Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
June 2024 5(6), 1868–1878

BLOCKCHAIN-POWERED VOTING: ENHANCING SECURITY, TRANSPARENCY, AND ACCESSIBILITY IN DIGITAL DEMOCRACY

Ramya P. [1], Arun R. [2], Dhinesh M. [2], Kamaleeshwaran M.P. [2], Prasanth G. [2]

[1] Faculty, Department of Computer Science and Engineering, Mahendra Engineering College, Mallasamudram, Namakkal, Tamil Nadu, India
[2] Student, Department of Computer Science and Engineering, Mahendra Engineering College, Mallasamudram, Namakkal, Tamil Nadu, India

DOI
10.29121/shodhkosh.v5.i6.2024.2652

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

Election officials encounter a range of challenges during electoral processes, notably issues like inaccurate vote confirmation and instances of unauthorized voting. To tackle these challenges, we introduce a cutting-edge online voting system that enhances the efficiency and security of elections. This autonomous system employs a camera to capture the images of voters, which are subsequently stored in a secure database. Utilizing Blockchain technology and Convolutional Neural Networks (CNN), the captured images are analyzed to facilitate accurate voter identification. The CNN is trained on a diverse dataset of labeled images to ensure high prediction accuracy. Furthermore, our system integrates a dual-factor authentication approach, combining facial recognition with Email One-Time Password (OTP) verification to confirm the identities of voters. This innovative methodology aims to bolster the integrity and trustworthiness of online voting mechanisms, paving the way for a more transparent and inclusive digital democratic process.

Keywords: Online Voting, Blockchain, Convolutional Neural Networks, Facial Recognition, Digital Democracy

1. INTRODUCTION

Elections are essential to democratic governance, allowing citizens to voice their collective preferences and influence the future of their nations. However, traditional voting methods have long struggled with challenges such as fraud, inefficiencies, and barriers to accessibility, undermining the core principles of fairness and transparency. In this context, the advent of blockchain technology combined with deep learning algorithms offers a transformative opportunity to revolutionize the electoral landscape. A new era of digital democracy is emerging, promising enhanced security, transparency, and accessibility in the voting process through the secure data storage capabilities of blockchain and the advanced facial recognition algorithms based on Convolutional Neural Networks (CNN).

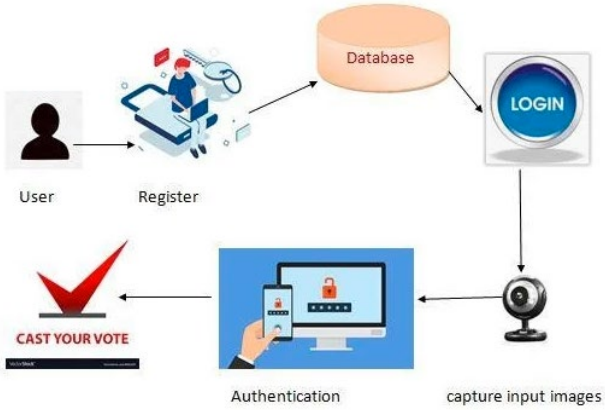

Figure 1. Introduction of E-Voting flow

This paper examines the development and implementation of a blockchain-based voting system fortified by CNN and facial recognition techniques to address existing issues and pave the way for a more robust and inclusive political framework. The primary objective is to present an innovative solution aimed at improving the accessibility, security, and transparency of online voting systems. The proposed approach integrates Convolutional Neural Networks, blockchain technology, and facial recognition to mitigate the limitations associated with conventional voting methods, including fraud, inefficiency, and limited access.The study aspires to reshape the electoral landscape by incorporating these advanced technologies, ensuring a more resilient, reliable, and inclusive democratic process. Additionally, this paper aims to advance research in digital democracy by providing an in-depth exploration of how blockchain-driven voting systems function and the application of deep learning algorithms for voter verification.To enhance the security and reliability of online voting systems, this research proposes a comprehensive strategy. First, blockchain technology is employed for secure data storage, safeguarding the integrity and confidentiality of voter information. This decentralized ledger approach minimizes the risks of tampering and unauthorized access, thus protecting the electoral process from fraudulent activities. Additionally, the study implements facial recognition technology, specifically utilizing Convolutional Neural Networks (CNN), to accurately verify voter identities. This method analyzes facial features and patterns, ensuring reliable identification of voters.Moreover, the system incorporates an additional layer of security through a secondary authentication process, in which voters receive an email containing a One-Time Password (OTP). By integrating blockchain, facial recognition, and OTP authentication, this system establishes a solid foundation for online voting that effectively addresses the challenges of accessibility, fraud, and transparency in digital democracies. The goal of this research is to contribute to the development of secure and inclusive voting systems by applying these cutting-edge concepts in practice.

1.1. DEEP LEARNING

Deep learning is a sophisticated branch of machine learning that has garnered significant attention for its capability to emulate the intricate neural networks found in the human brain. At its core, deep learning employs multi-layered neural networks to analyze vast amounts of data, uncovering subtle patterns and connections that traditional algorithms might overlook. This methodology has led to remarkable advancements across various fields, including image and speech recognition, natural language processing, and autonomous driving. The success of deep learning hinges on the use of advanced algorithms, such as Convolutional Neural Networks (CNNs), which excel in visual data interpretation, and Recurrent Neural Networks (RNNs), which are adept at handling sequential information. With its unparalleled ability to identify complex patterns and facilitate decision-making, deep learning has the potential to revolutionize research, technology, and numerous other sectors.

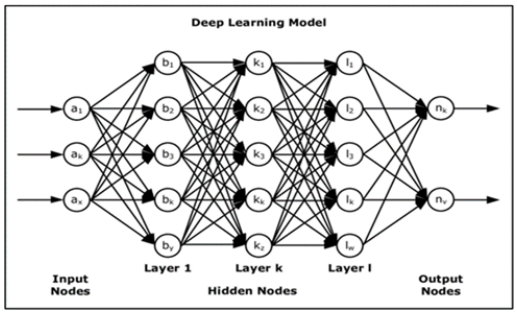

Figure 2: Deep Learning Model

As a subset of artificial intelligence, deep learning relies on the principle of training machines to learn from data representations, typically structured as neural networks inspired by human cognition. In the context of the proposed blockchain-based voting system, deep learning initiates with the aggregation of extensive facial image data from registered voters. These images serve as input for the Convolutional Neural Network (CNN), a specialized deep learning technique designed for image analysis.A CNN consists of convolutional layers for feature extraction, followed by pooling layers to reduce dimensionality. The subsequent layers are fully connected layers responsible for classification. During the training process, the CNN utilizes a method known as backpropagation to iteratively improve its ability to recognize patterns and features in the facial images. By adjusting the network's parameters based on the discrepancies between predicted and actual outcomes, the CNN minimizes errors. Once trained, the CNN can accurately identify and classify voters' faces, thereby streamlining the authentication process during voting.The integration of deep learning technology not only enhances the security and precision of voter verification but also ensures the overall integrity and reliability of the election system.

2. RELATED WORK

Sanskruti Dube; Mysore Venkata Siva Sandeep [1] This paper first proposes an online voting system for Indian elections. The voter's raised secure password must be verified before the vote is recorded in the large database that is owned by the Election Commission of our country, making the suggested model more secure. Voters can confirm that their vote was cast for the appropriate candidate or party thanks to the model's extra functionality. A voter may choose to cast their ballot from their preferred location or from a location other than the one assigned to them under this arrangement. The suggested method would allow for automatic vote counting, saving a substantial amount of time and enabling our country's Commission on Election.

Muhammad Asaad Cheema, Nouman Ashraf [2] Voting is an essential part of a country's political life cycle. Any evoting programme is expected to ensure the privacy, authentication, and integrity of citizens' votes and data. In order to address these problems, we offer a robust e-voting system based on blockchain and machine learning. We employ blockchain to assure vote integrity and security, and a machine learning algorithm to detect intrusions in voting data centres and e-voting stations. The proposed model employs the notions of personal and public blockchain. The personal blockchain is used to register and vote.

Y.Vijaya Lakshmi; V. Amrutha [3] The majority of people are mistaken to believe that casting paper votes is a thing of the past. These early paper votes seriously jeopardised voter secrecy, making voters easy prey for a range of election fraud techniques. Therefore, it is imperative to ensure that free and fair elections are used to choose the ruling body. The main goal of this research is to create a reliable and user-friendly online election platform. There is still an issue with voting in terms of security. The main component of this system is a web-based voting decision tool that utilises Gmail verification and facial recognition software. When using the "E-Voting System" described above, there are no obstacles to avoid.

D. Duong; B. Goertzel [4] This study presents the experimental findings of a comparison between SVM and a typical voting technique that aggregates four entity extractors each. We also outline our plans for incorporating agent-based technologies into our experimental testbed in the future, which will allow us to study the development of composite methodologies as a component of the analytic stream. We are evaluating the benefits of using cognitive agents that are deliberately incorporated into the data processing workflow, since a significant portion of the improvement stems from

fine-tuning the algorithms to the data stream with a human-in-the-loop. We imagine agents that learn the patterns in the data streams and adjust the algorithms accordingly to guarantee optimality as we refine them for improved performance on the streams.

Gayathri G S, Vimala Devi A [5] The goal is to provide a secure and user-friendly online voting system. The problem of voting remains essential in terms of safety and security. This system focuses on the design and implementation of a web-based voting system that uses face detection and an Aadhaar card to deliver excellent performance and security. The proposed Online Voting System allows voters to scan their faces, which are then matched to a previously saved image in a database and retrieved during voting. The voting system is administered in an easier manner, as all users must login using their Aadhaar card number and click on their preferred candidates to vote. By employing facial detection, it ensures adequate security and lowers dummy votes.

3. PROPOSEDMETHOD

The proposed system aims to revolutionize the electoral process by leveraging advanced technology to ensure integrity, security, and accessibility. At its core, the system is built on blockchain technology, which provides a secure and immutable ledger for storing voter information, particularly facial images. By integrating facial recognition algorithms with Convolutional Neural Networks (CNNs), the system facilitates efficient voter identification, guaranteeing that each individual can cast their vote only once. This layered approach not only minimizes the risk of voting fraud but also enhances transparency and accountability within the electoral framework.Moreover, the proposed solution offers voters an intuitive and user-friendly interface to engage in the electoral process. Upon successful validation, voters are presented with a list of parties and candidates, enabling them to express their preferences easily. The votes cast are securely recorded on a blockchain ledger, ensuring both transparency and immutability. Additionally, voting reports are generated and sent to stakeholders, providing opportunities for real-time monitoring and auditing of the electoral proceedings.This innovative system establishes a robust foundation for conducting fair, secure, and accessible elections through the use of facial recognition, One-Time Password (OTP) verification, and blockchain technology, ultimately fostering trust and confidence in the democratic process.

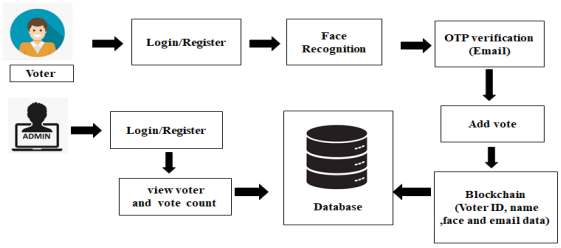

Figure 3. System architecture

Convolutional Neural Networks (CNNs)

consist of a series of layers designed to extract features from input data and generate predictions. The process begins with convolutional layers that apply filters to input images, enabling the detection of patterns and features such as edges and textures. Following these convolutional layers, activation functions like ReLU (Rectified Linear Unit) are utilized to introduce nonlinearity into the network, facilitating the capture of complex relationships within the data.To optimize performance, pooling layers are incorporated to reduce the dimensionality of the feature maps. This step retains essential information while lowering computational requirements.

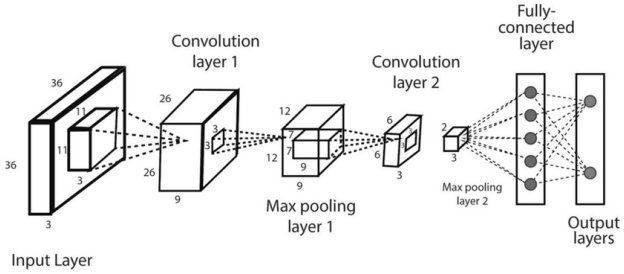

Figure 4. CNNs Model

After several rounds of convolution and pooling, the resulting flattened output is directed to fully connected layers, which are responsible for learning intricate patterns and relationships among features to carry out classification tasks.Ultimately, the output layer generates predictions based on the features learned throughout the network, enabling the CNN to categorize incoming data into various classes. Due to their systematic approach to feature extraction and classification, CNNs are particularly effective in applications such as image recognition, object detection, and facial recognition, making them vital tools across a wide range of machine learning fields.

Blockchain: Blockchain technology, widely acknowledged as a revolutionary advancement, fundamentally changes the ways in which data is stored, validated, and exchanged in digital environments. At its core, blockchain is a decentralized and distributed ledger system that securely and permanently records transactions across a network of computers. Each transaction is cryptographically linked to its predecessor, forming a continuous chain of blocks, which is how the term "blockchain" originated. This technology removes the necessity for intermediaries, such as banks or governmental entities, as transactions are validated by participants within the network.The applications of blockchain extend far beyond cryptocurrency, encompassing areas such as supply chain management, voting systems, and smart contracts, all of which benefit from its inherent transparency, security, and integrity. Overall, blockchain technology has the potential to revolutionize various sectors by fostering decentralization, enhancing efficiency, and building trust in the digital landscape.

Figure 5. Block chain

3.1. WORKING PROCESS

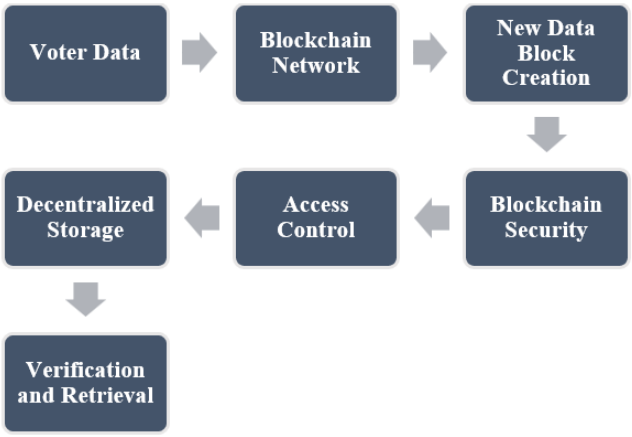

Figure 6: Blockchain working process

Blockchain technology is used in the proposed voting system to create a secure and immutable ledger for storing and managing voter data, specifically facial photos. The procedure starts with the collecting of voter facial photographs,

which are then securely encrypted and saved in a new data block on the blockchain. Each new block added to the blockchain includes a cryptographic hash of the previous block, which ensures the chain's integrity and continuity. Furthermore, because blockchain technology is decentralized, the stored data is resistant to alteration and unauthorized access, as it is copied across numerous nodes in the network. This method secures and protects voter facial photographs, laying the groundwork for a dependable authentication and verification system during elections. As the voting process unfolds, any new voter data, such as updated facial photos or voter preferences, is added to successive blocks of the blockchain. Each subsequent block is cryptographically connected to the preceding one, resulting in a public and auditable record of all voting activities. This ensures that voter data is securely stored and accessible, while simultaneously preserving the integrity and immutability of the voting process. By utilizing blockchain technology in this manner, the suggested voting method improves election security and transparency, fostering trust and confidence in the democratic process. Furthermore, it provides a solid platform for future advancements and scalability, as the blockchain expands with each new block published.

3.2. FACIAL RECOGNITION

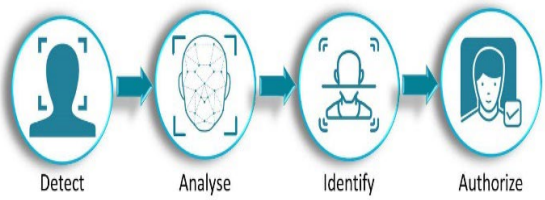

Figure 7: Facial Recognition

Facial recognition technology works inside a multistage workflow that includes detection, analysis, identification, and authorization. To begin, the system uses specialized algorithms to detect faces in photos or video streams, identifying facial features such as the eyes, nose, and mouth. Once recognized, the system analyses the face features to derive unique properties and patterns that distinguish one individual from another. This analysis phase frequently includes complex techniques such as machine learning and neural networks to improve accuracy and dependability. Following analysis, the algorithm compares the discovered faces to a database of known individuals. This identification procedure involves comparing the retrieved face features to previously stored templates or representations in order to find a close resemblance or match. Once a match is found or considered near enough, the system authorizes or authenticates the identified individual. This final stage frequently includes additional checks or validations to assure the accuracy and trustworthiness of the identification process, such as comparing alternative credentials or authorization methods.In essence, the workflow of facial recognition technology involves a smooth transition from detecting and analyzing visual traits to identifying and, eventually, authorizing persons. This methodical approach enables the technology to accomplish a wide range of activities with accuracy and efficiency, including access control and surveillance, as well as personal device authentication and biometric security. However, it is critical to recognize and address concerns about privacy, prejudice, and ethical implications at every stage of the workflow to ensure the responsible and transparent deployment of this powerful technology.

4. WORKING PROCESS

Facial recognition technology plays a crucial role in maintaining the integrity and security of the voting process, particularly in the context of voter face detection. The process begins by capturing the facial images of voters using devices such as webcams or mobile cameras. These images are subsequently analyzed using sophisticated algorithms, including Convolutional Neural Networks (CNNs), which are designed to identify and extract key facial features such as the eyes, nose, and mouth.Through advanced pattern recognition and analysis techniques, the system detects unique characteristics that differentiate one voter from another, enhancing the accuracy of voter identification. Once the facial features are extracted, the system compares them against a database of registered voters to verify identities. This verification process is essential for ensuring that only authorized individuals participate in the electoral process, thereby preventing instances of fraudulent voting.Moreover, facial recognition technology enhances accountability and

transparency in elections by enabling real-time monitoring and auditing of voter behavior. This capability allows electoral authorities to detect and address irregularities as they occur, reinforcing the overall integrity of the democratic process. By incorporating facial recognition into voter face detection systems, authorities can streamline the authentication process, minimize the risk of impersonation or duplicate voting, and ultimately foster public confidence in the electoral system.In addition to these security benefits, the integration of facial recognition technology can contribute to a more efficient voting experience. Voters can complete the identification process quickly, reducing wait times at polling stations. This improvement can lead to higher voter turnout, as individuals are more likely to participate when the process is straightforward and efficient. Furthermore, the use of facial recognition technology can help ensure compliance with election laws and regulations, as it provides an objective method for verifying voter identities.In summary, the implementation of facial recognition technology in the voting process not only protects the integrity of elections but also enhances the overall voter experience. By facilitating accurate identification and promoting transparency, this technology can significantly contribute to the advancement of democratic processes in a digital age.

5. MODULE ARCHITECTURE

Facial recognition technology plays a crucial role in maintaining the integrity and security of the voting process, particularly in the context of voter face detection. The process begins by capturing the facial images of voters using devices such as webcams or mobile cameras. These images are subsequently analyzed using sophisticated algorithms, including Convolutional Neural Networks (CNNs), which are designed to identify and extract key facial features such as the eyes, nose, and mouth.Through advanced pattern recognition and analysis techniques, the system detects unique characteristics that differentiate one voter from another, enhancing the accuracy of voter identification. Once the facial features are extracted, the system compares them against a database of registered voters to verify identities. This verification process is essential for ensuring that only authorized individuals participate in the electoral process, thereby preventing instances of fraudulent voting.Moreover, facial recognition technology enhances accountability and transparency in elections by enabling real-time monitoring and auditing of voter behavior. This capability allows electoral authorities to detect and address irregularities as they occur, reinforcing the overall integrity of the democratic process. By incorporating facial recognition into voter face detection systems, authorities can streamline the authentication process, minimize the risk of impersonation or duplicate voting, and ultimately foster public confidence in the electoral system.In addition to these security benefits, the integration of facial recognition technology can contribute to a more efficient voting experience. Voters can complete the identification process quickly, reducing wait times at polling stations. This improvement can lead to higher voter turnout, as individuals are more likely to participate when the process is straightforward and efficient. Furthermore, the use of facial recognition technology can help ensure compliance with election laws and regulations, as it provides an objective method for verifying voter identities.In summary, the implementation of facial recognition technology in the voting process not only protects the integrity of elections but also enhances the overall voter experience. By facilitating accurate identification and promoting transparency, this technology can significantly contribute to the advancement of democratic processes in a digital age.

1) Convolutional Layer Formula

$$O_{ij}^{(k)} = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} I_i + m_j + nK_{m,n}^{(k)} + b^k$$

Description: This formula describes the output of a convolutional layer in a CNN, where

O is the output feature map,

I is the input image,

K is the convolutional kernel,

Bis the bias term, and

M, N are the dimensions of the kernel. This operation helps extract features from voter images.

2) Activation Function (ReLU)

$$f(x) = \max(0, x)$$

Description: The Rectified Linear Unit (ReLU) activation function introduces non-linearity in CNNs, allowing the model to learn complex patterns in the data, which is crucial for distinguishing between different voters based on facial features.

3) Loss Function (Cross-Entropy Loss)

L (y,yˆ)= -1/N ∑_(i=1)^N[y_i log(yˆ_i)+(1-y_i)log(1-yˆ_i)

Description: This formula quantifies the difference between the predicted probabilities. It helps in training the CNN to improve accuracy in voter identification.

4) Euclidean Distance for Facial Recognition

$$d(x_{1,}x_2) = \sqrt{\sum_{i=1}^{n} (x_{1i} - x_{2i})2}$$

Description: This formula calculates the distance between two feature vectors, allowing the system to measure similarity between a voter's facial features and those stored in the database.

5) One-Time Password (OTP) Generation

$$OTP = H(K \oplus T)$$

Description: In this formula,

H is a hash function,

Kis a secret key, and

T is the current time (or a counter). This is used to generate time-based OTPs for dual-factor authentication, ensuring that only authorized users can cast votes.

6) Blockchain Hashing

$$H(m)=SHA\text{-}256(m)$$

Description: This formula illustrates how a message m (e.g., a vote) is hashed using SHA-256. The resulting hash is stored in a blockchain, providing an immutable and secure record of all votes.

7) Consensus Mechanism (Proof of Work)

$$Difficulty \leq (nonce \parallel block\_data)$$

Description: This formula describes a simplified version of a proof-of-work consensus mechanism used in blockchain technology. It ensures that transactions (votes) are verified by solving complex computational problems, enhancing security.

8) Accuracy Calculation

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Description: This formula evaluates the performance of the CNN model by calculating the ratio of correctly predicted instances (True Positives and True Negatives) to the total instances, crucial for assessing voter identification accuracy.

9) Precision and Recall

$$Precision = \frac{TP}{TP + FP}, Recall = \frac{TP}{TP + FN}$$

Description: These formulas measure the effectiveness of the facial recognition system. Precision indicates how many of the predicted positive cases were correct, while recall shows how many actual positive cases were captured.

10) Data Encryption (AES)

$$C = E_k(p)$$

Description: This formula shows how plaintext

P is encrypted into cipher text.

C using a symmetric encryption algorithm (AES) with key

k. This ensures that sensitive voter information is securely stored and transmitted.

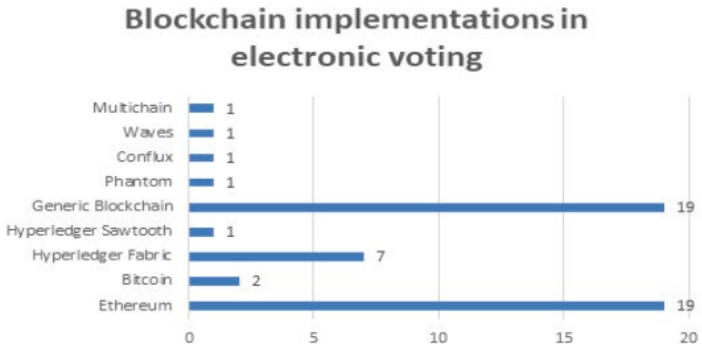

Figure 8. Trends in blockchain-based electronic voting systems

Blockchain-based electronic voting systems are emerging as a promising solution to address issues like security, transparency, and voter privacy in elections. These systems leverage block chain's decentralized nature to ensure that votes are immutable and securely stored, making tampering nearly impossible. Additionally, blockchain can increase voter trust due to its transparent and verifiable ledger of transactions, ensuring integrity and accuracy. Smart contracts can automate processes like vote counting and validation, further reducing human error. However, challenges such as scalability, voter anonymity, and access to technology remain prominent

"End-to-End Verifiable E-Voting Trial for Polling Station Voting" took place in Gateshead during the UK local elections on. This trial used a touchscreen-based system that ensured end-to-end (E2E) verifiability, allowing voters to independently verify that their votes were cast, recorded, and tallied accurately.

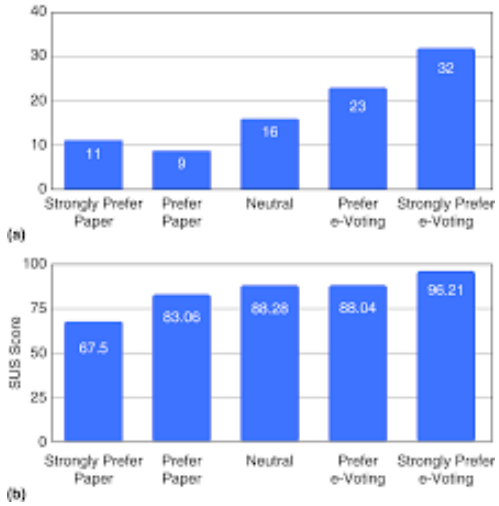

Figure 9. End-to-End Verifiable E-Voting Trial for Polling Station Voting explanation

The system-maintained voter privacy and ensured that the election process was transparent and tamper-proof, serving as a case study for future e-voting technologies

6. CONCLUSION

In conclusion, the proposed system represents a transformative approach to the electoral process by integrating advanced technologies such as blockchain, facial recognition, and Convolutional Neural Networks (CNN). This comprehensive framework addresses many challenges traditionally faced in voting systems, including security vulnerabilities, the potential for fraud, and inefficiencies in vote counting and verification. By leveraging a decentralized and tamper-proof blockchain ledger, the system ensures that voter data is securely stored and can be transparently audited, fostering trust among voters and stakeholders alike. This transparency is critical in a democratic process, where public confidence in the integrity of elections is paramount.The use of facial recognition technology enhances voter authentication, ensuring that each individual can only vote once and is who they claim to be. The system's multi-layered

security features, including OTP verification, significantly reduce the risk of unauthorized access and fraudulent activities, which have historically plagued electoral systems. By capturing clear facial images and processing them through advanced algorithms, the system provides a reliable means of identifying voters, thereby enhancing the overall security of the electoral process.Additionally, the modular design of the system allows for seamless integration and scalability. Each module, from user authentication to vote tallying, operates cohesively to deliver a streamlined and user-friendly experience for both voters and administrators. This ensures that the voting process is not only secure but also accessible, making it easier for citizens to participate in the democratic process. The real-time monitoring and reporting capabilities empower election officials to manage the election efficiently and respond swiftly to any anomalies or irregularities.Moreover, this innovative approach contributes to greater accountability in elections. The ability to audit and trace every vote back to its origin enhances the transparency of the electoral process, which is essential for maintaining public trust. Voters can have confidence that their votes are counted accurately and that the electoral system operates fairly.In a broader context, this system exemplifies how technology can enhance democratic governance and citizen engagement. By modernizing the voting process, we can encourage higher voter participation, particularly among younger demographics who are increasingly comfortable with digital interactions. As societies evolve, so too must our electoral systems, and this proposed solution sets a precedent for future advancements in voting technology.Ultimately, the integration of blockchain and AI-driven solutions into the voting process not only modernizes but also fortifies the democratic framework, paving the way for a more secure, transparent, and efficient electoral system. This innovative approach can serve as a model for other nations looking to enhance their electoral integrity and build trust in their democratic institutions, thus playing a crucial role in shaping the future of voting worldwide.

7. FUTURE ENHANCEMENT

Future enhancements to the proposed blockchain-based voting system can significantly improve its functionality, security, and user experience. One avenue for improvement lies in advancing facial recognition algorithms, incorporating more robust technologies that accurately identify individuals even under challenging conditions, such as poor lighting or varied angles. Implementing multi-factor authentication, including biometric methods like fingerprint or iris scanning, will further strengthen voter verification, minimizing the risk of impersonation. Developing a user-friendly mobile application could enhance accessibility and engagement by allowing voters to easily navigate the voting process and receive real-time election updates. The integration of AI and machine learning can facilitate predictive analytics to help election officials identify potential fraud patterns in real time. Utilizing smart contracts on the blockchain could automate election processes, such as managing voter registration and handling disputes, streamlining operations and reducing manual intervention. Comprehensive voter education initiatives, through interactive tutorials and accessible resources, can empower citizens to effectively navigate the voting process. As the system is deployed in larger jurisdictions, scalability will be crucial; optimizing the infrastructure will ensure efficiency and responsiveness during high-traffic periods, like election day. Implementing features for post-election audits and feedback mechanisms will provide insights into the system's effectiveness, informing future improvements. Enhancing interoperability with other electoral and governmental systems can facilitate data sharing and streamline processes, while creating customizable modules that adapt to local regulations will ensure the system's global applicability. By focusing on these enhancements, the blockchain-based voting system can evolve into a powerful tool for secure, transparent, and accessible elections, ultimately reinforcing public confidence in the democratic process and setting new standards for electoral integrity worldwide.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Vetrimani, E., and M. Arulselvi. "Computerized Online Voting System using RFID Technology and Image Processing." International Journal (AMIJ) Singaporean Journal of Scientific Research (SJSR) 11.1 (2019).

Choudhary, N., Agarwal, S., & Lavania, G. (2019). Smart Voting System through Facial Recognition. International Journal of Scientific Research in Computer Science and Engineering, 7(2), 7-10.

Motiwala, Aashay, Parshva Timbadia, Teerth Upadhyay, and Pankaj Kunekar. "E-Voting System Using Block Chain." SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology 11, no. SUP (2019): 434-438.

SH, Nandan Gowda, Jayam Haresh Tharun, B. N. Ashik, Deepak Lamani, and K. S. Priyadarshini. "Smart voting system using Face Recognition." (2020).

Singh, B., K. Sh Ranjan, and D. Aggarwal. "Smart voting web based application using face recognition, Aadhar and OTP verification." International Journal of Research in Industrial Engineering 9, no. 3 (2020): 260-270.

Damdoo, R., & Kalyani, K. (2020). Multilevel Voter Identity Protocol for Secure Online Voting. Int. J, 9, 3741-3745.

Pawar, B. M., Patode, S. H., Potbhare, Y. R., & Mohota, N. A. (2020, January). An Efficient and Secure Students Online Voting Application. In 2020 Fourth International Conference on Inventive Systems and Control (ICISC) (pp. 1-4). IEEE.

Kanimozhi, K., & Thangadurai, K. Aadhaar Based Unique Multimodal Based Biometric System for E-voting System with IANFIS Method.

Goulart, C., Valadão, C., Delisle-Rodriguez, D., Funayama, D., Favarato, A., Baldo, G., Binotte, V., Caldeira, E. and Bastos-Filho, T., 2019. Visual and thermal image processing for facial specific landmark detection to infer emotions in a child-robot interaction. Sensors, 19(13), p.2844.

Adekunle, Salako E. "A Review of Electronic Voting Systems: Strategy for a Novel." International Journal of Information Engineering & Electronic Business 12, no. 1 (2020).