Cluster Computing (2024) 27:4015–4034
https://doi.org/10.1007/s10586-023-04261-x

Transforming online voting: a novel system utilizing blockchain and biometric verification for enhanced security, privacy, and transparency

Md Jobair Hossain Faruk[1] · Fazlul Alam[2] · Mazharul Islam[3] · Akond Rahman[4]

Received: 17 August 2023 / Revised: 21 December 2023 / Accepted: 22 December 2023 / Published online: 19 April 2024

Abstract
As a cornerstone of democratic governance, elections hold unparalleled significance, shaping a nation's trajectory. However, the prevailing ballot-paper based voting systems continue to face trust issues among significant populations. As a result, e-Voting has emerged as an appealing alternative, with numerous countries opting for its implementation globally. While e-Voting systems offer several advantages, they also come with their own set of challenges. Even a minor vulnerability can lead to massive manipulations in voting results. In recent years, there have been efforts to revolutionize the e-Voting paradigm by harnessing the potential of emerging technologies such as biometrics and blockchain. This paper proposes a Internet-based voting that adopts blockchain technology and biometric identification techniques. We use biometric modalities, such as fingerprint and facial recognition, for voter authentication while leveraging Hyperledger Fabric framework as blockchain network and ensuring a secure, transparent, and tamper-evident voting record. We demonstrate the proposed system with 100 participants in a preset environment where we collect the biometrics data. The results indicate that 87% of participants successfully registered with biometrics, while 88% cast their votes with a combination of either voter ID and fingerprint or voter ID with facial recognition. Our findings suggest that the proposed system allows voters to access the system seamlessly and automate identity verification procedures while ensuring a secure, decentralized, and distributed database network that maintains transparency. Future research shall be carried out in collaboration with election officials and voters to improve the system in real-world scenarios.

Keywords Online voting · Electronic voting · Blockchain technology · Hyperledger fabric · Biometrics technology · Face recognition · Smart contract

1 Introduction

Elections represent a critical method of determining representative leadership in democratic societies, providing an essential channel for citizens to express their political preferences [1]. Despite their integral role, traditional voting systems, particularly those relying on ballot paper, often grapple with trust issues [2]. Factors such as electoral fraud, manipulation, and rigging have underscored the need for a more secure, transparent, and robust approach. To address these challenges, electronic voting (e-Voting) has gained considerable traction globally, positioned as an appealing alternative to traditional voting methods [3]. E-Voting was introduced to mitigate the risks inherent in ballot paper voting, e-Voting aimed to curtail electoral fraud, streamline the voting process, reduce cost, and

✉ Md Jobair Hossain Faruk
mhossa37@nyit.edu

[1] Department of Computer Science, New York Institute of Technology, Manhattan, USA

[2] Department of Computer Science and Engineering, Daffodil International University, Birulia, Bangladesh

[3] Department of Computing, Sultan Idris Education University, Perak, Malaysia

[4] Department of Computer Science and Software Engineering, Auburn University, Auburn, USA

enhance accessibility [4]. However, e-Voting in its early forms, even with its many benefits, was not exempt from its own array of vulnerabilities.

Electronic voting systems can be broadly categorized into two types: Internet-based voting (i-Voting), which enables voting from any location via the Internet, and non-internet electronic voting (e-Voting), which requires voters to cast their votes physically at voting centers using electronic machines [5, 6]. The conventional technologies underlying these systems, primarily centralized databases, are particularly prone to corruption and manipulation [7]. Security threats such as Denial-of-Service attacks, malicious software, and spoofing attacks pose considerable risks, undermining the integrity of the voting process.

Considering these concerns, the incorporation of blockchain technology into e-Voting systems has emerged as a promising approach [8]. Blockchain technology is characterized by its decentralized architecture, immutability, and fault tolerance that offers a robust shield against data manipulation and fraud [9]. This distributed ledger technology provides an incorruptible, tamper-evident record of digital events, thus fostering trust and transparency [10, 11]. Furthermore, the adoption of blockchain technology has extended beyond e-Voting systems, transforming various sectors, including transportation, education, and healthcare that demonstrate strong security and privacy measures [12–14].

In parallel, biometric technology can bolster the authenticity of the voting process [15, 16]. With government entities worldwide capturing and storing biometric data, such as facial recognition and fingerprints, these unique identifiers can be leveraged for voter authentication [17, 18]. By integrating biometrics with blockchain, a secure and transparent voting system can be achieved, enhancing the integrity of the election process [19].

This paper explores the potential of blockchain technology and biometric identification to enhance the security and transparency of online voting (i-Voting), one step advanced of electronic voting. We propose a novel architecture for i-Voting systems that uses Hyperledger Fabric to secure and transparently record votes, and biometric identifiers, such as facial recognition and fingerprints, to reliably authenticate voters. Further, we engage in a comprehensive evaluation of our proposed system using standard methodologies to ensure the system's robustness, ease of use and accessibility. We believe that i-Voting has the potential to make a significant contribution to ongoing discourse on secure, transparent, and efficient i-Voting systems, paving the way for future real-world implementations.

This paper makes several contributions to the e-Voting domain, encompassing both theoretical and practical perspectives. These contributions are as follows:

- We offer a comprehensive exploration of the capabilities of internet voting (i-Voting) based on blockchain and biometric technology.
- We propose a novel i-Voting system that integrates facial and fingerprint biometrics with blockchain technology to ensure robust security, authentication, verification, and validation while maintaining efficient privacy.
- We conduct an evaluation of the proposed system, outlining its performance metrics, potential challenges, and future trajectories.

The manuscript is systematically organized into well-defined sections to provide clarity, progression, and in-depth exploration. Section 2 provides a thorough exposition of the potential of blockchain in online voting and the merits and utilities of biometric modalities, specifically emphasizing facial and fingerprint recognition for voter authentication. Section 3 reviews the extant literature, emphasizing research gaps and the distinctiveness of the presented work. Section 4 introduces the architecture of the internet voting framework of the proposed system, explaining its detailed modular components. Section 5 provides details of the implementation of the proposed system. First, we explain the voting algorithm, from registration to vote casting. Then, we discuss the algorithms for biometric data collection and storage, voter authentication, casting, and tallying. Finally, we introduce the implemented prototype on RESTful API. Section 6 presents the evaluation setup, metrics, and experimental results. This section describes the experimental setup used to evaluate the system and interprets the results. Section 7 provides a more in-depth discussion of the results, potential challenges, limitations, and outlines potential extensions and trajectories of the current research. Section 8 summarizes the research journey, encapsulating key insights, findings, and implications for the realm of online voting.

2 Innovative technologies for i-Voting

2.1 Blockchain technology

Blockchain technology is a digital, distributed, and decentralized ledger that presents a significant advancement over traditional database systems [20]. It enables the creation of a tamper-evident, trusted, and shared ledger by appending cryptographically secure data transactions in a sequential manner [21]. Once added to the ledger, this data remains immutable and accessible only to authorized stakeholders [22]. Each transaction is also timestamped, which further reinforces the security of the network and makes it resilient to potential data tampering [23]. The concept of smart contracts, or chaincodes are self-executing contracts that are stored on the blockchain and enforced upon fulfillment of predefined security criteria [24]. This can be used to ensure the integrity of the voting process and to prevent fraud.

Figure 1 illustrates a comparative analysis of traditional voting systems and blockchain-based voting system [25]. While traditional systems rely on a central authority susceptible to data manipulation, blockchain-based systems distribute data across multiple nodes, reducing the possibility of a coordinated hacking attempt. Different types of blockchains, such as public, private, and consortium blockchains, cater to varying use cases, with Ethereum and Hyperledger Fabric representing two widely recognized blockchain frameworks [26, 27]. Given our emphasis on sensitive and confidential data, we leverage Hyperledger Fabric for the development of our proposed i-Voting application.

A. Hyperledger fabric in electronic voting as a distributed ledger platform tailored for enterprise solutions, Hyperledger Fabric offers an architecture that ensures high levels of confidentiality, resilience, flexibility, and scalability [28]. It also supports modular consensus protocols, which allows it to be customized for specific use cases and trust models [29]. Implementing hyperledger fabric in the context of a voting system offers a robust and secure mechanism for vote casting, as votes are recorded immutably with smart contracts facilitating the setup of a private blockchain. The system also guarantees voter anonymity and fosters trust in the election process. It offers potential benefits for election officials as well, enabling them to customize nodes in alignment with governing rules or constitutional requirements [30, 31].

2.2 Biometrics technology

Biometric technology refers to automated systems capable of measuring distinct physical characteristics to verify an individual's claimed identity or identify an individual [32, 33]. This technology can significantly enhance voting frameworks and the overall voting experience [34]. As shown in Fig. 2, a typical biometrics system comprises multiple phases, including enrollment, verification, identification, and matching [35]. By integrating biometric identifiers such as facial and fingerprint recognition in our proposed voting system, we aim to elevate its security, privacy, and operational efficiency [36, 37].

A. Facial and Fingerprint Recognition in Voting System Facial recognition technology (FRT) combined with artificial intelligence (AI) is a powerful tool for accurate, flexible, and rapid identification [39]. It has been used in a variety of fields, including security, finance, education, and government management, to enhance early detection of suspicious activities and tracking of suspects [40]. The use of FRT in voting systems can improve security and trustworthiness due to its capacity to verify the identity of voters, which can help to prevent voter fraud [41]. FRT modalities including fingerprint and facial recognition can be used to improve the security of voting systems [42, 43]. Fingerprints are unique to each individual, making them a reliable way to identify voters. Additionally, fingerprint recognition is a relatively non-intrusive biometric

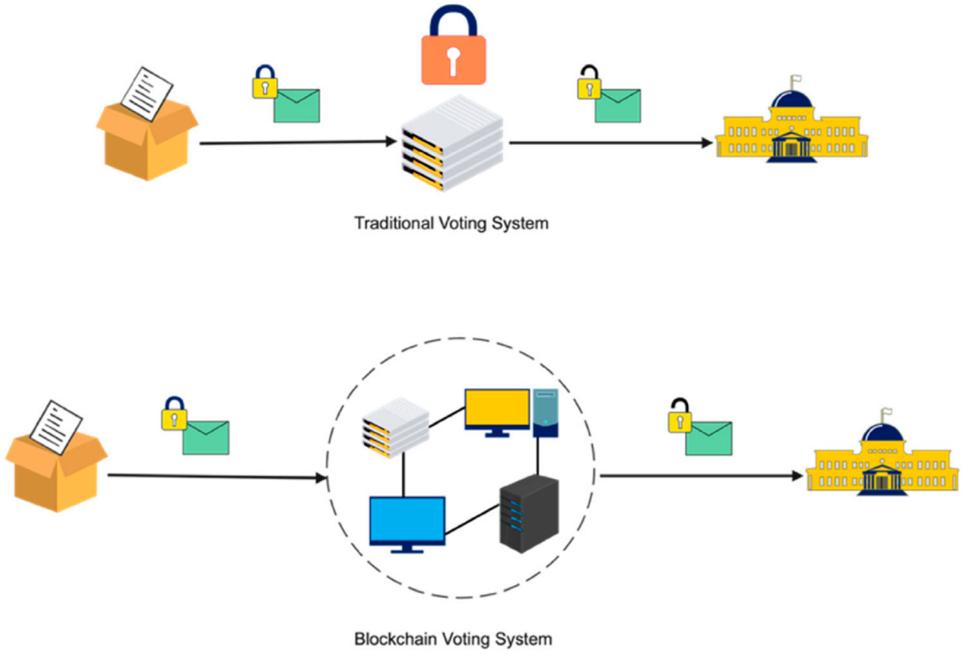


Fig. 1 Illustrates the traditional and blockchain voting system [25]

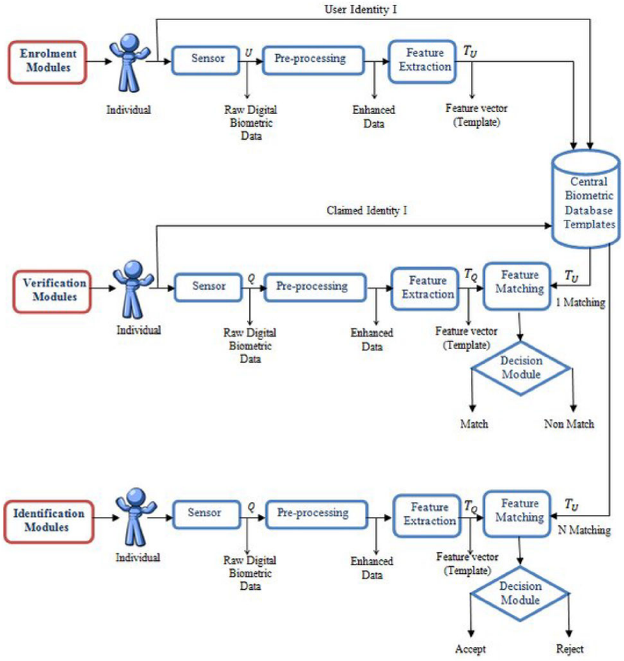


Fig. 2 Enrolment, verification, identification and matching modules of a general biometrics system [38]

technology, which can help to preserve voter privacy. The combination of FRT and fingerprint recognition can provide a high level of security for voting systems. By incorporating these technologies, we can create more transparent, secure, and efficient electoral processes (Fig. 3).

3 Related work

Blockchain technology has been proposed as a solution to address the security and transparency challenges of e-voting systems. Several studies have investigated the integration of blockchain technology into e-voting systems, with promising results. For example, Pawlak et al. [42] proposed an integrated e-voting system that effectively incorporated blockchain technology into a supervised non-remote internet voting system, thereby offering end-to-end verifiability. The system adopted the ABVS (Auditable Blockchain Voting System) for its architectural design and subsequent evaluation proved that the ABVS system outperformed other e-voting systems in terms of security and trustworthiness. Other studies [8, 43] have also utilized various blockchain frameworks such as Hyperledger Fabric and Ethereum to develop secure e-voting systems. These studies have demonstrated that blockchain technology can play a pivotal role in promoting transparency and security in public applications.

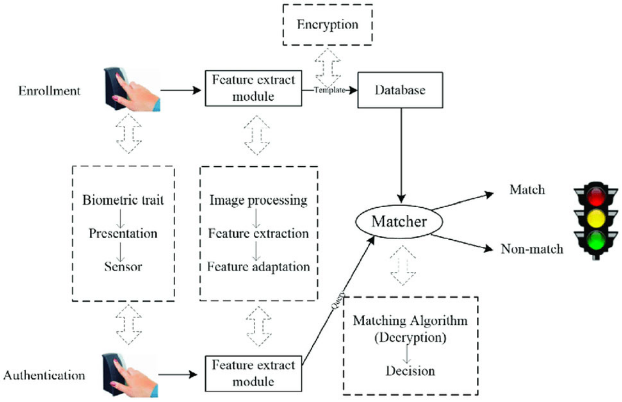


Fig. 3 An-example-of-two-stages-enrollment-and-verification-in-a-biometric-authentication-system [38]

In a different approach, researchers have proposed voting frameworks utilizing blockchain algorithms built using cryptographic techniques [44]. These researchers have demonstrated the efficiency and effectiveness of e-voting systems and the potential of significantly improving electronic voting through the application of blockchain [45, 46]. A recent study by Jafar et al. [25] conducted an in-depth investigation of conventional and blockchain-based voting systems, examining the present state of blockchain-oriented voting research. The study revealed that blockchain technology could potentially address and resolve many of the issues that currently hinder transparency in our election system. However, the researchers concluded that to develop a viable blockchain-based electronic voting system, the security of remote participation needs to be ensured, and transaction speed must be optimized for scalability. It was clear that the existing frameworks require significant enhancements for efficient integration into voting systems.

Blockchain technology has also been proposed as a solution to address the security and privacy challenges of healthcare data systems. Misic et al. [47] outlined an architecture for a blockchain-centric healthcare information system, with a focus on block validation. Their method employed collective signatures initiated by a pre-identified leader and carried out by a group of witnesses. Through the use of a Block Validation and Leader Selection Algorithm, the authors demonstrated that the application of blockchain in EHR/PHR systems resulted in enhanced security compared to traditional systems. In a related study, Faruk et al. [12] proposed a blockchain-based EHR data management system targeting healthcare stakeholders for efficient data storage and sharing. They leveraged the Ethereum framework for their architectural design. Their results demonstrated that blockchain-based solutions offered a secure and robust network for managing healthcare data.

These studies suggest that blockchain technology has the potential to significantly improve the security, transparency, and efficiency of e-voting and healthcare systems.

Table 1 Comparative analysis of existing electronic voting and online voting systems

Feature	Typical e-Voting systems	Proposed blockchain & biometric system
Authentication	Often relies on traditional ID checks, PINs or one-time tokens	Uses biometric modalities (fingerprint, facial recognition) for robust voter authentication
Data Integrity	Relies on central databases which can be vulnerable to tampering	Blockchain ensures a tamper-evident, transparent, and decentralized record of all votes
Transparency	Limited transparency, potential for vote manipulation without detection	Leveraging the Hyperledger Fabric, the system maintains a transparent and immutable voting record
Privacy	Variable, but traditional e-Voting systems can potentially link votes to voters	Biometric data ensures authentication without necessarily linking identity to a specific vote, enhancing voter privacy
Scalability	Dependent on the centralized server's capacity	Blockchain allows for a distributed network that is scalable and resilient
Accessibility	Typically requires a computer or specific machines to vote	Internet-based system allowing a broader range of devices, including mobiles, to access and cast votes
Security	Vulnerable to various cyber threats due to centralized nature	Utilizes both biometric identification and blockchain for enhanced security
Trust	Trust issues persist, especially after high-profile voting irregularities	Decentralized nature of blockchain combined with biometric verification increases trust and reliability
Usability	Can be complex due to various authentication steps	Simplified by using a combination of voter ID and biometric modality (fingerprint or facial recognition)

However, further research is needed to develop and evaluate practical blockchain-based solutions for these applications.

3.1 Gap analysis and research significance

Existing e-Voting systems have made significant progress in integrating emerging technologies such as blockchain. However, these systems have not adequately addressed voter authentication and verification issues, as well as potential vulnerabilities that could allow for significant manipulations in voting outcomes. The existing research also did not focus on web-based internet voting. This gap in the literature represents a crucial area where our research seeks to make a significant contribution. We performed a comparative analysis that we illustrate in Table 1.

Our research proposes an online or internet voting (i-Voting) system that harnesses the power of blockchain technology and biometric identification techniques, specifically fingerprint and facial recognition, to create a robust and secure i-Voting system. We propose using device cameras and fingerprint sensors, readily available in most smart devices, to capture voter biometric data for authentication purposes. This approach could significantly enhance the security and trustworthiness of i-Voting by providing a highly accurate and non-invasive method for voter authentication.

The use of Hyperledger Fabric in our blockchain architecture is another key differentiator. Hyperledger Fabric is a fully permissioned network that is suitable for sensitive operations like voting. It offers flexibility, scalability, and high-degree confidentiality, making it ideal for building an advanced voting system. To ensure our system is robust, secure, and user-friendly, we will employ a rigorous evaluation process involving security testing, usability testing, and compliance testing. This testing framework is intended to detect potential vulnerabilities, assess user-friendliness, and guarantee alignment with legal and regulatory standards.

The novelty and significance of our research lie in the effective integration of biometrics with blockchain technology to address existing challenges in i-Voting systems. Our proposed system offers enhanced voter authentication and overall voting security while maintaining transparency and ease of use. Future research will focus on applying this system in real-world voting scenarios, potentially transforming the current state of democratic elections.

4 System design

The proposed system is designed to enhance the security, privacy, and transparency of online voting processes by utilizing biometric identification and blockchain technology. This design is partitioned into three primary components, including the (1) Biometric Authentication Server, (2) Blockchain Network, and (3) Voting Application, and further classified into several subsystems. The following is a detailed technical explanation of the system's architecture, components, subsystems, operation, and security measures.

4.1 System architecture

In our endeavor to revolutionize the realm of internet voting, we have meticulously crafted an innovative architectural blueprint for the i-Voting system. We adopted the principles of the 4 + 1 view model [48], this design captures the myriad facets of the i-Voting ecosystem. At the center of the proposed framework lies an ensemble of integrated components (Fig. 4):

- Biometric-integrated registration: Voters and candidates embark on their i-Voting journey with a registration system fortified with biometric authentication. Leveraging state-of-the-art facial recognition and fingerprint scanning technologies, it ensures that each individual is distinctly recognized and authenticated.
- RESTful API ballot box: Providing a real-time interactive interface, the ballot box caters to dynamic voting sessions, with live results accessible via RESTful API.
- Smart registration and authentication component: Infusing intelligence into the registration realm, this component champions seamless, secure, and swift registration and sign-in processes.
- Central server with blockchain integration: Acting as the neural center, this server interfaces with a blockchain network, establishing an immutable, transparent, and decentralized record of every vote cast.
- Vote counting server: Inheriting attributes from the central server, it ensures a tamper-proof, transparent, and expedited vote tallying process.
- Election commission oversight: The overarching authority, the Election Commission, is endowed with robust monitoring tools, ensuring that the entire electoral process remains pristine, transparent, and secure (Fig. 5).

Figure 6 provides a visual representation in the form of a UML use case diagram, highlighting the interactions and processes of the e-Voting system. The system architecture is centered around four main stakeholders: voters, candidates, observers, and the election commission. Voters can view candidate profiles, which are managed and vetted by the election commission. Before casting a vote, voters are authenticated using biometric identifiers. As the voting progresses, real-time results are displayed and are accessible via the RESTful API. Candidates go through a detailed registration process using the same RESTful API. This registration mandates biometric verification and any other criteria set forth by the election commission. Observers can monitor the voting process to ensure its integrity. They can access the voting data through the RESTful API. The Election Commission has overall responsibility for the i-Voting system. They manage the candidate registration process, authenticate voters, and tally the votes .

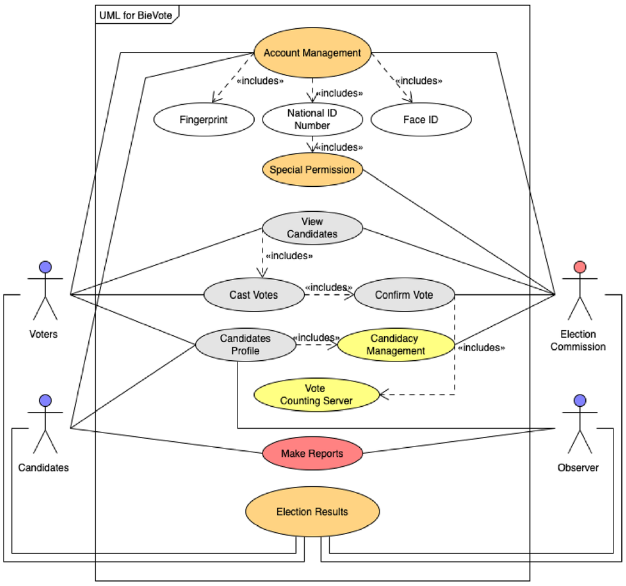


Fig. 4 UML use case diagram for e-Voting application

Figure 7 shows the process view of the e-Voting system, highlighting the real-time operations and dynamic interactions of the system components. The process begins with the biometric registration of candidates and voters. Each component’s role in data handling, transmission, and retrieval is depicted, with the central server playing a pivotal role, particularly for its integration with the blockchain database.

Figure 8 illustrates that the e-Voting system can be broadly divided into four stages: biometric-based login/registration, vote casting, vote counting, and result declaration. The web application primarily emphasizes biometric identification techniques, although there is a provision for using a national ID card (NID). However, this is secondary to the biometric methods and is subject to administrative approval. After logging in using biometrics, voters cast their votes based on their designated regions. Once the voting phase is over, repeated voting is prevented. The votes are then quickly tallied, and the results are prominently displayed on the e-Voting application’s dashboard.

4.2 System component and subsystems

The proposed system provides cross-platform compatibility, seamlessly accessible via both laptops and smartphones. Structurally, it integrates three pivotal components, each further encapsulating specific subsystems:

- Biometric authentication server (biometric authentication subsystem): Situated on a fortified server, this element is pivotal in ascertaining voters’ identities using their unique biometric data. During the voting process, it refers to the stored biometric templates of registered voters for authentication, cross-referencing them with live scans. Throughout, it maintains secure communication channels with other system constituents.

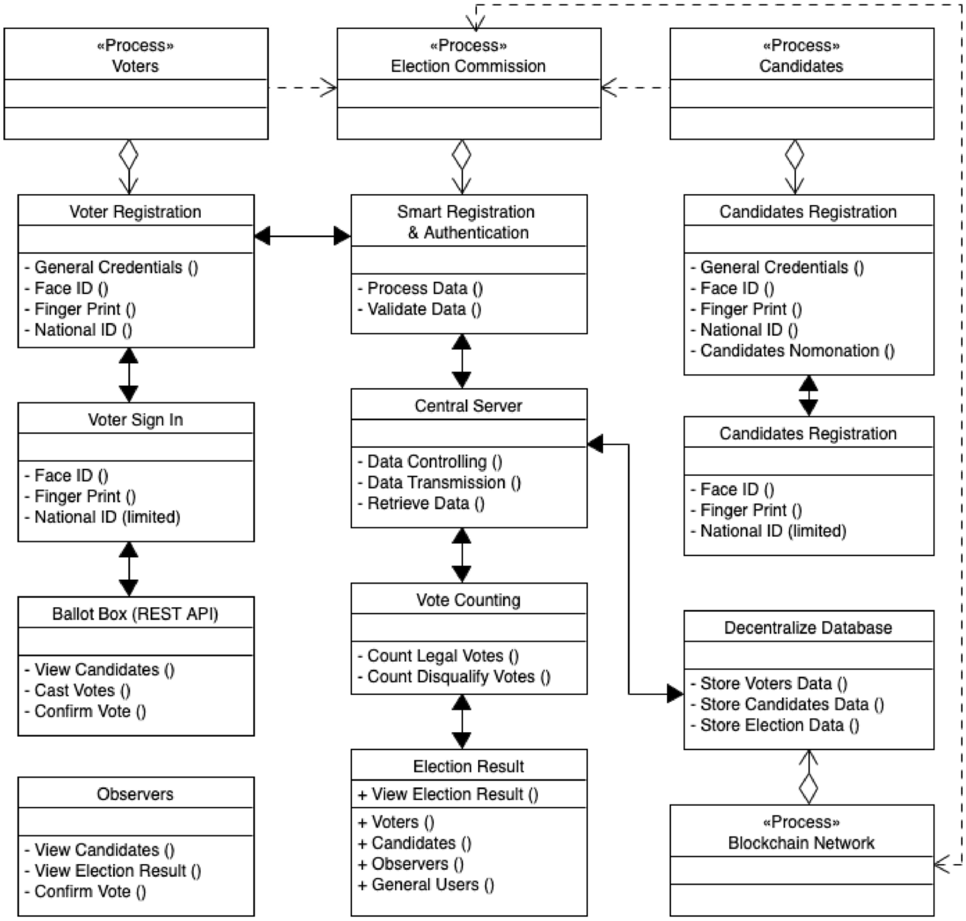


Fig. 5 Process view model of e-Voting system

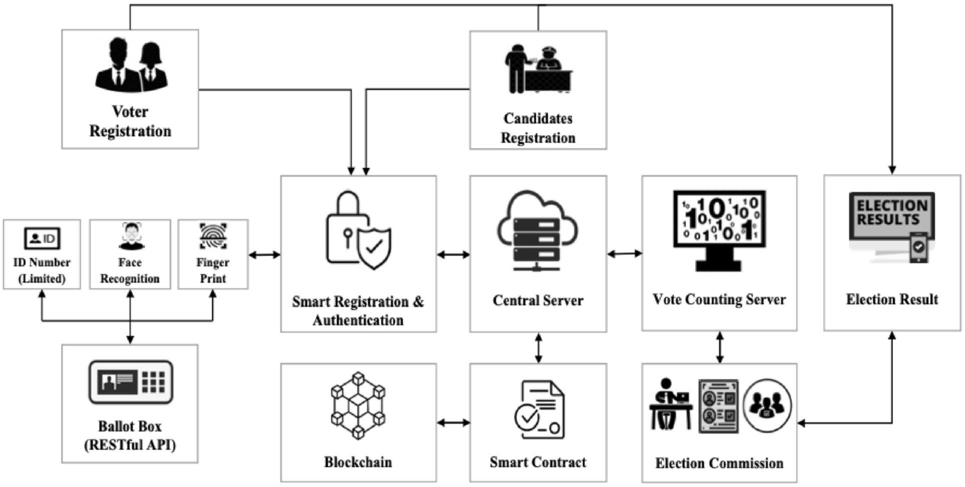


Fig. 6 Proposed architectural framework

- Blockchain network (blockchain network subsystem): This component is entrusted with the decentralized documentation and upkeep of voting records. Comprising the robust Hyperledger Fabric blockchain network, it facilitates node communication and transaction validation. Furthermore, embedded smart contracts meticulously outline the voting procedure, fortifying security and ensuring transparency at every juncture.
- Voting application (user interface subsystem): Serving as the gateway for voters, this component delivers an intuitive user interface, facilitating biometric-based identity authentication and subsequent voting. To streamline operations, it seamlessly interfaces with both the Biometric Authentication Server and the Blockchain Network, ensuring a cohesive, secure, and user-friendly voting experience.

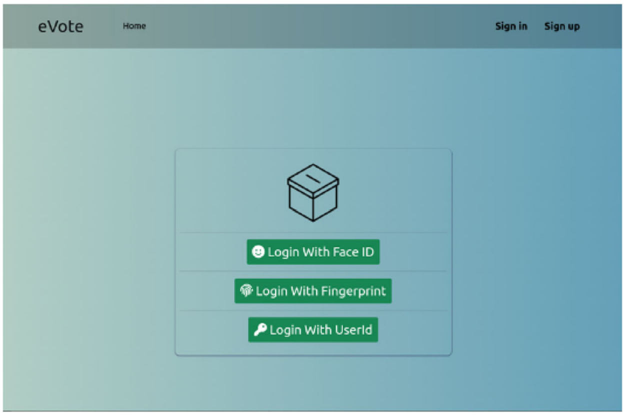


Fig. 7 Login interface of proposed system

4.3 Operation

The operation of the system involves distinct processes for smartphone and laptop access, incorporating user authentication, biometric data collection, data encoding, transaction creation, and verification.

4.3.1 Smartphone process

The smartphone process involves the following steps:

1. User authentication: Users provide their login credentials (email and password) to access the voting system.
2. Biometric collection: After authentication, users give their consent for biometric data collection. The smartphone's front-facing camera captures facial images, and the in-built fingerprint scanner captures fingerprints.
3. Data encoding: The facial image and fingerprint data are encrypted using industry-standard encryption methods.
4. Transaction creation: Encoded biometric data, along with the login credentials, are packaged into a transaction and sent to the Hyperledger Fabric network for verification.
5. Verification: The network nodes verify the transaction by comparing the encoded biometric data with the blockchain-stored data. If the data matches, the transaction is validated, granting the user access to the voting system.

4.3.2 Laptop process

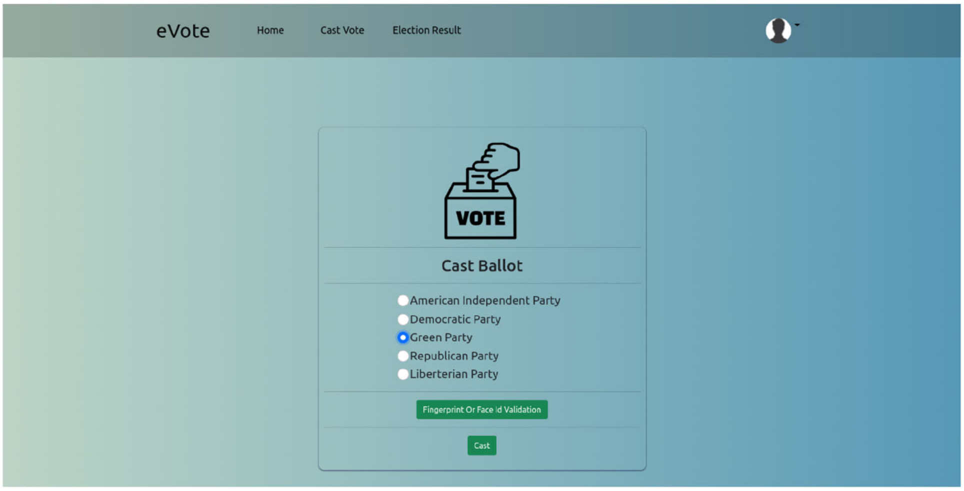
The laptop process mirrors the smartphone process, with some slight variations:

1. User authentication: Users provide their login credentials to access the voting system via a laptop.
2. Biometric collection: Upon authentication, users consent to biometric data collection. The laptop's built-in camera captures the user's facial image, and the in-built fingerprint scanner captures the fingerprint.
3. Data encoding: The facial image and fingerprint data are encrypted using industry-standard encryption methods.

4.4 Dual-factor authentication

In order to bolster the security and transparency of the voting system, the implementation of a rigorous dual-factor authentication mechanism is essential. Voters are mandated to furnish two distinct forms of verification: their unique Voter ID combined with a biometric identifier, either facial recognition or a fingerprint. By utilizing this dual-factor authentication model, the likelihood of unauthorized access or impersonation attempts is significantly curtailed. The biometric data, collected at the time of voter registration, is then securely retained within the system's database, thereby acting as a vital checkpoint to match and validate a voter's identity during the voting process.

Fig. 8 Cast Ballot interface of the proposed system



○ American Independent Party
○ Democratic Party
● Green Party
○ Republican Party
○ Liberterian Party

4.5 Biometric data collection and verification

The core of this novel system lies in its ability to collect, store, and verify biometric data, specifically facial and fingerprint recognition. Hyperledger Fabric, a highly secure blockchain network, shoulders the responsibility for the safekeeping and verification of this biometric information. Crucially, the verification process is decentralized, relying on a myriad of network nodes. This not only enhances security but also minimizes the risk of a single point of failure, ensuring consistent and reliable data verification.

4.6 Endorsement model

A crucial differentiation of our proposed architecture is the incorporation of device cameras and fingerprint sensors for voter authentication, which offer robust security due to their uniqueness across individuals. To ensure the tamper-resistant and transparent operation of our system, we employed the Hyperledger Fabric framework. Our selection of Hyperledger Fabric was deliberate due to its flexible endorsement model, which is essential for the integrity of voting transactions.

Hyperledger Fabric's endorsement model ensures that transactions are agreed upon by a specific set of endorsing peers before they are committed to the ledger. Our model adopts a majority-based endorsement policy, requiring more than half of the endorsing peers to validate a transaction for it to be considered legitimate. This ensures robustness against malicious activities. For consensus, we opted for the Raft ordering service, a crash-fault-tolerant consensus mechanism that guarantees total order delivery of transactions.

4.7 Database management

Entrusted with the vital task of managing encrypted biometric data, Hyperledger Fabric offers a database that is resistant to tampering or unauthorized modifications. By employing advanced access controls and state-of-the-art encryption techniques, the system ensures the utmost privacy and protection of user information, thus fostering trust among its users.

4.8 User interface and experience

Recognizing the diversity of its potential user base, the system boasts an intuitive and user-centric interface. This interface facilitates the seamless capture of biometric data, guides users through the login process, and enables hassle-free voting. It has been meticulously crafted to cater to a wide range of devices, from mobiles to laptops, ensuring universal accessibility.

4.9 System scalability and performance

Anticipating a surge in user registration and simultaneous voting sessions, especially during peak election periods, the system is architecturally designed for scalability. Through the integration of load balancing methodologies and refined algorithms, the system guarantees optimal performance, rapid response times, and a seamless voting experience for its users.

4.10 Security and privacy measures

Security remains paramount. The system is fortified with robust security protocols to ward off unauthorized intrusions and potential data breaches. Incorporating industry-standard encryption methodologies, secure communication channels, and stringent access controls, it presents a bulwark against threats, thereby instilling confidence among its users.

4.11 Backup and disaster recovery

Understanding the criticality of the data it handles, the system prioritizes consistent backups. Coupled with a well-orchestrated disaster recovery plan, it ensures continuity of operations even in the face of unexpected disruptions, be they technical glitches or external threats.

4.12 Compliance and legal considerations

The system not only champions security and transparency but also remains committed to legal compliance. Adhering to all pertinent regulations and privacy statutes concerning biometric data, it underscores the importance of informed consent, ensuring users are always aware and in control of how their data is utilized.

In conclusion, the proposed system combines biometric identification and blockchain technology to ensure an unparalleled level of security, privacy, and transparency in the online voting process. Its user-friendly interface and scalability make it a comprehensive solution for a reliable and trustworthy voting platform.

5 System implementation

5.1 Voting algorithm: from registration to vote casting

The following algorithm encapsulates the entire voting process from voter registration to the casting of a vote, factoring in the biometric verification mechanisms and the blockchain storage methodology:

Algorithm 1 Illustrates the general algorithm for e-Voting system

```
function RegisterVoter($voterDetails, biometricType, biometricData$)
    if $voterDetails \notin BlockchainNetwork$ then
        Store $voterDetails$ in $BlockchainNetwork$
        if $biometricType$ is “Facial” then
            Capture face using smartphone/laptop camera
        else if $biometricType$ is “Fingerprint” then
            Capture fingerprint using smartphone sensor
        end if
        Store $biometricData$ with $voterDetails$ in $BlockchainNetwork$
        return registration confirmation
    else
        return “Voter already registered.”
    end if
end function
function Authenticate-Votingr($voterID, biometricType$)
    Retrieve $storedBiometricData$ from $BlockchainNetwork$ using $voterID$
    if $biometricType$ is “Facial” then
        Capture $liveFace$ using smartphone/laptop camera
        if $liveFace$ matches $storedBiometricData$ then
            return “Authenticated”
        else
            return “Authentication failed”
        end if
    else if $biometricType$ is “Fingerprint” then
        Capture $liveFingerprint$ using smartphone sensor
        if $liveFingerprint$ matches $storedBiometricData$ then
            return “Authenticated”
        else
            return “Authentication failed”
        end if
    end if
end function
function CastVote($voterID, votingChoice$)
    if Authenticate-Votingr($voterID, biometricType$) is “Authenticated” then
        if $voterID$ has not voted in $BlockchainNetwork$ then
            Record $votingChoice$ in $BlockchainNetwork$
            return “Vote successfully cast”
        else
            return “Vote already cast”
        end if
    else
        return “Authentication failed. Vote not cast”
    end if
end function
```

The algorithm outlines the voting process for the e-Voting system, emphasizing biometric authentication. Initially, the *RegisterVoter* function ensures that a voter is not already registered within the Blockchain Network. If not, it captures and stores the voter’s details and their chosen biometric data, which can either be facial recognition or a fingerprint. The chosen biometric data is captured via a smartphone or laptop’s built-in hardware. Once registered, the *Authenticate* − *Votingr* function verifies a voter’s identity by comparing a live capture of their biometric data with the previously stored version in the Blockchain Network. This live data is acquired every time they attempt to vote, ensuring authenticity. If authenticated successfully, the *CastVote* function allows a voter to submit their choice. It first checks if a vote has been previously cast by the voter to prevent double voting. If no previous vote is found, it records the new vote and saves it to the Blockchain Network, ensuring a secure, transparent, and tamper-resistant voting record.

5.2 Algorithms for biometric data collection and storage

The algorithm's first step is to verify the provided voter ID using the 'VerifyVoter' function. Only after successful verification does the algorithm proceed with biometric data collection. Depending on the biometric type specified, it activates either the camera (for facial recognition) or the fingerprint sensor (for fingerprint data). The data captured from these sources is then returned. If the voter ID cannot be verified, the function informs the user that the verification failed.

Algorithm 2 Biometric collection and verification algorithm

```
function CollectAndVerifyBiometric($voterID, deviceType, biometricType$)
    if VerifyVoter($voterID$) then
        if $biometricType$ is "Facial" then
            if $deviceType$ is "Smartphone" OR $deviceType$ is "Laptop" then
                CaptureFace $\leftarrow$ ActivateCamera($deviceType$)
                CapturedBiometricData $\leftarrow$ CaptureFace
            end if
        else if $biometricType$ is "Fingerprint" AND $deviceType$ is "Smartphone"
then
            CaptureFingerprint $\leftarrow$ ActivateFingerprintSensor()
            CapturedBiometricData $\leftarrow$ CaptureFingerprint
        end if
        return CapturedBiometricData
    else
        return "Voter ID not verified"
    end if
end function
```

With the captured and verified biometric data, the system needs to securely store it. To ensure privacy and security, a hash of the biometric data is generated. This hash acts as a representation of the actual biometric data. Using the 'Hash' function, the algorithm generates this unique hash. With the hashed data, a transaction is then created, containing the voter's ID and the biometric hash. This transaction is sent to the Hyperledger Fabric network. If successfully processed, the algorithm confirms storage; if not, it indicates a failure.

Algorithm 3 Biometric storage algorithm

```
function StoreBiometric($voterID, capturedBiometricData$)
    $biometricHash \leftarrow$ Hash($capturedBiometricData$)
    Transaction $\leftarrow$ CreateTransaction($voterID, biometricHash$)
    Send Transaction to HyperledgerFabric
    if Transaction is successful then
        return "Biometric data stored"
    else
        return "Storage failed"
    end if
end function
```

5.3 Algorithms for voter authentication, casting, and tallying

To ensure that only valid voters cast votes, the system relies on biometric authentication. For the voter trying to cast a vote, the system retrieves the stored biometric hash from the blockchain. Depending on the biometric type (facial or fingerprint), the system captures live biometric data using the device's camera or fingerprint sensor. This freshly captured data is then hashed. If the newly generated hash matches the stored biometric hash, the voter is authenticated.

Algorithm 4 Biometric authentication

```
function AUTHENTICATE-VOTINGR(voterID, deviceType, biometricType)
    storedBiometricHash ← RetrieveFromBlockchain(voterID)
    if biometricType is “Facial” then
        liveFace ← ActivateCamera(deviceType)
        liveHash ← Hash(liveFace)
    else if biometricType is “Fingerprint” then
        liveFingerprint ← ActivateFingerprintSensor()
        liveHash ← Hash(liveFingerprint)
    end if
    if liveHash matches storedBiometricHash then
        return “Authenticated”
    else
        return “Authentication failed”
    end if
end function
```

Once authenticated, the voter can cast their vote. The system creates a transaction containing the voter’s ID and voting choice. This transaction is then sent to the Hyperledger Fabric network for secure storage. If the transaction is confirmed, the vote is considered cast successfully; otherwise, the system indicates a failure.

After voting concludes, the ‘TallyVotes’ function retrieves all votes from the blockchain. It then calculates the vote count for each choice. The final results are then published, providing transparency and assurance of integrity to all stakeholders.

Algorithm 5 Vote casting and tallying

```
function CASTVOTE(voterID, votingChoice)
    if AUTHENTICATE-VOTINGR(voterID, deviceType, biometricType) is
    “Authenticated” then
        voteTransaction ← Create-VotingTransaction(voterID, votingChoice)
        Send voteTransaction to HyperledgerFabric
        if Transaction is successful then
            return “Vote successfully cast”
        else
            return “Vote casting failed”
        end if
    else
        return “Authentication failed. Vote not cast”
    end if
end function
function TALLYVOTES
    votes ← RetrieveAllVotesFromBlockchain()
    result ← Calculate-Votings(votes)
    Publish result
    return result
end function
```

5.4 Hyperledger fabric endorsement and consensus

The Voter Authentication Process (Algorithm 6) ensures the security and legitimacy of a voter's attempt to access the system. The algorithm begins by prompting the user for their unique Voter ID and their preferred biometric modality for authentication. The chosen biometric data, either fingerprint or facial recognition, is then captured and defined as $\mathcal{B}$.

Algorithm 6 Hyperledger fabric endorsement and consensus

```
function VERIFY-ENDORSEMENT($transactionProposal, listOfPeers$)
    $endorsementCount \leftarrow 0$
    for each $peer$ in $listOfPeers$ do
        if $peer$ verifies $transactionProposal$ then
            $endorsementCount \leftarrow endorsementCount + 1$
        end if
    end for
    if $endorsementCount > \frac{length(listOfPeers)}{2}$ then
        return ORDERTRANSACTION($transactionProposal$)
    else
        return "Endorsement failed"
    end if
end function
function ORDERTRANSACTION($transactionProposal$)
    $orderingService \leftarrow$ ActivateOrderingService()    ▷ Using Raft consensus
    $orderedTransaction \leftarrow orderingService$.Order($transactionProposal$)
    if $orderedTransaction$ is not null then
        CommitToLedger($orderedTransaction$)
        return "Transaction Successful"
    else
        return "Transaction Ordering Failed"
    end if
end function
```

This biometric data, $\mathcal{B}$, is sent to a set of endorsing peers, represented as $\mathcal{E}$. Each endorsing peer individually verifies the authenticity of $\mathcal{B}$ against the stored record in the blockchain. A count, $\mathcal{C}$, keeps track of the number of endorsements.

A transaction proposal, $\mathcal{T}$, is generated only if the majority of the endorsing peers validate $\mathcal{B}$. The majority is determined as more than half of the total endorsing peers, ensuring a robust protection against potential adversarial activities. Once $\mathcal{T}$ gets the majority endorsement, it's ordered using the Raft ordering service and is committed to the ledger, post which the voter is granted access. If not, the voter's access attempt is denied.

5.5 System implementation

Our e-Voting System is an intricate melding of cutting-edge technologies and methodologies aimed at enhancing the security, privacy, and transparency of online voting. To achieve this goal, we divide the system into three distinguished layers, each contributing to its overall functionality.

- Front-End Layer: Our aim is to present a user-friendly interface to the voters. We have designed a web-based platform to offer a seamless voting experience on both smartphones and laptops. We integrated the system with essential functions to access in-built cameras and fingerprint sensors. Web-based platforms ensure a broader reach as it can cater to various operating systems without device-specific modifications.
- Application layer: Developed as a RESTful API, this layer orchestrates the entire voting process, right from registration to vote submission. Using Node.js with the Express.js framework, we have ensured this API provides platform-independent services with impeccable scalability. The combination of Node.js and Express.js provides a lightweight yet powerful platform to develop RESTful APIs. This ensures our e-Voting System can handle thousands of concurrent requests without compromising speed or security.

- Data layer: We integrated Hyperledger Fabric for our e-Voting System which provides strong security for the system. As Hyperledger Fabric is a permissioned blockchain that guarantees that once a vote is cast, it's immutable and transparent. Moreover, the blockchain structure ensures that every voter is unique, curbing the potential of dual voting.

5.5.1 Biometric data collection and verification

- Facial recognition: Tapping into the potential of OpenCV, a seasoned computer vision library, we have sculpted a system that captures faces with precision. To ensure that the face captured is genuine and not a photo or video spoof, we integrated deep-learning models. These models, trained on a predefined dataset, compare the live capture against the stored biometric data to authenticate voters accurately.
- Fingerprint authentication: Given the ubiquity of fingerprint sensors in modern devices, our e-Voting System seamlessly ties into the APIs. This ensures that when voters opt for fingerprint-based authentication, they have a swift and secure experience.

5.5.2 Development of the e-Voting system

- Voter registration (Function RegisterVoter): First and foremost, before capturing any biometric data, we query the blockchain. This is to ascertain that the voter has not previously registered. Post this verification, our system activates the requisite biometric module (facial/fingerprint) to capture the voter's unique attributes. Once captured, the voter's details, along with their biometric data, find a secure spot in our Hyperledger Fabric blockchain.
- Voter authentication (Function Authenticate-Votingr): Voter authentication is pivotal to ensure only eligible voters cast their votes. To facilitate this, our system fetches the biometric data associated with the voter ID from the blockchain. With data in tow, it activates the respective biometric module to capture live data. A deep comparison ensues between the live data and stored data. A match results in a successful authentication.
- Vote casting (Function CastVote): The culmination of our system's processes is in vote casting. Leveraging the authentication methods elucidated above, it verifies the voter's identity. Post successful authentication, the system checks the blockchain to ensure the voter hasn't previously cast their vote. If all checks pass, the voter's choice is encrypted and securely recorded on the blockchain.

6 Experiment and result

We developed an electronic voting system that is web-based and accessible using both laptops and smartphones using a RESTful API. The system allows voters to vote with verification and validation using a combination of voter ID and fingerprint or voter ID and facial recognition. All transactions are stored and verified in a blockchain network.

6.1 Experiment

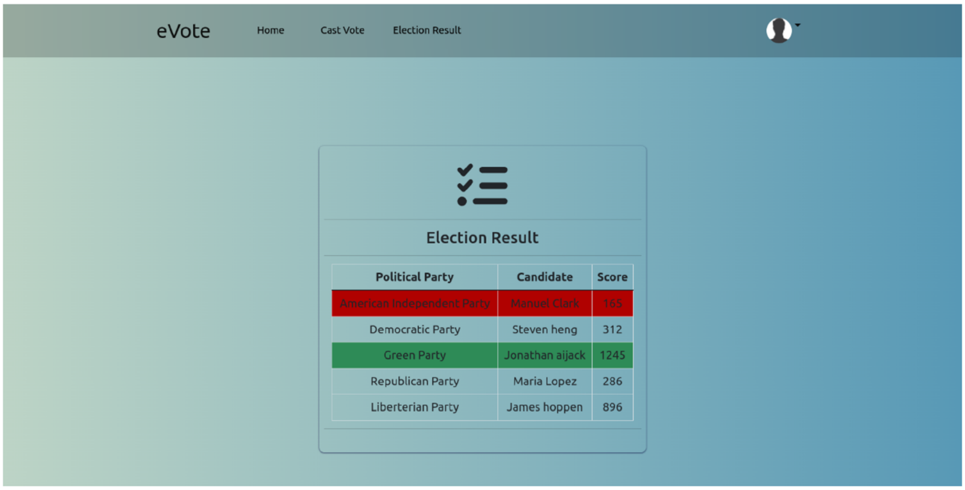
We conducted an experiment where a total of 100 voters were chosen for this experiment. We assigned a unique ID (as Voter ID) to each participant and the proposed system registered the voters with either smartphones or laptops that have both fingerprint sensors and cameras. We first captured the fingerprints and facial recognition data and stored it against the voter ID in the blockchain network (Hyperledger Fabric). Then, participants were provided with a secure link to access the voting platform.

There are different steps in the voting procedure. The voter first needed to enter their correct voter ID first. Then, the system would ask them to select either fingerprint or facial recognition for final verification and validation. If the verification and validation were correctly identified through the blockchain against the stored data, then the system would allow the voter to cast their vote. Upon successful verification against the blockchain's stored data, access to the voting portal was granted. A two-attempt system was implemented for biometric verification. Failure to authenticate on the second attempt resulted in session termination.

After voting, the system autonomously compiles the results at a predetermined time, displaying the vote count for each candidate and the respective percentages of the total votes.

6.2 Findings

The experiment results showed that the process of biometric data collection was notably efficient. Out of 100 participants, 97 successfully registered their biometrics on the first attempt. The remaining 3 participants faced minor hitches due to device compatibility issues but were able to register successfully on subsequent attempts. All of the votes were cast successfully and the results were tallied accurately. In terms of biometric verification, the system demonstrated an accuracy rate of 87%. There were 13% of instances (13 out of 100) where voters could not authenticate even after the second attempt, leading to session



Election Result

Political Party	Candidate	Score
American Independent Party	Manuel Clark	165
Democratic Party	Steven heng	312
Green Party	Jonathan aijack	1245
Republican Party	Maria Lopez	286
Liberterian Party	James hoppen	896

Fig. 9 Election result interface of the proposed system

termination. The following are some of the key findings of the experiment (Fig. 9):

- The blockchain network provided a secure and tamper-proof way to store and verify voting data. The system is also able to prevent any fraudulent voting attempts.
- The biometric verification methods were effective in preventing fraudulent voting attempts.
- The RESTful API made it easy for voters to cast their votes from their laptops or smartphones.

Overall, the experiment results were very promising and showed that the proposed system is a feasible and secure way to conduct electronic voting. Periodic checks on the blockchain entries verified the integrity and immutability of the stored data. No discrepancies or unauthorized alterations were found during the course of the experiment, underscoring the system's resilience against potential tampering. In addition to the findings mentioned above, the experiment also revealed some of the following limitations of the system:

- The system requires voters to have a smartphone or laptop with a fingerprint sensor and camera.
- The system requires voters to be registered with the system in advance.
- The system does not allow voters to change their votes once cast.

7 Authentication mechanism's performance

Our authentication mechanism's performance was gauged on pivotal biometric metrics, including authentication time, False Acceptance Rate (FAR), and False Recognition Rate (FRR). Table 1 elucidates these findings.

Table 2 indicates that the average authentication time for fingerprint recognition was relatively faster than that for facial recognition. The FAR for both modalities remained low, suggesting that unauthorized users were seldom granted access. However, FRR indicates a slightly higher percentage for facial recognition, implying that there were instances where legitimate users might have faced challenges during authentication.

Table 2 Biometric metrics for the proposed blockchain & biometric system

Metric	Fingerprint	Facial recognition
Authentication Time (avg.)	1.8 s	3.1 s
FAR	1.2%	2.5%
FRR	2.5%	3.0%

7.1 Analysis of intra-class variation and accuracy enhancement

Biometric technology is robust, but it inherently grapples with intra-class variation, which often leads to false positives and false negatives. Our system's accuracy rate of 87% underscores this challenge, especially given the universal importance of voting accuracy. In analyzing the false positives, we observed potential influences from varied lighting conditions, minor injuries to fingerprint regions, and even subtle differences in facial expressions or angles during facial recognition. To bolster accuracy, we can consider several proactive steps:

- Device standardization: Implementing a set of recommended devices or device specifications can mitigate compatibility-related inaccuracies.
- Advanced algorithms: Integrating machine learning-based algorithms that adapt and learn from verification attempts could significantly increase accuracy over time.

- Multi-modal biometrics: Combining multiple biometric modalities, such as facial and fingerprint recognition, for simultaneous verification can drastically reduce false positives.
- Voter Education: By educating voters on optimal conditions for biometric registration and verification, such as consistent lighting and positioning, we can ensure improved data capture.

To specifically address the concern of proxy voting, a more granular analysis of false positives is essential. We acknowledge that while the sample size of 100 participants provides insights, a larger dataset would allow for a more nuanced understanding of the system's false positives, laying the groundwork for necessary refinements.

These limitations could be addressed in future iterations of the system. For example, the system could be made to work with other biometric verification methods, such as iris scanning or voice recognition. The system could also be made to allow voters to change their votes before the voting period ends.

8 Discussion

In the realm of electoral processes, the transition from paper ballots to electronic voting marked a significant evolution. While this evolution promised increased efficiency, it brought forth its unique set of challenges, especially concerning security. The vulnerabilities of electronic systems to threats, attacks, and risks necessitate robust security integrations to maintain the democratic sanctity of the process. The inception of electronic voting was indeed to alleviate the many pitfalls of manual paper voting, such as forgeries and counting errors. Yet, despite its merits, it soon became apparent that a digital system wasn't immune to flaws.

A novel feature of e-Voting is its capacity for real-time monitoring. This is transformative as it permits all stakeholders, from voters to observers, to oversee the voting process, fortifying its credibility. By leveraging biometric technology, e-Voting's promise of heightened security and transparency becomes tangible. Additionally, the benefits of cost-efficiency and time-effectiveness that accompany online voting get accentuated.

The system addressed the challenges of both paper-based voting and conventional electronic systems. Notably, many existing online voting mechanisms remain susceptible to external threats, often lacking in reliability. e-Voting's aspiration is to craft a harmonious confluence of transparency, privacy, and security. Utilizing hyperledger fabric, the system reinforces data integrity. With the inclusion of the hash function, there's a solid encryption layer, bolstering the security apparatus and ensuring data access remains stringent, limited only to authorized entities.

Usability and accessibility are cornerstones of any successful e-voting system, ensuring a broader demographic reach and inclusion of voters from diverse backgrounds and technological aptitudes. Despite leveraging the latest in blockchain and biometric technology, our proposed i-voting system must be adaptable to different sections of society, especially for voters in remote and technologically underserved areas (e.g., villages).

While our study focused primarily on security, privacy, and transparency, it shed light on the overall usability of our model, with 88% of participants successfully casting their votes using biometric authentication. However, broader implementation in areas with limited internet infrastructure or low technological literacy still requires attention. We recognize that the efficacy of an online voting system depends not only on its technological superiority but also on its flexibility to accommodate voters from all walks of life.

For voters in remote areas such as the countryside, the system's compatibility with basic smartphones or community-based voting kiosks, combined with simplified user interfaces and localized language support, could be key to facilitating their participation. Further research will explore these facets, aiming to develop a more inclusive online voting platform that bridges the digital divide and ensures that every voter, regardless of location or technical expertise, can confidently engage in the democratic process.

With a focus on enhanced security, privacy, and transparency, the experiment validates the feasibility of integrating blockchain technology with biometric verification in the electoral process. Feedback from participants suggested that the voting process was largely user-friendly and intuitive. The average time taken to complete the voting, from accessing the link to casting the vote, was approximately 4 min. Some participants appreciated the additional layer of security offered by biometric verification. The system's result compilation was cross-checked against manual tallies for a subset of votes. The findings showed an 87% match, confirming the accuracy and reliability of the platform in counting and presenting voting results.

8.1 Scalability considerations

8.1.1 Scalability from technological aspects

While our initial experiment with a modest sample of 100 participants validated the proof of concept and ensured the foundational integrity of our system, scalability remains paramount for national elections. Hyperledger Fabric, the blockchain network we used, is renowned for its scalability and performance. It is designed to support pluggable implementations of different components and accommodate the complexity and intricacies of large-scale operations. Extrapolating our system to a national scale requires considering the following key factors:

- Distributed ledger capacity: The distributed nature of blockchain can handle vast numbers of transactions, making it suitable for extensive voter registrations and vote casts.
- Network infrastructure: To maintain system performance during the high transaction volumes typical of a national election, we would need to upgrade our infrastructure with more nodes and higher computational resources.
- Parallel processing: Parallel processing techniques and robust cloud infrastructure can enable simultaneous processing of multiple biometric authentications, ensuring minimal latency and real-time responsiveness, even during peak usage.

We acknowledge that transitioning from a pilot study to a nationwide implementation is challenging. However, the modularity and scalability potential of Hyperledger Fabric, combined with advances in cloud technology, positions our system to handle the demands of an entire country's electorate.

8.1.2 Biometric scalability in diverse populations

The promise of biometric technology for secure and efficient identification is undeniable. However, scaling its successful implementation in diverse populations presents substantial challenges. Biases inherent in algorithms, accessibility limitations, privacy concerns, and public trust barriers require careful consideration and proactive solutions. We are considering the following to address the challenges:

1. Mitigating algorithmic biases
   - Multi-modal biometric systems: We combined multiple biometric modalities such as fingerprints and facial recognition that compensate for individual limitations and strengthen inclusivity.
   - Diverse Training Data: We are considering to generate and utilize datasets that genuinely reflect the global demographic landscape in terms of age, ethnicity, and gender is crucial for training algorithms that perform accurately across populations.
2. Ensuring accessibility and inclusivity
   - Alternative authentication methods: We have designed the authentication process by combining a pattern of alternative login options, either a combination of facial recognition and NID or fingerprint and NID. Such an approach caters to individuals who lack compatible biometric features or technology access, including those with disabilities.
   - Accessibility standards: We aim to design biometric systems that adhere to accessibility standards and equal participation for all demographics.
3. Addressing data privacy and security
   - Robust data security: We considered implementing best-in-class encryption, secure storage protocols, and strict data minimization practices to safeguard biometric information with blockchain technology.
   - Transparency and user control: We would implement a clear policy for data collection and usage alongside user control over their biometric data to build trust and address privacy concerns.
4. Fostering public acceptance and trust
   - Extensive public awareness campaigns: Considering the future collaboration with election officials for real-world testing of our proposed system, we plan to educate the selected stakeholders about the benefits, security measures, and ethical considerations surrounding biometric technology fosters trust and encourages adoption.

8.2 Future research direction

While the proposed i-Voting system presents considerable advancements in the domain of online voting, there is an array of potential research trajectories that can further amplify its capabilities:

- Decentralized identity verification: Future studies can delve into leveraging decentralized identity platforms in conjunction with biometrics to further strengthen voter identity verification.
- Alternative blockchain protocols: While Hyperledger Fabric was the choice for this research, exploring other blockchain protocols might offer different benefits in terms of scalability, speed, or security.
- Voter experience enhancement: User experience research could provide insights into making the voting process more intuitive and user-friendly, encouraging broader adoption.
- Post-election audit mechanisms: Researching automatic, blockchain-based post-election audits could provide another layer of trust and verification to the process.

- Accessibility and inclusivity: Further studies can look into making the system more inclusive, catering to voters with disabilities or those who might not have ready access to sophisticated devices.
- Resilience against quantum attacks: As quantum computing evolves, it poses threats to many cryptographic methods. Researching quantum-resistant cryptographic methods for our voting system will be crucial.
- Integration with national systems: How can the e-Voting system be integrated or interfaced with existing national or regional voting systems? This would require both technical and policy-based research.

The domain of electronic voting, with the convergence of blockchain and biometrics, is teeming with possibilities. e-Voting, as a prototype, sets the stage for further innovations that can redefine the way democracies function in the digital age.

9 Conclusion

With the advancement of social digitalization, modernizing the electoral process is a necessity. Although significant effort has been made so far in the past decades that paved the transformation of paper-based voting into electronic voting. In this paper, we proposed a novel, web-based online voting system that utilizes blockchain technology and biometric identification techniques to improve the security, privacy, and transparency of elections. The system utilized Hyperledger Fabric, a permissioned blockchain, to store and maintain a secure and tamper-evident voting record. Biometric modalities including fingerprint and facial recognition are integrated for dual-factor voter authentication and security. We implemented a prototype of the system and evaluated its performance with predefined experimental settings. The results of the evaluation demonstrate that the proposed system provides seamless access to voters to conduct online voting. The experiment was conducted with 100 participants where 87% successfully registered their biometrics on the first attempt while the remaining 3% participants faced issues. In terms of biometric verification during the voting process, 88% of selected voters were able to authenticate voting. In essence, our research presents a groundbreaking blueprint, promising a future where voting is not just a right, but a seamless, secure, and transparent experience for every citizen. Future research shall be carried out that shall involve working with election officials and voters to understand their needs and requirements.

Author Contributions MJHF was the lead author and made the most significant contribution to the study. FA and MI were responsible for the Literature review and played a key role in the development of the prototype. The remaining (last two) authors are our advisors, contributed substantially to the ideation process, organizing the paper, providing feedback for improving the algorithm, and enhancing the overall quality of the manuscript. All authors thoroughly reviewed and approved the final manuscript.

Funding The authors have not disclosed any funding.

Data availability Data is not available.

Declarations

Conflict of interest The authors declare no competing interests.

References

1. Jennings, W., Wlezien, C.: The timeline of elections: a comparative perspective. Am. J. Polit. Sci. **60**, 219–233 (2016)
2. Simons, B., Jones, D.W.: Internet voting in the U.S. Commun. ACM **55**(10), 68–77 (2012). https://doi.org/10.1145/2347736.2347754
3. Kohno, T., Stubblefield, A., Rubin, A.D., Wallach, D.S.: Analysis of an electronic voting system. In: IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004, pp. 27–40 (2004). https://doi.org/10.1109/SECPRI.2004.1301313
4. Kumar, D.A., Begum, T.U.S.: Electronic voting machine—a review. In: International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME-2012), pp. 41–48 (2012). https://doi.org/10.1109/ICPRIME.2012.6208285
5. Lalitha, V., Samundeswari, S., Roobinee, R., Swetha, L.S.: Decentralized online voting system using blockchain. In: 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), pp. 1387–1391 (2022). https://doi.org/10.1109/ICAAIC53929.2022.9792791
6. Bederson, B.B., Lee, B., Sherman, R.M., Herrnson, P.S., Niemi, R.G.: Electronic voting system usability issues. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. CHI '03, pp. 145–152. Association for Computing Machinery, New York, NY, USA (2003). https://doi.org/10.1145/642611.642638
7. Zachary, G.P.: Digital manipulation and the future of electoral democracy in the U.S. IEEE Trans. Technol. Soc. **1**(2), 104–112 (2020). https://doi.org/10.1109/TTS.2020.2992666
8. Daramola, O.J., Thebus, D.: Architecture-centric evaluation of blockchain-based smart contract e-Voting for national elections. Informatics **7**, 16 (2020)

9. Hossain Faruk, M.J., Islam, M., Alam, F., Shahriar, H., Rahman, A.: Bie vote: A biometric identification enabled blockchain-based secure and transparent voting framework. In: 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA), pp. 253–258 (2022). https://doi.org/10.1109/BCCA55292.2022.9922588
10. Hossain Faruk, M.J., Subramanian, S., Shahriar, H., Valero, M., Li, X., Tasnim, M.: Software engineering process and methodology in blockchain-oriented software development: A systematic study. In: 2022 IEEE/ACIS 20th International Conference on Software Engineering Research, Management and Applications (SERA), pp. 120–127 (2022). https://doi.org/10.1109/SERA54885.2022.9806817
11. Gibson, J.P., Krimmer, R., Teague, V., Pomares, J.: A review of e-Voting: the past, present and future. Ann. Telecommun. **71**, 279–286 (2016)
12. Hossain Faruk, M.J., Shahriar, H., Valero, M., Sneha, S., Ahamed, S.I., Rahman, M.: Towards blockchain-based secure data management for remote patient monitoring. In: 2021 IEEE International Conference on Digital Health (ICDH), pp. 299–308 (2021). https://doi.org/10.1109/ICDH52753.2021.00054
13. Shivers, R., Rahman, M.A., Faruk, M.J.H., Shahriar, H., Cuzzocrea, A., Clincy, V.: Ride-hailing for autonomous vehicles: Hyperledger fabric-based secure and decentralize blockchain platform. In: 2021 IEEE International Conference on Big Data (Big Data), pp. 5450–5459 (2021). https://doi.org/10.1109/BigData52589.2021.9671379
14. Ocheja, P., Agbo, F.J., Oyelere, S.S., Flanagan, B., Ogata, H.: Blockchain in education: a systematic review and practical case studies. IEEE Access **10**, 99525–99540 (2022). https://doi.org/10.1109/ACCESS.2022.3206791
15. Agarwal, S., Haider, A., Jamwal, A., Dev, P., Chandel, R.: Biometric based secured remote electronic voting system. In: 2020 7th International Conference on Smart Structures and Systems (ICSSS), pp. 1–5 (2020). https://doi.org/10.1109/ICSSS49621.2020.9202212
16. Hossain Faruk, M.J., Saha, B., Islam, M., Alam, F., Shahriar, H., Valero, M., Rahman, A., Wu, F., Alam, Z.: Development of blockchain-based e-voting system: Requirements, design and security perspective. In: 2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 959–967 (2022). https://doi.org/10.1109/TrustCom56396.2022.00132
17. Deepika, J., Kalaiselvi, S., Mahalakshmi, S., Shifani, S.A.: Smart electronic voting system based on biometrie identification-survey. In: 2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM), pp. 939–942 (2017). https://doi.org/10.1109/ICONSTEM.2017.8261341
18. Rezwan, R., Ahmed, H., Biplob, M.R.N., Shuvo, S.M., Rahman, M.A.: Biometrically secured electronic voting machine. In: 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), pp. 510–512 (2017). https://doi.org/10.1109/R10-HTC.2017.8289010
19. Ibrahim, M., Ravindran, K., Lee, H., Farooqui, O., Mahmoud, Q.H.: Electionblock: An electronic voting system using blockchain and fingerprint authentication. In: 2021 IEEE 18th International Conference on Software Architecture Companion (ICSA-C), pp. 123–129 (2021). https://doi.org/10.1109/ICSA-C52384.2021.00033
20. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An overview of blockchain technology: Architecture, consensus, and future trends. In: 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557–564 (2017). https://doi.org/10.1109/BigDataCongress.2017.85
21. Andrian, H.R., Kurniawan, N.B., Suhardi: Blockchain technology and implementation : A systematic literature review. In: 2018 International Conference on Information Technology Systems and Innovation (ICITSI), pp. 370–374 (2018). https://doi.org/10.1109/ICITSI.2018.8695939
22. Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., Amaba, B.: Blockchain technology innovations. In: 2017 IEEE Technology & Engineering Management Conference (TEMSCON), pp. 137–141 (2017). https://doi.org/10.1109/TEMSCON.2017.7998367
23. Sunny, F.A., Hajek, P., Munk, M., Abedin, M.Z., Satu, M.S., Efat, M.I.A., Islam, M.J.: A systematic review of blockchain applications. IEEE Access **10**, 59155–59177 (2022). https://doi.org/10.1109/ACCESS.2022.3179690
24. Golosova, J., Romanovs, A.: The advantages and disadvantages of the blockchain technology. In: 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), pp. 1–6 (2018). https://doi.org/10.1109/AIEEE.2018.8592253
25. Jafar, U., Aziz, M.J.A., Shukur, Z.: Blockchain for electronic voting system-review and open research challenges. Sensors **21**, 5874 (2021)
26. Zhao, Z.: Comparison of hyperledger fabric and ethereum blockchain. In: 2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC), pp. 584–587 (2022). https://doi.org/10.1109/IPEC54454.2022.9777292
27. Foschini, L., Gavagna, A., Martuscelli, G., Montanari, R.: Hyperledger fabric blockchain: Chaincode performance analysis. In: ICC 2020-2020 IEEE International Conference on Communications (ICC), pp. 1–6 (2020). https://doi.org/10.1109/ICC40277.2020.9149080
28. Poniszewska-Marańda, A., Rojek, S., Pawlak, M.: Decentralized electronic voting system using hyperledger fabric. In: 2022 IEEE International Conference on Services Computing (SCC), pp. 339–348 (2022). https://doi.org/10.1109/SCC55611.2022.00056
29. Stan, I.-M., Barac, I.-C., Rosner, D.: Architecting a scalable e-election system using blockchain technologies. In: 2021 20th RoEduNet Conference: Networking in Education and Research (RoEduNet), pp. 1–6 (2021). https://doi.org/10.1109/RoEduNet54112.2021.9638303
30. Yuan, P., Xiong, X., Lei, L., Zheng, K.: Design and implementation on hyperledger-based emission trading system. IEEE Access **7**, 6109–6116 (2019). https://doi.org/10.1109/ACCESS.2018.2888929
31. Yamashita, K., Nomura, Y., Zhou, E., Pi, B., Jun, S.: Potential risks of hyperledger fabric smart contracts. In: 2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE), pp. 1–10 (2019). https://doi.org/10.1109/IWBOSE.2019.8666486
32. Jain, A., Hong, L., Pankanti, S.: Biometric identification. Commun. ACM **43**(2), 90–98 (2000). https://doi.org/10.1145/328236.328110
33. Dastbaz, M., Halpin, E., Wright, S.: Emerging Technologies and the Human Rights Challenge of Rapidly Expanding State Surveillance Capacities, pp. 108–118 (2013). https://doi.org/10.1016/B978-0-12-407191-9.00010-7
34. Zamir, M.A., Khan, D.A., Umar, M.S.: Secure electronic voting machine using biometric authentication. In: 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), pp. 511–516 (2022). https://doi.org/10.23919/INDIACom54597.2022.9763202
35. Sumner, S.: Biometrics and the Future, pp. 183–198 (2016). https://doi.org/10.1016/B978-0-12-803405-7.00010-2
36. Li, L., Mu, X., Li, S., Peng, H.: A review of face recognition technology. IEEE Access **8**, 139110–139120 (2020). https://doi.org/10.1109/ACCESS.2020.3011028
37. Liu, R., Liu, Y., Wang, Z., Tian, H.: Research on face recognition technology based on an improved lenet-5 system. In: 2022

International Seminar on Computer Science and Engineering Technology (SCSET), pp. 121–123 (2022). https://doi.org/10.1109/SCSET55041.2022.00036

38. Al-Shiha, A.: Biometric face recognition using multilinear projection and artificial intelligence. PhD thesis (2018)
39. Rafika, A.S., Sudaryono, Hardini, M., Ardianto, A.Y., Supriyanti, D.: Face recognition based artificial intelligence with attendx technology for student attendance. In: 2022 International Conference on Science and Technology (ICOSTECH), pp. 1–7 (2022). https://doi.org/10.1109/ICOSTECH54296.2022.9829122
40. Ali, M.M.H., Mahale, V.H., Yannawar, P., Gaikwad, A.T.: Overview of fingerprint recognition system. In: 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 1334–1338 (2016). https://doi.org/10.1109/ICEEOT.2016.7754900
41. Heiberg, S., Krips, K., Willemson, J., Vinkel, P.: Facial Recognition for Remote Electronic Voting - Missing Piece of the Puzzle or Yet Another Liability?, pp. 77–93 (2021). https://doi.org/10.1007/978-3-030-93747-8_6
42. Pawlak, M., Poniszewska-Maranda, A., Kryvinska, N.: Towards the intelligent agents for blockchain e-Voting system. Proc. Comput. Sci. **141**, 239–246 (2018). https://doi.org/10.1016/j.procs.2018.10.177
43. Buldas, A., Mägi, T.: Practical security analysis of e-voting systems. In: Proceedings of the Security 2nd International Conference on Advances in Information and Computer Security. IWSEC'07, pp. 320–335. Springer, Berlin (2007)
44. Patil, S., Bansal, A., Raina, U., Pujari, V., Kumar, R.: E-smart voting system with secure data identification using cryptography. In: 2018 3rd International Conference for Convergence in Technology (I2CT), pp. 1–4 (2018). https://doi.org/10.1109/I2CT.2018.8529497
45. Naidu, P.R., Bolla, D.R., G, P., Harshini, S.S., Hegde, S.A., Harsha, V.V.S.: E-voting system using blockchain and homomorphic encryption. In: 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), pp. 1–5 (2022). https://doi.org/10.1109/MysuruCon55714.2022.9972661
46. Uddin, M.N., Ahmmed, S., Riton, I.A., Islam, L.: An blockchain-based e-voting system applying time lock encryption. In: 2021 International Conference on Intelligent Technologies (CONIT), pp. 1–6 (2021). https://doi.org/10.1109/CONIT51480.2021.9498566
47. Mišić, V.B., Mišić, J., Chang, X.: Towards a blockchain-based healthcare information system : Invited paper. In: 2019 IEEE/CIC International Conference on Communications in China (ICCC), pp. 13–18 (2019). https://doi.org/10.1109/ICCChina.2019.8855911
48. Kruchten, P.B.: The 4 + 1 view model of architecture. IEEE Softw. **12**(6), 42–50 (1995). https://doi.org/10.1109/52.469759

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Md Jobair Hossain Faruk (Graduate Research Assistant, Member - IEEE) is a Ph.D. student in Computer Science at the New York Institute of Technology (NYIT). He is working as a Graduate Research Assistant under the guidance of Professor Jerry Cheng. His research interests lie at the intersection of machine learning and blockchain technology, with a focus on their applications in healthcare and cybersecurity. Additionally, he is passionate about refining traditional software engineering (SE) approaches for blockchain-oriented and intelligent software development, aiming to enhance the quality, safety, security, and privacy of emerging software products. Prior to joining NYIT, he completed his first year of Ph.D. education in CS and earned an MS degree in Software Engineering at Kennesaw State University. He accomplished several National Science Foundation (NSF) and National Institutes of Health (NIH) funded projects. He published memorious research papers in prestigious academic venues such as IEEE, ACM, Elsevier, and Springer Nature. His research was recognized with two Best Paper Awards and multiple NSF travel grants. Furthermore, he was fellows for two different organizations. He was a SciAuth Fellow at the National Center for Supercomputing Applications (NCSA) at the University of Urbana-Champaign and RCE's SDGs Future Fellow.

Fazlul Alam graduated with a Bachelor of Science in Computer Science and Engineering (CSE) from Daffodil International University. With a keen interest in technology and software development, he pursued a career as a software engineer. Through his expertise and dedication, he have contributed significantly to various projects in the field of software engineering. His research interest is about cyber security and block chain technology. As a software engineer, He is responsible for designing, developing, and maintaining software applications, systems, and tools. He has a strong understanding of computer science fundamentals, programming languages, and software development methodologies. He skilled in creating scalable, reliable, and efficient software that meets the needs of clients and users. His technical expertise includes proficiency in a variety of programming languages, such as Java, Python, and JavaScript, as well as knowledge of software development frameworks and tools like Angular, React, Spring Boot, and Node.js. He have experience in database design and management, API development, cloud computing, and software testing and debugging. As a driven professional, He continue to explore new avenues in software development and technological innovation, aiming to make meaningful contributions to the field and shape the future of digital democracy.