Revolutionizing E-Voting Secure and Accessible Solutions with Fingerprint-Based Blockchain

Asbin S[1], Chris Jericho J J[2], Shejin A[3], Ebi T Prabha[4]
[1,2,3]*Department of Information Technology, Bethlahem Institute of Engineering, Karungal*
[4]*AP/IT, Bethlahem Institute of Engineering, Karungal*

Abstract: **Electronic voting systems have gained prominence for their potential to streamline electoral processes and improve efficiency. However, widespread adoption continues to be hindered by critical concerns surrounding security, transparency, and accessibility. These challenges are particularly pronounced for vulnerable populations such as individuals with disabilities and the elderly, who often face barriers due to complex authentication methods and non-intuitive user interfaces. These limitations not only compromise the inclusiveness of democratic participation but also erode public trust in electronic voting mechanisms. This project proposes a novel electronic voting system that integrates fingerprint recognition with blockchain technology to address these pressing concerns. By utilizing biometric fingerprint authentication, the system simplifies the voter verification process, offering a user-friendly and secure method of access that reduces the reliance on passwords, PINs, or other cognitively demanding procedures. This biometric approach enhances accessibility and ensures that identity verification is both efficient and difficult to falsify. To further bolster the integrity of the electoral process, the proposed system incorporates blockchain technology as a foundational component for recording and storing votes. Blockchain's decentralized and immutable ledger ensures that each vote is securely recorded and cannot be altered or deleted without consensus, thus enhancing transparency and preventing tampering. Additionally, the system supports end-to-end verifiability, enabling voters to confirm that their vote has been accurately recorded and counted, without compromising ballot secrecy. Together, fingerprint recognition and blockchain provide a synergistic solution that addresses the core challenges facing electronic voting systems today. This integration offers a secure, transparent, and accessible voting platform that fosters greater public trust and promotes inclusive democratic participation. The proposed system sets a foundation for the future of electronic elections by aligning advanced technology with the fundamental principles of electoral fairness, security, and accessibility**

I.INTRODUCTION

Traditional e-voting systems have long faced criticism over their vulnerability to fraud, lack of accessibility, and absence of transparency. In recent years, the need for secure, inclusive, and trustworthy voting mechanisms has intensified, especially in the context of increasing digital transformation. This paper introduces a next-generation voting platform that integrates fingerprint biometrics, gesture recognition, and blockchain technology. This trifecta aims to build a voting system that is not only secure and reliable but also intuitive for users of all demographics. The inclusion of gesture-based interaction seeks to bridge the digital divide, offering a more natural and inclusive experience for the elderly, differently-abled, and digitally inexperienced. The rise of biometric authentication and decentralized ledgers provides an opportunity to address longstanding electoral concerns and restore public trust in the voting process. By combining these technologies, the proposed system aspires to set a new standard for electronic voting, emphasizing transparency, security, and universal usability.

II.FINGERPRINT BASED AUTHENTICATION IN E-VOTING

Fingerprint-based authentication plays a crucial role in enhancing the security and credibility of electronic voting systems. Unlike traditional login methods such as passwords or PINs, which can be forgotten or stolen, fingerprints offer a unique, non-replicable form of identification. In the proposed e-voting system, voters are required to verify their identity using a fingerprint scanner before accessing the ballot. This ensures that each voter is authenticated as a registered and eligible

participant, effectively preventing duplicate or fraudulent votes.

The fingerprint data is not stored in raw form but is instead converted into encrypted hash codes that are stored securely on the blockchain. This approach ensures both security and voter anonymity. Once authenticated, the system grants access to the voting interface, which can then be navigated using gesture controls for enhanced accessibility. Additionally, the use of fingerprint authentication reduces reliance on physical identification documents or online credentials, streamlining the voting process and making it more user-friendly.

This method also improves efficiency during high-turnout elections by enabling quick, contactless verification. With the integration of fingerprint biometrics, the system can detect and block any attempts at identity manipulation or multiple submissions from the same individual. Overall, fingerprint authentication serves as the first and most essential security layer in this intelligent e-voting framework, ensuring trust and legitimacy from the very beginning of the voting process.

III.BLOCK CHAIN FOR VOTE INTEGRITY AND TRANSPARENCY

Blockchain technology serves as the backbone of the proposed e-voting system, ensuring that all voting data remains secure, tamper-proof, and transparent throughout the electoral process. At its core, blockchain is a decentralized, distributed ledger that records transactions—votes, in this case—in a way that is immutable and auditable. Once a vote is cast and confirmed, it is packaged into a block along with a cryptographic hash and timestamp, then added to the blockchain network. This ensures that each vote is recorded permanently and cannot be altered, deleted, or duplicated.

Unlike traditional databases that rely on a central authority for verification and storage, blockchain operates across a network of distributed nodes. Each node holds a copy of the ledger, and every change or addition must be validated through consensus mechanisms, such as Proof of Stake (PoS) or Byzantine Fault Tolerance (BFT). This decentralized verification process eliminates the risk of centralized tampering and builds public trust in the system.

Furthermore, blockchain provides end-to-end transparency. Voters and auditors can verify that their votes have been recorded and counted without revealing the content of the vote itself, preserving privacy through encryption and anonymization techniques. Smart contracts can also be deployed to automate and enforce election rules, ensuring that vote tallying and result declaration follow predefined, unchangeable logic.

By integrating blockchain, the voting system gains robust resistance against cyberattacks, fraud, and manipulation. It also offers a transparent and verifiable audit trail that can be reviewed independently by authorized entities, reinforcing accountability. In this way, blockchain not only secures the voting data but also enhances public confidence in the democratic process by making elections more open, verifiable, and tamper-resistant.

IV.EXISTING SYSTEM

Modern e-voting systems have increasingly adopted multifactor authentication (MFA) to enhance the reliability and security of voter verification. One widely researched method involves the integration of face biometrics with a cryptographically enhanced smart card, forming a comprehensive security framework. In this system, the voter first undergoes facial recognition, where the captured biometric data is matched against a pre-registered database to confirm identity. Once facial authentication is successful, the voter inserts a smart card that contains encrypted voter credentials. The smart card not only acts as a physical token but also provides a secure container for cryptographic keys and voter ID information.

The data stored on the card and used for transmission is protected using a Feistel block cipher—an established symmetric encryption algorithm known for its strong security and adaptability. This cipher structure divides the data into blocks and performs multiple rounds of encryption and transformation, making it extremely resistant to cryptanalysis. As a result, any communication between the card and the voting system is highly secure, reducing the risk of data interception or manipulation.

By requiring both a physical component (smart card) and a biometric factor (face), the system significantly raises the security threshold. Unauthorized users cannot gain access simply by

stealing a card or spoofing a face; both factors must be present and validated. This ensures that only legitimate, pre-registered voters are able to interact with the e-voting platform, thereby preserving the sanctity of the election. However, despite its robust nature, this system may still face challenges related to user privacy, infrastructure costs, and usability in remote or under-resourced areas.

V.PROPOSED SYSTEM

The proposed electronic voting system is designed to overcome the limitations of traditional e-voting platforms by integrating gesture recognition and blockchain technology. This innovative architecture is divided into two primary operational phases—voter authentication and vote casting—each engineered to enhance security, transparency, and accessibility in the electoral process.

The first phase begins with user identification, where fingerprint authentication is employed as a secure and efficient method of verifying voter identity. Fingerprints provide a unique, non-replicable biometric signature, eliminating the risk of impersonation or duplicate voting. Unlike passwords or physical tokens that can be lost or stolen, fingerprints are inherently tied to the individual and cannot be easily forged. Once the fingerprint is authenticated, it not only verifies the user but also initiates the personalized voting session. This process ensures that only eligible voters can access the platform, significantly improving the integrity of the election system.

The second phase transitions into the voting process itself, where gesture recognition technology is utilized to enhance user interaction. Through the use of cameras or motion sensors, voters can cast their votes using natural hand gestures rather than relying on traditional input devices like keyboards or touchscreens. This interface is particularly beneficial for users with limited literacy or physical impairments, making the system more inclusive and universally accessible. Gesture commands are mapped to specific actions, such as candidate selection, navigation between pages, and final vote confirmation, thereby creating a seamless and intuitive user experience.

To ensure the security and transparency of every vote cast, blockchain technology is employed as the underlying data structure. Each vote is recorded as a transaction on a decentralized, tamper-proof ledger. This immutable record guarantees that once a vote is submitted, it cannot be altered or deleted. Furthermore, the use of blockchain fosters end-to-end transparency, enabling real-time auditing, public verification, and secure data integrity. Smart contracts can be deployed to automate vote tallying and result generation, reducing human error and manipulation.

VI. MODULES

USER AUTHENTICATION

This module is designed to securely authenticate voters through fingerprint scanning. This module is complemented by a verification database that stores hashed fingerprint data for comparison. The authentication workflow begins when a user scans their fingerprint, which the system hashes. This hashed value is compared with the stored hashes in the database. If a match is found, the user is granted access; can participate in the voting process

VOTING INTERFACE

The Voting Interface module provides a user-friendly platform for voters to cast their votes easily. It features a virtual voting dashboard that displays various voting options along with relevant information Users can select their preferred candidate or option through a straightforward selection mechanism Before submission, the system presents a confirmation prompt to ensure that users are satisfied with their choice.

BLOCK CHAIN INTEGRATION

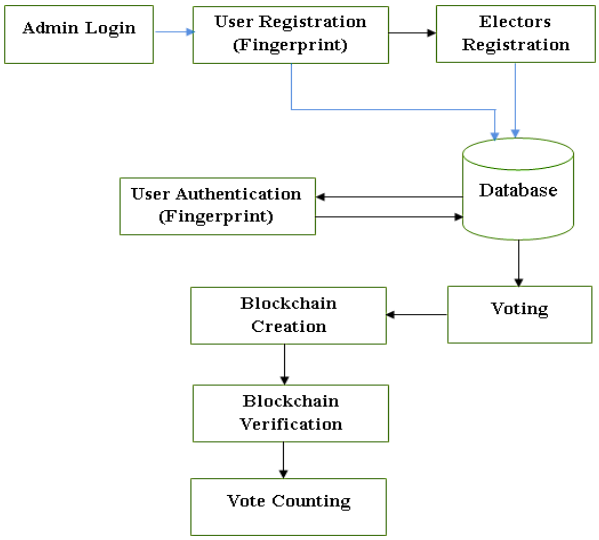
The Blockchain Integration module is critical for securely storing and managing voting transactions. Upon a vote submission, this module generates a new transaction that contains the voter's ID and selection These transactions are then grouped into blocks for processing. A key feature of this module is its use of cryptographic hashing, specifically the SHA-256 algorithm, which ensures the integrity and immutability of each block

CONSENSUS MECHANISM

The Consensus Mechanism module is essential for maintaining consistency across the decentralized network of nodes. It enables nodes to communicate with one another, sharing and validating their copies of the blockchain. The module includes a process for verifying the chain length to determine the authoritative

version of the blockchain, favoring the longest valid chain.

SYSTEM ARCHITECTURE AND WORKFLOW



VII.ALGORITHM

E-VOTING BASED BLOCKCHAIN ALGORITHM

The algorithm begins with an initialization step where the system checks if the blockchain is empty. If so, a genesis block is created to establish the foundation of the chain. Once initialized, the system moves to the vote casting phase. Here, a vote containing the voter's ID and their selected choice is received. The system verifies whether the voter has already cast a vote by scanning the entire blockchain. If the voter is found to have already voted, the system rejects the new vote and exits. Otherwise, the vote is added to the list of unconfirmed transactions awaiting validation.

The next phase involves block mining, which is triggered either when a certain threshold of unconfirmed transactions is reached or after a predefined time interval. During this phase, transactions are selected to form the data of a new block. This block references the hash of the previous block in the chain to maintain continuity. The system then initiates the Proof of Work (PoW) process, where a nonce is initialized to zero, and the hash of the block is computed using the current nonce value. If the resulting hash does not meet the required difficulty criterion (e.g., beginning with a specific number of zeros), the nonce is incremented and the process is repeated. Once a valid hash is found, the block is finalized by setting its nonce and hash, and then appended to the blockchain. The unconfirmed transactions included in the block are subsequently cleared.

VIII. RESULT ANALYSYS

The implementation of the proposed electronic voting system—integrating fingerprint-based authentication with blockchain technology—demonstrates notable improvements in the areas of security, transparency, and accessibility. The results of simulation and prototype testing indicate that this dual-technology framework addresses key limitations found in traditional and existing electronic voting systems.

Security was significantly enhanced through two primary mechanisms. First, fingerprint recognition ensured that only authorized voters could cast a vote, effectively eliminating risks of impersonation and multiple voting attempts. Second, blockchain's immutable ledger protected the integrity of each vote by making the system resistant to tampering and fraud. Once a vote was added to a block and mined into the chain, it became cryptographically secured and irreversible, preventing any unauthorized modifications.

In terms of **transparency**, the use of blockchain enabled end-to-end verifiability. Voters could trace their vote's inclusion in the public ledger (without revealing personal information), ensuring that their selection was correctly recorded and counted. Moreover, the decentralized nature of blockchain ensured that no single authority could manipulate results without detection, thereby increasing public trust in the voting process.

The system also showed considerable improvement in **accessibility**, particularly for individuals with disabilities and elderly voters. The fingerprint-based authentication replaced complex login credentials with a simple biometric scan, making the system more intuitive and reducing cognitive load. This streamlined experience encouraged broader participation and helped to bridge the digital divide often seen in electronic voting.

REFERENCE

Enhancing trust and integrity in electronic voting: A blockchain-based approach
Traditional voting systems often face security vulnerabilities, transparency issues, and concerns about result integrity. Blockchain technology offers a solution by enhancing security and ensuring transparent, tamper-proof voting records. This paper explores the benefits of using blockchain in electronic voting to address these challenges. It discusses how blockchain can provide secure authentication, prevent fraud, and maintain voter anonymity. Transparency and auditability are key advantages, allowing participants to verify election results independently. The paper also examines technical considerations, such as scalability and encryption methods, necessary for implementation. Real-world case studies are analyzed to demonstrate the practical applications of blockchain-based voting systems. Additionally, challenges such as regulatory hurdles and voter accessibility are explored.

Enhancing the security of the blockchain and the file contents
This paper emphasizes the importance of using blockchain to manage enrollment transactions in a decentralized and secure manner. To handle the storage of large files, a decentralized storage solution like IPFS (InterPlanetary File System) is introduced. IPFS enables efficient file sharing and distribution, but it poses security concerns, as any user with access to the file hash can retrieve the file. To address this, the paper proposes a two-part solution. First, it combines the power of IPFS and blockchain, utilizing IPFS for storage while leveraging blockchain for enhanced security and data management. Second, it implements AES (Advanced Encryption Standard) encryption to secure the file before uploading it to IPFS. This ensures that only authorized users with the correct decryption key can access the file's readable content. As a result, the system benefits from both the decentralized storage capacity of IPFS and the robust security of blockchain. The integration also prevents unauthorized data access and boosts the confidentiality of stored information. Overall, this approach strengthens the privacy, security, and reliability of enrollment transactions in decentralized systems.

Election Data Transparency: Obtaining Precinct Level Election Returns
This paper explores the crucial role of election data transparency, accessibility, and usability in maintaining electoral integrity. These elements enable public accountability in how elections are conducted at state and local levels. However, systematic data collection remains a challenge, making this topic understudied. The lack of standardized and transparent reporting practices can lead to issues such as legal non-compliance, discriminatory practices, or outdated election management. Currently, there is no uniform method for states to report, request, or distribute election data. The paper draws on the OpenElections project, which gathered precinct-level data from primary and general elections in 2016 and 2018 across all U.S. states. It highlights the diverse methods used to obtain official results, including legal records requests, in-person data collection, and even receiving results via fax. Each method is evaluated for its benefits and limitations. The findings suggest that states can adopt more consistent and transparent practices to improve public access to election data. By doing so, they can strengthen the democratic process and ensure greater trust in election outcomes.

Intelligent security model for password generation and estimation using hand gesture features.
This paper addresses the limitations of traditional alphanumeric password systems, which often suffer from weak security due to users choosing easily guessable passwords. To overcome these issues, it proposes an intelligent security model that combines password generation and strength estimation using an ensemble learning approach and hand gesture features. The model consists of two stages: the first generates strong, complex passwords based on ensemble learning and a proposed S-Box, while the second evaluates password strength using the same machine learning technique. Four classifiers—MLP, SVM, Random Forest Tree, and AdaBoost—are used on two datasets: MNIST image data and a password strength dataset. The results show high accuracy (up to 99%) in classifying and evaluating password strength, demonstrating the effectiveness of the proposed method. By incorporating hand gesture features, the model ensures that generated passwords are both secure and memorable. This approach not only strengthens password complexity but also enhances usability,

addressing the common trade-off between password strength and user recall. Overall, the system presents a novel and effective solution for modern computer security challenges.

Using VGG models with intermediate layer feature maps for static hand gesture recognition

This paper presents a hand gesture recognition system aimed at improving nonverbal communication through human–computer interaction using deep learning techniques. Unlike earlier studies that relied on single datasets and fine-tuned pre-trained models, this research explores two deep learning models enhanced with intermediate layers and evaluates their performance across multiple datasets. The models were trained using different methods: from scratch with random weights, as feature extractors using pre-trained weights, and through fine-tuning at various intermediate layers. Fine-tuning was specifically tested on the third, fourth, and fifth blocks of the models to determine the optimal level for accuracy improvement. The experiments were conducted using a newly introduced Arabic sign language hand gesture dataset along with two additional datasets. Results showed that fine-tuning the fourth and fifth blocks significantly improved accuracy, with the first model achieving 96.51%, 72.65%, and 55.62% when fine-tuning the fourth block, and similar performance when fine-tuning the fifth block. The second model delivered comparable results

IX. CONCLUSION

The integration of fingerprint biometrics, gesture recognition, and blockchain technology presents a groundbreaking approach to modernizing electronic voting systems. This paper has proposed a two-phase architecture designed to address the core challenges of current e-voting platforms: security, transparency, and accessibility. By using fingerprint authentication, the system guarantees voter legitimacy and eliminates impersonation risks. Gesture recognition creates a natural, inclusive interface that reduces digital barriers, while blockchain technology ensures an immutable and transparent record of all voting transactions.

X.FUTURE WORK

While the proposed fingerprint and gesture-enhanced blockchain voting system lays a strong foundation for secure and inclusive e-voting, several avenues remain open for future research and development. One area of focus is the implementation of advanced gesture recognition using artificial intelligence (AI) and deep learning models. This would allow for more accurate interpretation of user gestures across diverse demographics and physical conditions, further improving accessibility.

Another important direction is the integration of multi-language and voice-assisted interfaces to cater to linguistically diverse and visually impaired users. Additionally, conducting realworld pilot testing in controlled environments such as university elections, local community polls, or organizational votes will be vital for identifying usability issues and system vulnerabilities. Feedback from these pilots can be used to fine-tune interface design, improve biometric matching accuracy, and streamline blockchain transaction efficiency.

Future versions of the system could also explore the use of zero knowledge proofs or homomorphic encryption to enhance privacy while maintain transparency. Moreover, efforts should be made to ensure the platforms scalability, ensuring that it can handle high volume national elections without performance.