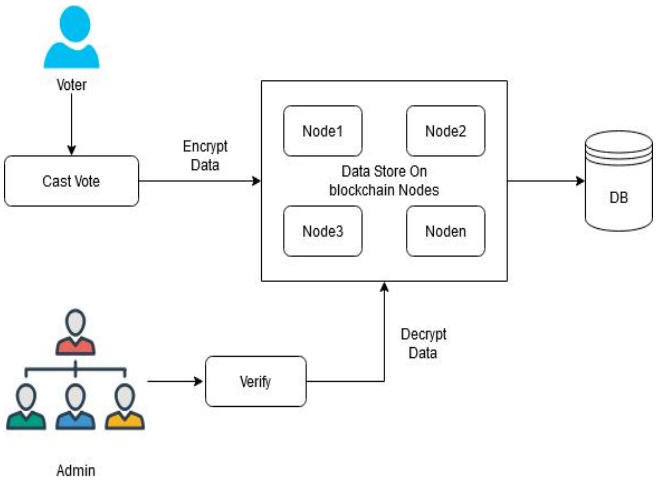


Fig 2: System architecture of e-voting system

V. IMPLEMENTATION

To achieve our goal of developing a decentralized voting system, we have designed and implemented a robust platform that leverages smart contracts to securely and transparently store and verify voters' data transactions. Our system has undergone extensive evaluation, taking into consideration key factors such as security, ease of use, and decentralization.

At the core of our decentralized voting system, we have created several classes to effectively manage and store users' identity, name, location, and other relevant information. These classes serve as the foundation for maintaining a reliable and organized user database within the system. Additionally, we have incorporated the use of one-time passwords (OTPs) to enhance security measures. These OTPs can be generated and sent to users via SMS or email using appropriate libraries, ensuring that only authorized individuals can access and participate in the voting process.

To guarantee the integrity and accuracy of the votes, we have implemented a thorough validation process. This includes verifying the correctness of the OTP entered by the voter, ensuring that only legitimate users can cast their votes. By employing such validations, we prevent any unauthorized or fraudulent attempts to manipulate the voting outcome. To ensure the confidentiality of the votes, we employ advanced encryption techniques. We utilize the AES (Advanced Encryption Standard) algorithm to encrypt the votes before they are added to the blockchain. This cryptographic process adds an additional layer of security, making it extremely difficult for any unauthorized parties to access or tamper with the votes. To calculate the cryptographic hashing value, we rely on the "MessageDigest" class available in the "java.security" package. This class enables us to perform secure hashing operations, maintaining the confidentiality and integrity of the votes as they are added to the blockchain. By utilizing cryptographic hashing, we can verify the integrity of the votes at any point in the future, providing assurance that no tampering has occurred.

In a decentralized voting system using blockchain, the SHA-512 (Secure Hash Algorithm 512) is employed to enhance the security and integrity of the data stored in the blockchain. SHA-512 is a widely used cryptographic hash function that generates a fixed-size hash value (512 bits) from any input data. Here are some ways in which SHA-512 can be utilized in a decentralized voting system:

Hashing User Data: When users register or provide their personal information, their data can be hashed using SHA-512 before being stored in the blockchain. This ensures that sensitive information such as names, addresses, and identification numbers are securely protected. The hashed values act as unique identifiers while maintaining the privacy of the original data.

Hashing Votes: Each vote cast by a user can be hashed using SHA-512 before adding it to the blockchain. This process ensures that the votes remain confidential and cannot be linked back to individual voters. The hashed votes are stored in the blockchain, making it practically impossible for anyone to determine the actual voting choices of specific individuals.

Verifying Data Integrity: SHA-512 can be used to verify the integrity of the data stored in the blockchain. By hashing the entire blockchain or specific blocks, one can generate hash values and compare them to previously stored hash values. If the generated hash matches the stored hash, it indicates that the data has not been tampered with, ensuring the integrity of the voting records.

Blockchain Consensus: In a decentralized voting system, multiple nodes or participants maintain a copy of the blockchain. These nodes can use SHA-512 to verify the consistency and validity of the blockchain. By comparing the hash values of the blockchain across different nodes, consensus can be reached to ensure the accuracy and reliability of the stored data.

It's important to note that SHA-512 alone may not provide complete security against all types of attacks. Additional security measures such as encryption, digital signatures, and access control mechanisms should be considered to build a comprehensive and secure decentralized voting system.

In terms of the frontend implementation, we have developed separate sections for the admin and the voters. The admin section provides the necessary tools and functionalities for managing the voting process, including user registration, vote tallying, and result generation. On the other hand, the voter section is designed to be user-friendly and intuitive, ensuring a seamless and easy-to-use experience for voters. The frontend sections have been implemented using HTML, CSS, and Bootstrap, allowing for a responsive and visually appealing user interface. These technologies enable us to create a consistent and well-designed interface that caters to the needs of both the administrators and the voters.

In the backend, we utilize Java to iterate through the blockchain, decrypt the votes, and calculate the final voting results. Java's versatility and robustness make it an ideal choice for processing and analysing the encrypted data stored in the blockchain. By leveraging Java, we can efficiently handle the computational tasks required to generate accurate and reliable voting results.

A smart contract is a self-executing digital contract with the terms of the agreement written directly into code on a blockchain. It automatically enforces the terms, verifies transactions, and facilitates interactions between parties without the need for intermediaries. Smart contracts provide transparency, security, and efficiency in various decentralized applications and eliminate the need for trust in traditional contract enforcement.

Smart contracts are used in blockchain-based voting systems for several reasons:

Transparency: Smart contracts provide transparency in the voting process. The code of the smart contract is visible to all participants, ensuring that the rules and procedures for voting are clear and cannot be altered without consensus. Security: Smart contracts utilize cryptographic techniques to secure the voting process. The immutability of the blockchain ensures that once a vote is recorded, it cannot be altered or tampered with.

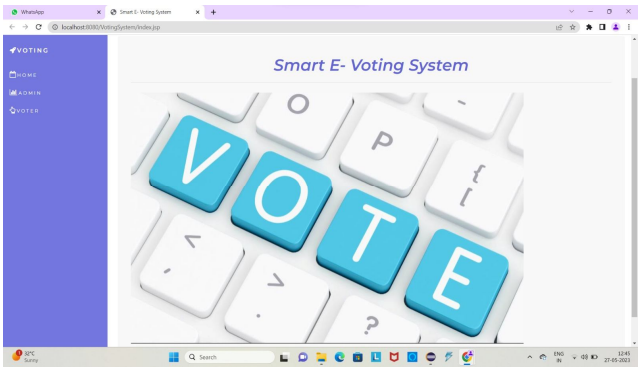
Decentralization: Blockchain-based voting systems leverage the decentralized nature of the technology. Smart contracts are executed on a network of nodes, eliminating the need for a centralized authority or trusted intermediaries. This decentralized approach ensures that no single entity has control over the voting process, making it more resistant to censorship and manipulation.

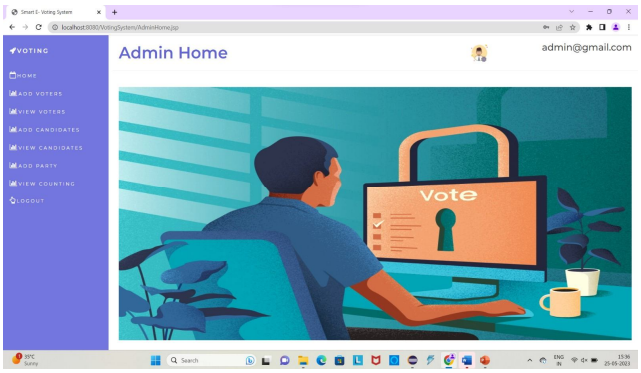
Trust and Auditability: By using smart contracts, the voting process becomes auditable and verifiable. Every vote recorded on the blockchain can be traced back to its source, providing a transparent and auditable trail of the entire voting process. This auditability helps in verifying the legitimacy of the results and resolving any disputes that may arise.

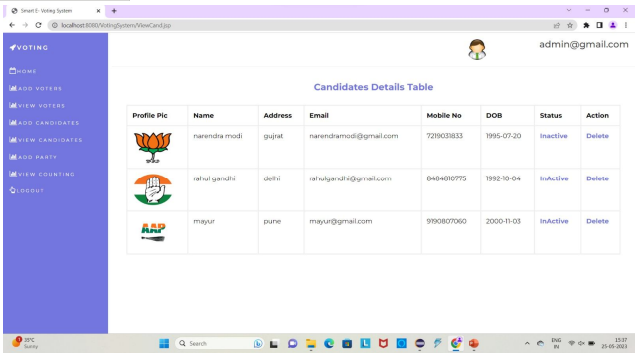
Our decentralized voting system combines smart contracts, advanced encryption techniques, and secure validation processes to create a secure and transparent platform.

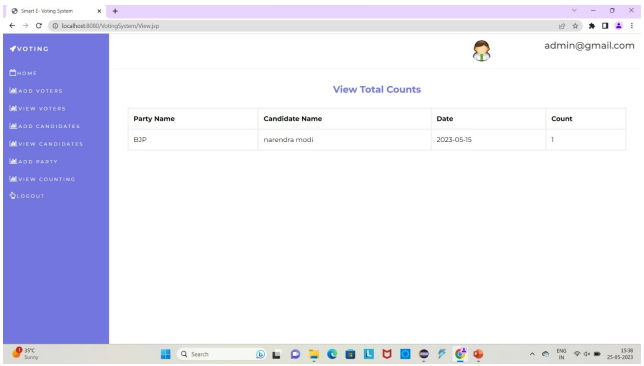
VI. RESULT

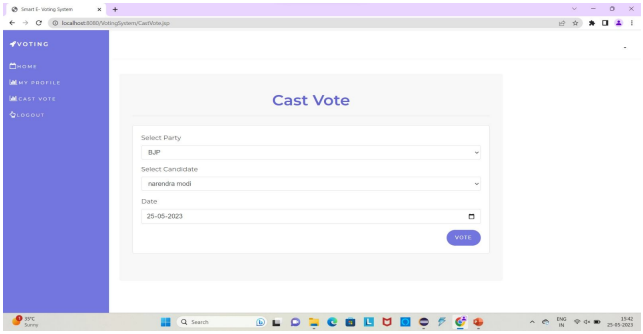
The system allows convenient participation in elections through digital devices, eliminating the need for physical polling stations. Utilizing blockchain technology ensures the immutability and integrity of votes, preventing any manipulation. The implementation has demonstrated real-time verification and accurate vote counting. Overall, it has showcased the potential of blockchain in revolutionizing elections and promoting democracy.

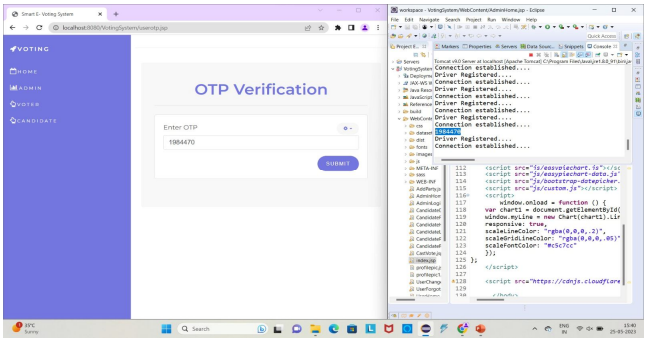












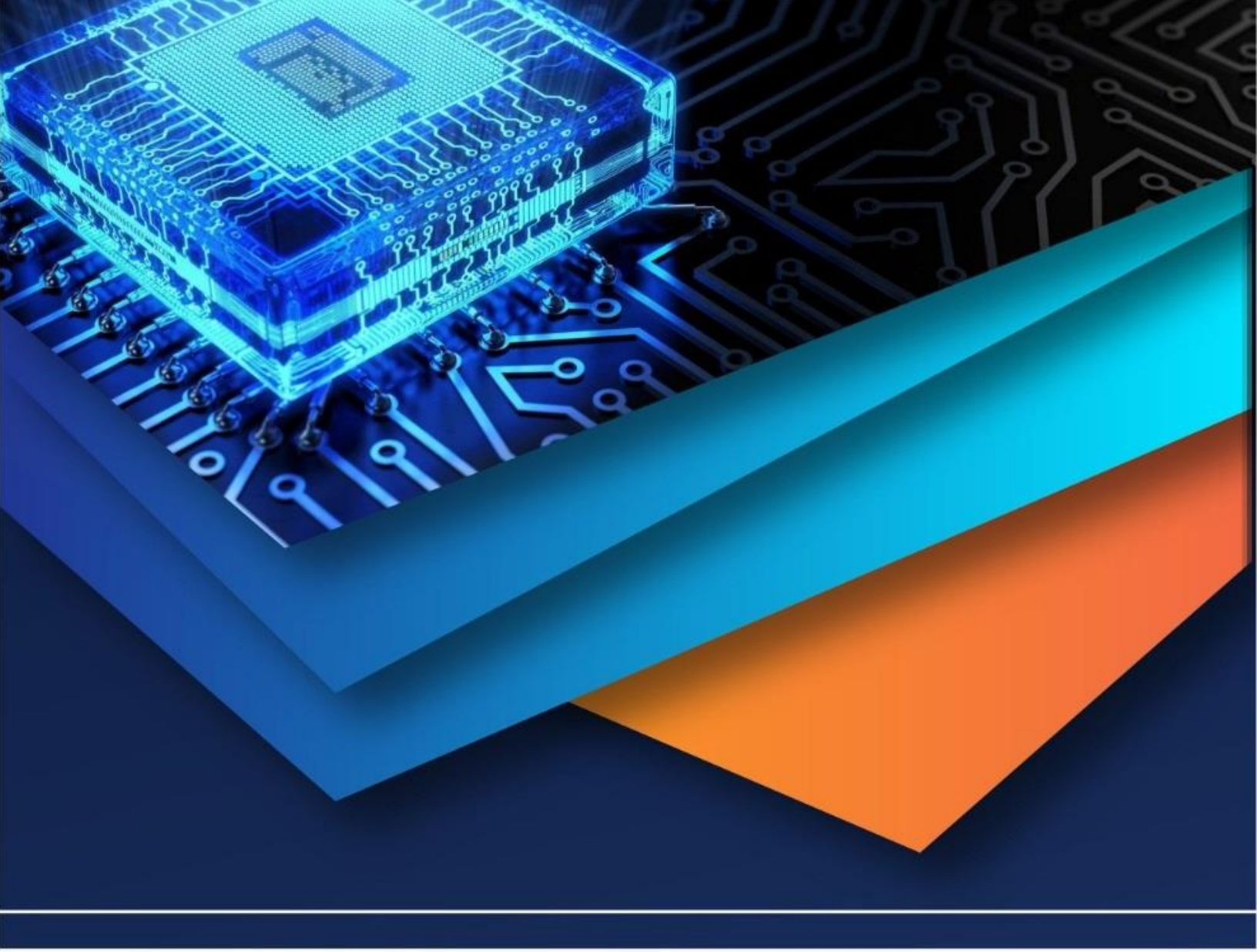
VII. CONCLUSION

Our decentralized voting system is a robust platform that utilizes smart contracts, advanced encryption techniques, and secure validation processes to create a secure, transparent, and user-friendly voting experience. By implementing classes to manage user data, employing one-time passwords, and leveraging AES encryption and SHA-512 hashing, we ensure the confidentiality, integrity, and accuracy of votes stored in the blockchain. With separate admin and voter sections designed with HTML, CSS, and Bootstrap, our system offers a visually appealing and intuitive interface. Using Java in the backend, we efficiently process and analyse encrypted data, generating reliable voting results. In summary, our decentralized voting system achieves the goal of secure and decentralized voting, providing a seamless experience for administrators and voters alike.

REFERENCES

[1] J.Deepika, S.Kalaiselvi, S.Mahalakshmi, S.Agnes Shifani, “Smart Electronic Voting System Based On Biometric Identification-Survey”, International Conference on Science Technology Engineering Management (ICONSTEM) March 2017.
[2] Ravindra Mishra, Shildarshi Bagde, Tushar Sukhdeve, J. Shelke, “Review on Aadhaar Based Voting System using Biometric Scanner”, International Research Journal of Engineering and Technology(IRJET), Feb 2018.
[3] Girish H S, Gowtham R, Harsha K N, Manjunatha B, “Smart Voting System”, International Research Journal of Engineering and Technology (IRJET) May 2019.
[4] K. Lakshmi, R. Karthikamani, N. Divya “Aadhar Card based smart e-voting system”, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 8958, Volume-8, Issue-2S, December 2018.
[5] G.Saranya, R.Mahalakshmi, J.Ramprabu, “Smart Electronic Voting Machine surveillance”, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 8958, Volume-8, Issue- 2S, December 2018.
[6] Ashish Singh, Kakali Chatterjee, SecEVS: Secure Electronic Voting System Using Blockchain Technology, International Conference on Computing, Power and Communication Technologies (GUCON) Galgotias University, Greater Noida, UP, India. Sep 28-29, 2018.
[7] Prof. Mrunal Pathak, Amol Suradkar, Ajinkya Kadam, Akansha Ghodeswar, Prashant Parde, "Blockchain Based E-Voting System", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 8 Issue 3, pp. 134-140, May-June 2021.
[8] Ritika Singh, Riya Chaudhary, Adarsh Tripathi, “Electronic Voting System Using Blockchain”, International Journal of Scientific Research in Engineering and Management (IJSREM), Volume: 05 Issue: 05 | May -2021
[9] Abhijit J. Patankar, Kotrappa Sirbi, Kshama V. Kulhalli, “Preservation of Privacy using Multidimensional K-Anonymity Method for Non-Relational Data”, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-2S10, September 2019.
[10] Ashraf Darwish and Maged M El-Gendy, A New Cryptographic Voting Verifiable Scheme for E-Voting System Based on Bit Commitment and Blind Signature, International Journal of Swarm Intelligence and Evolutionary Computation.
[11] A.B. Ayed, ”A conceptual secure blockchain-based electronic voting system,” Int. J. Netw. Secur., vol. 9, no. 3, pp. 01-09, May. 2017.
[12] S. Panja, S. Bag, F. Hao and B. Roy, “A Smart Contract System for Decentralized Borda Count Voting,” IEEE Trans. on Eng. Manag.,DOI: 10.1109/TEM.2020.2986371, 2020.

[13] Yu, J.K. Liu, A. Sakzad, S. Nepal, R. Steinfeld, P. Rimba, and M.H. Au, "Platform-Independent Secure Blockchain-Based Voting System," in ISC, Guildford, UK, Sept. 2018, pp. 369-386.
[14] P. McCorry, S.F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in FC, Sliema, Malta, Apr. 2017, pp. 357-375.
[15] N. Kshetri and J. Voas, "Blockchain-enabled e-voting," IEEE Softw., vol. 35, no. 4, pp. 95-99, Jul. 2018



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY