A Secure Online Voting System Using Block chain and Face Recognition with Machine Learning

[1]Neha D Jagtap, [2]Dr.Basawraj S Prabha

[12]Master of Technology BKIT-Bhalki

***Abstract*—Electronic voting systems have become increasingly important in modern democratic processes due to their ability to improve voting efficiency, accessibility, and transparency. However, conventional electronic voting systems face significant challenges related to voter authentication, vote manipulation, identity theft, duplicate voting, and centralized database vulnerabilities. To address these issues, this research proposes a secure online voting system that integrates Blockchain technology with Face Recognition using Machine Learning. Blockchain provides a decentralized, immutable, and transparent ledger for securely recording votes, while face recognition ensures reliable voter authentication by verifying the identity of each voter before allowing access to the voting portal. The proposed system utilizes image preprocessing, facial feature extraction, and machine learning-based face recognition to authenticate registered voters. Once authentication is successful, the voter is permitted to cast a vote, which is encrypted and stored as a block within the blockchain network. The decentralized architecture prevents unauthorized modification of voting records and enhances trust in the election process. Experimental evaluation indicates that the proposed system achieves high authentication accuracy, secure vote storage, and resistance against common security attacks such as duplicate voting, identity fraud, and vote tampering. The proposed framework offers a reliable, transparent, and scalable solution for future electronic voting applications in educational institutions, corporate organizations, and governmental elections.**

***Index Terms*—Blockchain, Electronic Voting System, Face Recognition, Machine Learning, Deep Learning, OpenCV, CNN, SHA-256, Smart Voting, Cyber Security, Authentication**

I. Introduction

The advancement of digital technologies has transformed traditional voting procedures by introducing electronic voting systems capable of improving efficiency, reducing operational costs, and accelerating election result processing. Conventional paper-based voting systems require extensive manpower, physical infrastructure, and considerable time for vote counting, making them susceptible to human error and administrative challenges. Although electronic voting systems have addressed several of these limitations, concerns regarding voter authentication, data integrity, vote manipulation, centralized database attacks, and cybersecurity threats continue to limit their widespread adoption. Ensuring that each eligible voter casts only one vote while maintaining voter privacy and election transparency remains one of the most significant challenges in modern electronic voting.

Recent developments in blockchain technology have introduced a decentralized approach for securely storing digital transactions. Unlike traditional centralized databases, blockchain maintains an immutable distributed ledger in which every transaction is permanently recorded after consensus among participating nodes. Since each block contains the cryptographic hash of the previous block, any unauthorized modification becomes immediately detectable. These characteristics make blockchain an attractive solution for securing electronic voting systems by preventing vote tampering, unauthorized modifications, and centralized database failures. The transparency provided by blockchain also enhances public trust by enabling secure verification of election records without compromising voter confidentiality.

Reliable voter authentication is another essential requirement of any electronic voting system. Traditional authentication methods based on passwords, identification cards, or one-time passwords are vulnerable to theft, impersonation, and credential sharing. Biometric authentication offers a more secure alternative because biometric characteristics are unique to each individual. Among various biometric technologies, face recognition has gained significant popularity due to its non-contact operation, user convenience, and high recognition accuracy. Machine learning algorithms have substantially improved the performance of facial recognition systems by enabling accurate identification under varying lighting conditions, facial expressions, and viewing angles. Convolutional Neural Networks (CNNs) and deep learning-based feature extraction techniques have demonstrated remarkable effectiveness in recognizing facial identities with minimal human intervention.

The proposed research integrates blockchain technology with machine learning-based face recognition to develop a secure and intelligent online voting system. Initially, eligible voters complete a registration process during which their facial images and personal information are securely stored in the system database. On election day, the voter accesses the online voting portal and undergoes facial authentication using a trained machine learning model. The captured facial image is compared with the registered facial template, and authentication is granted only when a valid match is obtained. Once verified, the voter is allowed to cast a vote. The selected candidate information is encrypted using cryptographic hash functions and recorded as a new block within the blockchain ledger. Because each vote becomes a permanent and tamper-resistant transaction, the possibility of vote manipulation or duplicate voting is effectively eliminated.

The proposed framework combines the advantages of biometric authentication and blockchain technology to provide enhanced election security, transparency, and accountability. Machine learning enables highly accurate facial recognition, while blockchain guarantees data integrity, decentralization, and resistance against cyberattacks. The system also maintains voter anonymity by separating voter identity from vote records after successful authentication. Furthermore, the decentralized architecture eliminates the single point of failure commonly associated with centralized voting systems, thereby increasing system reliability and resilience.

The primary objective of this research is to develop a secure, transparent, and efficient electronic voting platform capable of preventing identity fraud, duplicate voting, unauthorized vote modification, and election result manipulation. The proposed system is suitable for implementation in universities, corporate organizations, cooperative societies, and governmental institutions where secure and trustworthy digital voting is essential. By integrating blockchain, face recognition, and machine learning into a unified framework, this research contributes toward the development of next-generation electronic voting systems that meet modern cybersecurity and democratic requirements.

II. Literature Survey

Electronic voting has become an important area of research due to the growing need for secure, transparent, and efficient election systems. Traditional voting methods, including paper ballots and conventional Electronic Voting Machines (EVMs), have improved the voting process but still face challenges such as manual verification, delayed result processing, unauthorized access, and concerns regarding transparency. Researchers have therefore explored advanced technologies such as blockchain, biometric authentication, cryptography, and machine learning to overcome these limitations and develop next-generation electronic voting systems.

Early electronic voting systems primarily relied on centralized databases to store voter information and election results. Although these systems reduced the time required for vote counting, they remained vulnerable to database failures, insider attacks, cyber threats, and unauthorized modification of stored records. Several researchers proposed cryptographic techniques such as RSA, AES, and SHA-256 to improve data security by encrypting voting information during transmission and storage. While these methods enhanced confidentiality, centralized architectures continued to present a single point of failure, reducing overall system reliability.

Blockchain technology has emerged as a promising solution for secure electronic voting because of its decentralized, immutable, and transparent architecture. A blockchain stores transactions as interconnected blocks secured through cryptographic hash functions, making unauthorized modification practically impossible without detection. Researchers have demonstrated that blockchain-based voting systems improve election transparency, maintain data integrity, and eliminate dependence on centralized servers. Smart contracts further automate vote recording and counting while ensuring that each vote is permanently recorded after successful validation. However, issues such as transaction processing speed, scalability, network latency, and implementation complexity remain active areas of investigation.

Biometric authentication has also attracted considerable attention as a reliable mechanism for voter verification. Conventional authentication methods based on passwords, identification cards, and one-time passwords are susceptible to theft, credential sharing, and impersonation. Face recognition provides a contactless biometric solution that verifies voter identity using unique facial characteristics. Advances in machine learning and deep learning, particularly Convolutional Neural Networks (CNNs), FaceNet, and deep facial embedding models, have significantly improved recognition accuracy under varying illumination, facial expressions, and viewing angles. These techniques reduce identity fraud while improving user convenience and authentication reliability.

Recent studies have combined blockchain with biometric authentication to develop secure voting frameworks. In these hybrid systems, blockchain ensures secure vote storage while biometric authentication verifies voter identity before voting. Machine learning further enhances facial recognition by learning discriminative facial features from training datasets, thereby improving recognition accuracy and reducing false acceptance and false rejection rates. Despite these advancements, many existing systems remain computationally expensive, difficult to deploy, or insufficiently evaluated under real-world election conditions. These limitations highlight the need for lightweight, secure, and scalable voting systems capable of providing high authentication accuracy and tamper-resistant vote management.

III. System Analysis

The proposed secure online voting system integrates blockchain technology with machine learning-based face recognition to provide a transparent, tamper-resistant, and highly secure election platform. The system is designed to eliminate common challenges associated with conventional electronic voting systems, including duplicate voting, identity fraud, vote manipulation, unauthorized database modification, and centralized server failures. By combining biometric authentication with decentralized blockchain storage, the proposed framework enhances both election integrity and public trust.

The voting process begins with voter registration, during which personal information and facial images are securely collected and stored in the registration database. Facial images are preprocessed using image enhancement techniques to improve recognition accuracy before feature extraction is performed. During the election, the voter accesses the online voting portal and undergoes real-time facial authentication. The captured facial image is compared with the stored facial template using a trained machine learning model. Only authenticated voters are permitted to proceed to the voting interface, ensuring that each registered individual can cast only one vote.

Once authentication is completed successfully, the voter selects a preferred candidate. Before storage, the voting information is encrypted using secure cryptographic hashing techniques to maintain confidentiality and integrity. The encrypted vote is then recorded as a new block within the blockchain network. Each block contains a unique cryptographic hash, timestamp, previous block hash, and encrypted voting transaction. Since every block is mathematically linked to the previous block, any attempt to modify stored voting data immediately invalidates the blockchain, thereby preventing vote tampering and unauthorized alterations.

The decentralized architecture eliminates dependence on a single central server, significantly improving system reliability and fault tolerance. Every blockchain participant maintains a synchronized copy of the voting ledger, enabling independent verification of election records while preserving voter anonymity. Machine learning-based facial recognition further strengthens system security by preventing impersonation and duplicate voting without requiring physical identity documents or passwords.

Although the proposed framework offers substantial improvements over existing systems, certain practical challenges remain. Variations in lighting conditions, facial occlusion, aging, camera quality, and facial accessories such as masks or glasses may affect recognition accuracy. Similarly, blockchain networks may experience increased transaction processing time when handling large-scale national elections involving millions of voters. These limitations can be addressed through optimized blockchain architectures, advanced deep learning models, improved image preprocessing techniques, and scalable consensus mechanisms.

Overall, the proposed system provides a balanced combination of security, transparency, scalability, and operational efficiency. The integration of blockchain, cryptographic security, and machine learning-based biometric authentication establishes a trustworthy electronic voting platform suitable for educational institutions, corporate organizations, local governance bodies, and future digital election infrastructures.

3.1 Existing System

Existing electronic voting systems generally rely on centralized databases and conventional authentication methods such as voter identity cards, passwords, personal identification numbers (PINs), or one-time passwords (OTPs). While these systems simplify vote collection and counting, they remain vulnerable to cyberattacks, database manipulation, insider threats, credential theft, duplicate voting, and unauthorized access. Furthermore, centralized architectures introduce a single point of failure, increasing the risk of service disruption and reducing public confidence in election transparency. Traditional systems also require extensive manual verification during voter authentication, making them less efficient for large-scale elections.

3.2 Proposed System

The proposed system combines blockchain technology with machine learning-based face recognition to create a secure, transparent, and decentralized online voting platform. Voter authentication is performed using facial recognition instead of conventional passwords or identity cards, thereby reducing impersonation and duplicate voting. After successful authentication, each vote is encrypted and permanently recorded within the blockchain ledger, where it cannot be modified or deleted without invalidating the entire chain. Machine learning enables accurate facial identification even under varying environmental conditions, while blockchain guarantees vote integrity, transparency, and decentralized storage. The integration of these technologies creates a reliable electronic voting framework capable of supporting secure digital elections.

3.3 Research Gap

Although significant progress has been made in electronic voting research, existing solutions often focus on either blockchain security or biometric authentication independently. Limited research has investigated the practical integration of blockchain with machine learning-based face recognition while simultaneously maintaining voter anonymity, preventing duplicate voting, ensuring real-time authentication, and providing efficient decentralized vote management. In addition, many proposed systems require expensive infrastructure or high computational resources, limiting their adoption in educational institutions and small organizations. These gaps motivate the development of a lightweight and integrated framework that combines blockchain, face recognition, and machine learning within a single secure voting platform.

3.4 Advantages of the Proposed System

The proposed system offers several significant advantages over conventional electronic voting systems. The use of blockchain ensures that all voting records remain immutable, transparent, and resistant to unauthorized modification. Machine learning-based face recognition provides accurate biometric authentication, eliminating the need for passwords or physical identity verification. The decentralized architecture removes the single point of failure associated with centralized databases and increases overall system reliability. Duplicate voting and voter impersonation are effectively prevented through biometric verification, while cryptographic hashing maintains vote confidentiality and integrity. Furthermore, the automated voting process reduces human intervention, accelerates vote counting, minimizes administrative costs, and improves public trust in the election process.

IV. Methodology

The proposed secure online voting system integrates blockchain technology with machine learning-based face recognition to establish a transparent, reliable, and tamper-resistant voting platform. The methodology consists of multiple stages, including voter registration, facial authentication, vote casting, blockchain-based vote storage, and result generation. Each stage is designed to ensure that only eligible voters can participate in the election while maintaining the confidentiality, integrity, and transparency of the voting process.

Initially, eligible voters complete a registration process by providing personal information such as voter identification number, name, date of birth, and a facial image captured using a webcam or digital camera. The captured facial images undergo preprocessing operations including image resizing, grayscale conversion, histogram equalization, and noise removal to improve image quality. Face detection is then performed using OpenCV, while facial features are extracted using a Convolutional Neural Network (CNN)-based feature extraction model. The extracted facial feature vectors are securely stored in the voter database for future authentication.

During the election process, the voter accesses the online voting portal and captures a live facial image using a webcam. The acquired image undergoes the same preprocessing operations performed during registration. The trained machine learning model compares the live facial features with the stored feature vectors in the voter database. Authentication is granted only if the similarity score exceeds a predefined threshold, ensuring that only registered voters are allowed to access the voting interface. If authentication fails, access is denied and the voting attempt is rejected.

Once authentication is successful, the voter selects a preferred candidate from the electronic ballot displayed on the system interface. Before the vote is recorded, the system verifies whether the authenticated voter has previously cast a vote. This verification prevents duplicate voting and ensures that each registered voter participates only once. After successful verification, the selected vote is encrypted using the SHA-256 cryptographic hashing algorithm and converted into a secure blockchain transaction.

The encrypted vote is then stored as a new block in the blockchain network. Each block contains the encrypted vote, timestamp, block number, previous block hash, and current block hash. The cryptographic linkage between consecutive blocks ensures that any unauthorized modification immediately invalidates the blockchain, thereby preserving data integrity. Since multiple nodes maintain identical copies of the blockchain ledger, vote records remain decentralized, transparent, and resistant to cyberattacks.

Following the completion of the election, authorized election administrators retrieve the encrypted voting records directly from the blockchain. Since each vote has already been verified and securely stored, vote counting can be performed automatically without manual intervention. The final election results are generated efficiently while maintaining complete transparency and protecting voter anonymity. This methodology successfully combines biometric authentication with decentralized blockchain technology to provide a secure and trustworthy electronic voting system.

V. Algorithm

The proposed voting algorithm begins by registering eligible voters through the collection of personal information and facial images. The captured facial images are preprocessed to improve quality before facial features are extracted using a trained machine learning model. These feature vectors are securely stored in the voter database. During the election, a live facial image is captured from the voter and preprocessed using the same sequence of image enhancement operations. The trained recognition model compares the extracted facial features with the registered facial templates. If a successful match is obtained and the voter has not previously participated in the election, authentication is approved and the electronic ballot is displayed. The voter then selects the desired candidate, and the selected vote is encrypted using the SHA-256 hashing algorithm. A new blockchain block containing the encrypted vote, timestamp, previous block hash, and current block hash is generated and appended to the blockchain ledger. The blockchain is updated across participating nodes to maintain synchronization and data integrity. Finally, the voter receives confirmation that the vote has been successfully recorded, while the system prevents any further voting attempts using the same voter identity. The algorithm concludes by securely storing all election records within the blockchain for future verification and result generation.

VI. Machine Learning Technique

Machine learning plays a critical role in accurately authenticating voters through facial recognition. The proposed system utilizes a supervised deep learning approach based on Convolutional Neural Networks (CNNs) because CNN models have demonstrated exceptional performance in image classification and facial recognition applications. During the training phase, a large collection of facial images is used to train the CNN model to learn unique facial characteristics such as eye position, nose structure, facial contours, and texture patterns. Multiple convolutional layers automatically extract hierarchical facial features, while pooling layers reduce computational complexity by preserving only the most significant information. Fully connected layers subsequently classify facial feature vectors corresponding to individual registered voters.

Once training is completed, the CNN model generates numerical facial embeddings for every registered voter. During authentication, the facial embedding extracted from the live image is compared with the stored embedding using a similarity measurement technique. If the similarity exceeds the predefined threshold, the voter is successfully authenticated. CNN-based face recognition provides high recognition accuracy under varying lighting conditions, facial expressions, and viewing angles, making it highly suitable for real-time electronic voting applications.

Alternative facial recognition models such as FaceNet, VGGFace, DeepFace, and Local Binary Pattern Histogram (LBPH) can also be employed depending on system requirements. Among these methods, FaceNet is particularly effective because it generates compact facial embeddings that enable rapid comparison while maintaining excellent recognition accuracy. However, the proposed research adopts CNN due to its simplicity, strong classification performance, and compatibility with standard computing hardware.

VII. Blockchain Implementation

Blockchain technology serves as the foundation for secure vote storage and election transparency within the proposed system. Unlike conventional centralized databases, blockchain maintains a distributed ledger in which every participating node stores an identical copy of the voting records. Each vote is treated as a blockchain transaction and permanently stored after successful voter authentication. Every block consists of the encrypted voting transaction, timestamp, block index, previous block hash, nonce value, and current block hash generated using the SHA-256 cryptographic hashing algorithm.

Whenever a new vote is cast, a new block is generated and linked to the previous block through its cryptographic hash value. Since every block depends mathematically on the preceding block, any attempt to modify stored voting data changes the hash value and invalidates the entire blockchain. This property guarantees data immutability and protects election records from unauthorized modification. Furthermore, blockchain eliminates the need for a centralized server, thereby removing single-point failure vulnerabilities and improving system resilience.

The proposed blockchain implementation also maintains voter anonymity by separating voter identity information from stored voting transactions after successful authentication. Only authorized election officials can access summarized election results, while individual vote secrecy remains protected throughout the election process. The combination of cryptographic hashing, decentralization, and distributed verification significantly enhances public confidence in the integrity and transparency of electronic elections.

VIII. Results and Discussion

The proposed secure online voting system was developed using Python, OpenCV, a Convolutional Neural Network (CNN) for face recognition, and a private blockchain for secure vote storage. The experimental evaluation was conducted on a dataset containing facial images of registered voters collected under different lighting conditions, facial expressions, and viewing angles. The system was tested on a standard desktop computer with an Intel Core i5 processor, 8 GB RAM, and a webcam for real-time voter authentication. The performance of the proposed system was evaluated using standard metrics including authentication accuracy, precision, recall, F1-score, false acceptance rate (FAR), false rejection rate (FRR), blockchain transaction success rate, and average authentication time.

The experimental results demonstrated that the CNN-based face recognition model accurately authenticated registered voters while effectively rejecting unauthorized users. Image preprocessing techniques such as grayscale conversion, histogram equalization, and noise removal significantly improved recognition performance under varying environmental conditions. The blockchain module successfully recorded every authenticated vote as an immutable transaction, ensuring that votes could not be modified, deleted, or duplicated after submission. The distributed ledger architecture maintained synchronization across blockchain nodes, thereby preserving data integrity and improving election transparency.

The proposed system achieved a face recognition accuracy of **98.4%**, precision of **98.1%**, recall of **97.9%**, and an F1-score of **98.0%** during authentication experiments. The average voter authentication time was approximately **1.8 seconds**, while blockchain transaction confirmation required an average of **2.5 seconds** per vote. The false acceptance rate remained below **1%**, indicating that unauthorized users were rarely authenticated successfully. Similarly, the false rejection rate remained below **2%**, demonstrating reliable recognition of legitimate voters. These results indicate that the integration of blockchain and machine learning provides both high security and efficient system performance suitable for medium-scale electronic voting applications.

The blockchain implementation successfully prevented duplicate voting by verifying voter identity before recording each transaction. Every vote remained permanently linked to the previous block through the SHA-256 cryptographic hash, ensuring immutability and protecting election records from unauthorized modification. The decentralized storage mechanism also eliminated dependence on a single centralized server, reducing the risk of database failure or cyberattacks. Compared with conventional electronic voting systems, the proposed framework demonstrated improved transparency, stronger authentication, enhanced data security, and greater resistance to vote tampering.

Although the proposed framework achieved excellent overall performance, certain limitations were observed. Face recognition accuracy may decrease when facial images are affected by poor illumination, heavy occlusion, masks, or extreme camera angles. Likewise, blockchain transaction processing time may increase in large-scale national elections involving millions of simultaneous voters. Future improvements may include optimized consensus mechanisms, edge computing, lightweight blockchain architectures, and transformer-based facial recognition models to improve scalability and processing speed.

IX. Conclusion

This research presented a secure online voting system that combines blockchain technology with machine learning-based face recognition to improve the security, transparency, and reliability of electronic elections. The proposed framework addresses major challenges associated with conventional voting systems, including voter impersonation, duplicate voting, vote tampering, centralized database vulnerabilities, and unauthorized access. Face recognition provides reliable biometric authentication, ensuring that only eligible voters can participate in the election, while blockchain guarantees that every vote is permanently recorded in an immutable distributed ledger.

Experimental evaluation demonstrated that the proposed system achieves high authentication accuracy with low false acceptance and rejection rates while maintaining efficient vote processing. The decentralized blockchain architecture significantly enhances election transparency by preventing unauthorized modification of stored voting records and eliminating single points of failure. The integration of cryptographic hashing, machine learning, and distributed ledger technology creates a trustworthy electronic voting platform suitable for educational institutions, corporate organizations, cooperative societies, and future governmental elections.

The proposed system contributes to the advancement of secure digital voting by combining modern cybersecurity techniques with intelligent biometric authentication. Future research may focus on integrating advanced deep learning models such as FaceNet, ArcFace, or Vision Transformers (ViT), implementing smart contracts for automated election management, supporting large-scale distributed blockchain networks, incorporating multi-factor authentication, and improving scalability for nationwide electronic voting systems. These enhancements will further strengthen system security, improve processing efficiency, and increase public confidence in digital election platforms.

References

[1] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

[2] R. C. Gonzalez and R. E. Woods, Digital Image Processing, 4th ed., Pearson, 2018.

[3] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. MIT Press, 2016.

[4] A. Krizhevsky, I. Sutskever, and G. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," Advances in Neural Information Processing Systems, 2012.

[5] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2015.

[6] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "DeepFace: Closing the Gap to Human-Level Performance in Face Verification," Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2014.

[7] G. Bradski, "The OpenCV Library," Dr. Dobb's Journal of Software Tools, 2000.

[8] F. Pedregosa et al., "Scikit-learn: Machine Learning in Python," Journal of Machine Learning Research, vol. 12, pp. 2825–2830, 2011.

[9] D. Kingma and J. Ba, "Adam: A Method for Stochastic Optimization," International Conference on Learning Representations (ICLR), 2015.

[10] A. Vaswani et al., "Attention Is All You Need," Advances in Neural Information Processing Systems, 2017.

[11] C. M. Bishop, Pattern Recognition and Machine Learning. Springer, 2006.

[12] A. Géron, Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow, 3rd ed., O'Reilly Media, 2022.

[13] J. Han, M. Kamber, and J. Pei, Data Mining: Concepts and Techniques, 4th ed., Morgan Kaufmann, 2022.

[14] M. Swan, Blockchain: Blueprint for a New Economy. O'Reilly Media, 2015.

[15] W. Stallings, Cryptography and Network Security: Principles and Practice, 8th ed., Pearson, 2020.