IJECBE (2025), **3**, **3**, 598–619
Received (22 April 2025) / Revised (23 July 2025)
Accepted (6 August 2025) / Published (30 September 2025)
https://doi.org/10.62146/ijecbe.v3i3.116
https://ijecbe.ui.ac.id
ISSN 3026-5258

International Journal of Electrical, Computer and Biomedical Engineering

RESEARCH ARTICLE

Modernizing Voting Systems: A Comprehensive Approach Using Blockchain, Biometrics and Zero Knowledge Proofs

Narendar Kumar[*†], Abdul Waqar[‡], Clavincy Francis Yohanes Ngantung[†], and Surendar Kumar[¶]

†Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia, Depok, Indonesia
‡Department of Computer Systems Engineering, MUET, 76062, Pakistan
¶School of Computing and Informatics, University of Louisiana at Lafayette, 70504, LA, United States
*Corresponding author. Email: narendarkumaroad@gmail.com

Abstract

This paper introduces a new voting system for in-person and remote voting with focus on security, privacy, and transparency. Countering growing electoral fraud and tampering, the system is developed on a blockchain platform for tamper-resistant, verifiable election processes. Innovations involve the application of biometric authentication to avoid double voting and identity theft, and the use of Zero-Knowledge Proofs to maintain confidentiality of votes without undermining accuracy. In contrast to traditional systems, this architecture builds voter trust by an open digital architecture that supports secure registration, voting, and result verification. The design in the system tackles contemporary electoral issues and provides a base for scalable, reliable, and accessible voting systems in the future.

Keywords: Blockchain, Hyperledger Fabric, Chaincode, Electronic Voting Machine. ZKPs, Biometric features

1. INTRODUCTION

Free and fair elections are essential to democratic societies. Yet, traditional voting systems and many Electronic Voting Machines (EVMs) face persistent issues such as vote manipulation, double voting, data breaches, and lack of transparency. These challenges have created public mistrust and highlighted the urgent need for secure, transparent, and reliable electoral processes [1][2].

To address these vulnerabilities, recent studies emphasize the potential of blockchain technology— especially its core attributes of decentralization, immutability, and transparency—in improving voting systems [3]. Among various platforms, Hyperledger Fabric stands out due to its enterprise-grade privacy controls, modular architecture, and support for smart contracts (chaincode) that enable automated and auditable processes such as voter registration, vote casting, and result verification [4]. Despite its advantages, existing blockchain-based voting systems remain susceptible to identity fraud and do not fully ensure voter anonymity. This paper proposes a novel integration of two key technologies—ZeroKnowledge Proofs (ZKPs) and biometric authentication—into a Hyperledger Fabric-based e-voting framework to address these gaps.

Zero-Knowledge Proofs (ZKPs): ZKPs enable verification of a valid vote without revealing the content of the vote itself. This protects voter privacy and enhances the trust and transparency of the process by making vote validation publicly verifiable but confidential [5].

Biometric Authentication: Fingerprint and facial recognition technologies provide strong identity verification, preventing double voting and impersonation. Biometric data, when securely stored and matched, ensures that only legitimate voters can cast votes, while also improving the speed and accessibility of the voting process [6]. By combining these technologies, the proposed system enables both in-person and remote voting while maintaining high security and usability. Hyperledger Fabric's flexible and scalable architecture supports integration with modern web technologies and accommodates growing electoral demands [7].

1.1 Background

Understanding every applied technology is certainly very important because mastering one part applied is a requirement so that the process created can run as one wishes. Thus, this idea needs to be developed as there are many problems faced with the selection process in which there are moments of inadequacy from the participants involved.

Traditional Voting System Vulnerabilities—Well-known issues in traditional voting system as in "Vulnerabilities and securities in the electronic voting: a review" and discussed further in secure ballot A secure open-source e-Voting system, thus provide significant challenges that have been plaguing manual voting for years. As each of these documents put into consideration together, it portrays multidimensional threats of the traditional voting system. This makes traditional systems extremely vulnerable to human error and alteration, something that can deeply affect the accuracy and integrity of election results. Manual vote counting, physical transportation of ballots, and insecure mechanisms to securely verify voter identities make several loose ends in vulnerability. Such vulnerabilities not only undermine the reliability of the election result but also may disenfranchise voters, both with an impact on public confidence in the democratic process[8].

Also, mechanisms that ensure transparency and verifiability are not developed enough within such systems. Inability to effectively and transparently audit the results raises the possibility of disputes in the election outcome; that in turn diminishes trust

in the electoral process even more. Physical security of urns/ballot boxes and overall secrecy of votes continue to be a source of concern as traditional methods cannot efficiently prevent unauthorized access or leaks of sensitive voter information[9] . To all these issues, by using the proposed system, it is likely to enhance participants' trust as well because all data belonging to each voter will be secure and will never be leaked.

Challenges Existing E-Voting Machines—The paper "Vulnerabilities and securities in the electronic voting: a review" found, though, that while EVMs lower some traditional vulnerabilities, they combine with new complexities in terms of data security and system integrity. More important issues in this direction pertain to the susceptibility towards software bugs, hacking, and vulnerable data transmission. This has always been because the security mechanisms have often been struggling to be in tandem with the sophisticated attacker methods, hence breaching the integrity of the vote process. However, from the foregoing, it does make the case even stronger for open-source solutions as a way of increasing transparency and trust in EVMs. It explains that without giving more meat to the arguments or explanations, it can easily mint attack soft targets, as well, which are typical in many proprietary systems yet problematic for an EVM[10].

On the other hand, Viola et al. wrote that integrating modern technology such as biometrics presented certain challenges for their study, "Enhancing Voting Security and Efficiency: An Electronic Voting Machine (EVM) System Integrated with Biometric Identifiers." Though it is the full intention to further protect the voting process by enabling more reliable authentication of voter identity, privacy and technological issues come along with it. The precise performance of biometric systems is not consistent across all systems, which may lead to a case of possible disenfranchisement through a false rejection or the ethical burden of handling and storing sensitive biometric data[11].

For such issues, the development of EVM systems is required, which will not only include developing the technical and security concerns itself but also increasing the levels of transparency and confidence of the voters[9]. The idea should be to create a voting environment where technology becomes a tool for enhancement and not to further complicate the democratic process. This would mean an effective security architecture based on transparency and verifiability, continued assurances of access and usability by all voters, and retention of a critical level of manual auditability to assure integrity in conducting the election. Encouraging cooperation with technology experts and fostering partnerships with an open-source community can result in enhanced security and confidence in the use of these systems in the electoral process[12].

Need for A Transparent Voting System—Transparency in voting systems is important for a number of reasons. First, transparency signifies that all the actions within the scope of the voting process-from registration of individual voters to the final counting of votes-are visible and verifiable by all the stakeholders without any possibility of voter identities being compromised. This visibility helps in building confidence in the presently used systems since stakeholders can verify the integrity of the electoral process independently. Also, current systems have the tendency to become 'black boxes'. [13] This could engender suspicion of manipulation and fraud because of

the lack of a clear manner in which one can ascertain that the votes were actually counted as cast. Since its very essence requires it, blockchain technology provides a decentralized ledger of transactions chronologically sorted-an ideal location for votes. Such a system is by its very nature immune to manipulation because any change in information would require an agreement on that change by all the nodes spread over the entire network-the possibility of which is almost impossible.

Furthermore, the smart contract implementation on platforms like Ethereum and Chain code connects the electoral process with a secure, transparent, and autonomous implementation [3]. In that respect, predefined conditions can be executed in such contracts without any human intervention so there is less chance of manipulation. Conversely, these contracts permit even a clear audit trail of performed actions. Hence, there is a need for an open voting system and quite urgently so. Using blockchain technology to that effect, but more specifically in Hyperledger Fabric, it is possible to come up with a voting system in which openness is not an afterthought, but an integral part. This would mainly serve to ensure that the whole process of voting is laid bare for all scrutiny, thereby in protecting democracy and strengthening it[14].

The already proven blockchain platform, Hyperledger Fabric, offers the infrastructure needed to tackle these challenges. Decentralization, transparency, and high data security are features that form a basis for the use of Hyperledger Fabric in the context of electronic voting machines in order to develop a system that actually guarantees data integrity and successfully reflects voter privacy. This therefore means that all transactions or votes written into the blockchain are unchangeable and are thus irrevocable due to its immutability and cannot be changed or deleted, and this positively implies another layer of security against manipulation and fraud[1].This research article therefore entails the incorporation of two key innovations towards ensuring that the voting process is further totally enhanced in terms of security and integrity: ZeroKnowledge Proofs and biometric features for voter identification.

Zero-Knowledge Proofs (ZKPs)—Zero-Knowledge Proofs are cryptographic methods allowing one party to prove to another that a statement is true without revealing information besides the validity of such a statement. By incorporating ZKP in our blockchain-based voting system, we will guarantee voters the confidentiality and verifiability of their votes without exposing the contents of the actual votes[6]. This will keep voters anonymous and ensure that the overall result of the election is transparent. Notwithstanding, the application of ZKPs in secure data sharing and secure authentication without revealing sensitive information of the parties involved has been identified as carrying potential security enhancements in domains as divergent as blockchain and healthcare to transportation. Zero-knowledge proofs are to be exactly utilized to ensure proof of each vote's validity while keeping the anonymity and preferences of the voters in a zero-knowledge state[15]. This provides for greater privacy and security during the voting process, and it makes it more immune to fraud and manipulation (ZKPs).

Biometric Features—The biometric authentication methods could differ, but largely are based on fingerprint recognition or facial recognition for voter identification purposes in order to enhance the voting process. This will help prevent voter fraud activities that may arise, such as double voting or even voting using stolen identities.

Biometric data ensures that all from genuine unmatched votes are cast, only adding more value to the integrity of the election. Instead, biometric systems have overwhelmingly been implemented to have a great enhancement effect on security in different applications, which includes privacy and data protection under cybersecurity[16]. Through integration of the Hyperledger Fabric with the EVM platform. Every step of the electoral process, from registration and casting of votes to the tallying of votes, is transparent and verifiable by all involved parties due to the use of chaincode, which is used in implementing smart contracts. It means that the chaincode could easily be customized to support the multiple forms of elections, given that it is based on the chaincode. For example, applying smart contracts, the voting process can be automated, so they are free from human mistakes; all the actions are logged so that one can confirm everything at any time later [17].

Besides, the system architecture will be highly scalable and stable enough to accommodate a volume of numerous transactions during the peak period of voting without necessarily failing the system and is equally secure. Confidence in this is extremely vital to ascertain that the system can handle a large voter turnout and, accordingly, the voting process proceeds without hiccups. What makes this framework of Hyperledger Fabric so modular is the extra security features and additions that can be brought in as and when required. If needs be, it means that the system is able to be resilient and adaptable to a dynamic set of threats and requirements, otherwise known as attacks[18].

Especially, it becomes significant in the provision of balancing democratic process chances for all eligible voters regardless of origin, location, or physical ability[1]. Many supported programming environments have unlimited freedom to update, modify, and upgrade in line with emerging trends in technology and electoral demands[19].

More recent work by Sharma et al. (2022) presents a blockchain-based e-voting architecture that emphasizes the use of permissioned blockchains like Hyperledger Fabric for large-scale national elections. Their work emphasizes important trade-offs between scalability and privacy and requires modular frameworks capable of supporting secure identity verification[20]. Their architecture does not, however, support ZKPs and biometric authentication, which are required to provide strong voter privacy and identity verification in rural areas. Reen et al. (2023) conducted an extensive review of some of the blockchain frameworks for e-voting systems, i.e., Ethereum, Hyperledger, and private blockchains. Their report indicates that there are several projects, but none of them can achieve a pragmatic balance among voter anonymity, verifiability, and system scalability[21]. The survey particularly identifies the privacy guaranteeing vulnerability of Ethereum's public ledger and suggests permissioned blockchains as an appropriate starting point. Our proposed framework considers this suggestion by selecting Hyperledger Fabric and augmenting it with biometric authentication and ZKPs.

A comprehensive review of over 40 blockchain e-voting proposals was carried out by Ismail et al. (2022), categorizing them according to architecture, authentication mechanisms, and performance metrics. Despite the review acknowledging growing momentum toward decentralization and automation, it identifies that the majority of the systems lack robust identity authentication mechanisms and extensive empirical

testing[22]. In contrast to this, our solution addresses these problems by employing a real-worldoriented architecture that includes strong voter authentication (biometrics), confidentiality of the vote (ZKPs), and transparency (Hyperledger).

Table 1. Summary of Literature Review on Blockchain-Based E-Voting Systems

Source / Study	Technology / Focus	Key Contribution	Limitation / Gap
Meza & Supe (2021)	Traditional & Electronic Voting	Highlights weaknesses in manual and EVM systems	Poor auditability, vulnerable to fraud
Agate et al. (2021)	Secure Ballot (Blockchain-based voting)	Open-source secure e-voting system	No biometric or ZKP integration
Wishwasara (2023)	Zero-Knowledge Proofs (ZKPs)	Reviews ZKPs for privacy in digital security	No practical implementation for voting
Kloppenburg & Van der Ploeg (2020)	Biometric Authentication	Discusses biometric tools (fingerprint, facial) for ID verification	Privacy and ethical concerns
Viola et al. (n.d.)	EVM + Biometrics	Explores biometric integration into voting systems	Performance inconsistencies, risk of false rejections
Hartono & Kusumastuti (2023)	Blockchain in Elections	Describes potential of blockchain to combat election fraud	Lacks detailed architecture
Sharma et al. (2022)	Permissioned Blockchain Voting	Discusses scalability, privacy tradeoffs, and architecture for national voting systems	Emphasizes privacy but lacks biometric/ZKP fusion
Reen et al. (2023) [E-Voting Meets Blockchain]	Blockchain Voting Survey	Extensive survey comparing blockchain platforms (e.g., Ethereum, Hyperledger) for voting applications	Survey only; no proposed integrated framework
Ismail et al. (2022) [Analysis of Blockchain...]	Systematic Literature Review on Blockchain for Voting	Synthesizes 40+ blockchain voting solutions and classifies by architecture, security, and performance	No empirical testing; gaps in identity verification methods
This Paper	Hyperledger Fabric + ZKP + Biometric Authentication	Integrates blockchain with privacy-preserving ZKPs and biometrics to ensure voter identity and secrecy	Addresses identity fraud, privacy, and transparency simultaneously

2. Research Methodology

Based on the references provided, this is the approach to execute each logic, from the beginning to the end of the methodology.

Understanding the Component—Provided by Hyperledger Fabric at the core of our system, the distributed ledger technology creates a secure, immutable, and transparent way of record keeping. This is the underlying technology in our electronic voting system, which therefore states that a vote should not just be tamper-evident but also

verifiable by any interested party, which goes a long way in keeping the electoral process integer.

Utilizing Blockchain for Enhanced Security and Transparency—Blockchain is used to combat the inherent security flaws in e-voting systems with classic weaknesses: authorized access and alteration of votes. With the introduction of blockchain, it is guaranteed that every single transaction recorded on the ledger cannot be modified or deleted by anyone. It is this immutability that ensures such crucial trust among participants and fairness in the electoral process.

Implementing Smart Contract for Automated Processes—It simply means that smart contracts-or chaincode, as it is called in Hyperledger Fabric-can automate the electoral process right from the registration of voters to vote counting and result declaration. Smart contracts are written for automated execution on the occurrence of certain conditions, which allows very minimal manual intervention, thus averting human error and bias.

Ensuring Voter Privacy and Integrity—Ensuring privacy in any type of voting system is very crucial. The architecture cares for that where, though fraud in voter identity is eliminated, the privacy of the voter is ensured. This becomes viable by sophisticated encryption technologies securing the voting data from possible cyber threats. Along with it, anonymity is supported at places, where it becomes a must to ensure that the voter cast votes without fear of being reprisal or as a result of coercion.

Integrating Advance Technology—It makes use of modern technologies for its construction such as Docker for containerization, CouchDB for database purposes, and a collection of web technologies that include Node.js, Express.js, HTML5, CSS3, and JavaScript. This union not only makes the performance and scalability of the system more efficient but also keeps it negotiable in the dynamically changing landscape of technologies.

Accessibility and Inclusivity in Voting—Based on Hyperledger Fabric, it empowers the system to activate options for remote vote-casting without making any compromise on security. It will increase the turnout of voters. Anyway, democracy requires such inclusivity whereby participants from diversified demography and geography can easily take part in the electoral process.

Hyperledger Framework—Hyperledger Fabric makes the core of our electronic voting system. It forms the basis of f undamental technology to deal with such important security, transparency, and privacy issues at their core, which inherent in the voters. The usage of this blockchain forms a vital part of the methodology for developing overall universal rigorous electronic voting solution; all actions into the system, from voter registration to counting, are secure and absolutely credible.". Hyperledger Fabric's architecture supplies a permissioned modular blockchain platform that supports the creation and management of complex distributed ledgers in a secure and scalable environment. This will be important in our voting system, that it is possible participants in the system are verified entities only and for the satisfaction of the integrity and privacy demands of the voting process. In our system, Hyperledger Fabric uses two major functionalities.

Chaincode Deployment—In this election management use case, the smart contract feature of chaincode will be used for the creation of voter and candidate registration to

vote tallying. From this, automated management the least possible human intervention is made in the process. Reducing errors and biases during elections All the electoral processes are executed exactly as intended.

Consensus Mechanism—It is actually a form of a consensus mechanism that validates the transactions and also assures that the state of the ledger is in agreement among all the nodes in the network. This is paramount as an act to avoid fraud, and also once the votes are recorded, they cannot be altered unless a consensus is reached amongst all participating nodes.

Enhanced Security Protocols—Embedding the latest encryption technologies to ensure the highest degree of security in the transmission of data across the network, thereby ensuring that the sensitive data of voters is secured from any unwanted access and cyber threats.

Scalability and Performance—It answers the question of scalability because, with this, it allows a large number of transactions to be processed very fast and efficiently, especially where there is peak voting. It has high throughputs capacity and supports different pluggable components.

Integration With Existing Systems—The methodology also encompasses the integration of Hyperledger Fabric with existing electoral technologies, particularly Electronic Voting Machines (EVMs). This is to utilize blockchain's immutability in making these machines secure and transparent, with a verifiable audit trail of all votes cast, so that the election results represent the true will of the participants.

Addressing Election Challenges—In par with the issues outlined in our project documentation, Hyperledger Fabric addresses several critical challenges:

- Fraud Prevention: Hyperledger Fabric prevents some very common problems, such as vote manipulation and unauthorized access, by creating an immutable ledger of all transactions, hence building trust in the process of election.
- Transparency and Verifiability: All transactions occurring within the blockchain are auditable and verifiable by all its stakeholders, yet without a single breach of an individual's privacy, and this fosters further trust in the system.
- Inclusivity: Remote voting options that are facilitated with the least possible security risks allow for higher voter participation and make it easier for voters to vote anywhere, thus theoretically maximizing the chances of getting more people to vote.

3. Diagram System

As explained in the figure 1, Blockchain-Based Electronic Voting System Architecture A robust permissioned blockchain framework holds the potential to transform the landscape of electoral processes since it addresses the two most important problems in this field—trust deficit and security weaknesses— while also boosting the traditionally low voter turnout (Harpreetvirkk, n.d.). This system utilizes a distributed ledger to enable immutability and transparency, which underpins the integrity of each vote cast.

This is because the consensus protocol forms the core of the system's architecture, as it ensures that the accuracy of the ledger—across all nodes—is maintained through

the unanimous agreement of all transactions before entering the permanent record. This way, fraud is minimized, hence making each transaction record a reflection of a state that is true and unchanged. A chaincode will be deployed—a type of smart contract—to define and automate processes in a way that an election would deal with voter and/or candidate registration, taking votes, and recording votes into results that make it easy and secure against rigging.

The peer-to-peer network and ordering service underlay the system's overall infrastructure. Peers maintain the ledger and also run the chaincode, while the ordering service ensures that the sequence of transactions, and hence data across the network, is consistent and fault-free. Such a configuration absolutely ensures that increased resiliency and increased scalability are provided to the system; it should, in turn, sustain heavy transaction volumes during peak voting periods without changes. All the users interact with the help of the system through the highly interactive web application. This is designed for three major user groups: voters, candidates, and the Election Commission. All of this accesses a well-driven interface to meet their needs, be it for vote casting, campaigning, or electoral oversight. The modern web tech-stack underlying the web application and data is supported by Docker Containers, CouchDB, Node.js, Express.js, and front-end technologies: HTML5, CSS3, and JavaScript, which will ensure a seamless, secure, and responsive user experience [3]. Thus, a blockchain voting system reinforces security and transparency for the entire electoral process and restores voter confidence since every vote can be verified and is counted. Such an overall approach with election technologies represents a quantum leap in trying to assure that more reliable and democratic electoral systems be used worldwide.

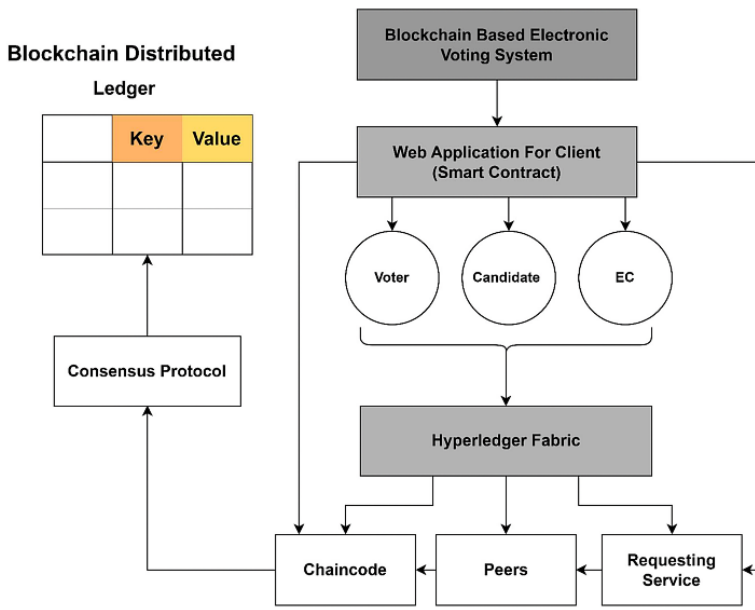

Figure 1. Blockchain-Based Architecture

Candidate—The registration of a candidate in Figure 2, through the electoral system, is a multistage, clearly defined process that is designed to enable only valid and authenticated candidates to flow into the electoral ring. This flowchart assumes that the more painful and detailed steps of candidate verification have already taken place, so it's prudent to say that any possible candidate has basically been very heavily vetted by the time they reach the final step of this process: candidate registration on the Election platform, fully verified and certified by the Election Commission. Upon completion of these preliminary verification processes, the candidates are issued with a National Identity Card, which they were to use as a means of identification at every subsequent stage they had to go through in the election process. The issuing of the NIC was to be a key benchmark point that determines that the candidate had managed to meet all previous requirements and submitted all the necessary papers to the election officials. This code is not just an identification number; it is the life and soul of the eligibility and genuineness of the candidate, and it is the key to unlock the last portal into election proceedings.

The registration process inside the Election platform, at the time of registration, has very simple steps: it asks the candidates for their NIC as well as general information. The steps are critical in that they bind verified information by the Election Commission with an applicant who is submitting a new application. The system automatically cross-checks the submitted NIC against the Election Commission's database for consistency and accuracy. Should there be the slightest of discrepancies in the NIC entered and the record held by the election Commission, in the past records, old records, or even intentionally bogus entries, the registration using this method will be halted immediately, and the candidacy application of the governmental official will be denied. This is the most important safeguard toward maintaining the integrity of the election process because it prevents unverified entries from proceeding further.

On the other hand, if there is a match with that in the Election Commission, the system has successfully verified the registration of the candidate. This verification shall lead the candidate to be added to the list of legally recognized candidates authorized to be voted for in the election. This is no ordinary procedural activity but the final gatekeeper that will ensure that the candidates presented are only those duly vetted and validated.

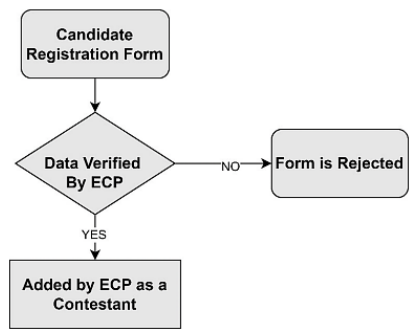

Figure 2. Candidate's portal architecture

Voters—As can be seen from Figure 3, however, the processes themselves are much more complicated than what has been presented for the candidates, part of a system that has been structured with many levels of scrutiny and user action to maintain its fairness. Also, like candidates, but at a far more critical level, all voters are given an identification called the KTP number or National ID's number, also an essential component to verify that only valid and current persons are participating in the election. This identifier not only acts as a vital protection against unauthorized access but also makes sure the voter's identity is secure during the entire poll process—such that voter's interaction can be traced and authenticated properly.

The registration of the voters is very strictly monitored and conducted by the Election Commission. The registration procedure ensures that a person submits details for registration including their number of KTP or National ID, the name, and other inclusions. This data is then compared effectively with the information contained in the centralized data bank that the Election Commission maintains with it to point out any discrepancies or errors. Found to have discrepancies, or the information given does not match with the commission database, automatically the registration is disallowed summarily. This is a very important step because it avoids the potential of being fraudulent with the election and ineligible voters. However, if everything jibes with the data of the Election Commission, that will lead the voter to be accepted, and he will be given a PIN and password. This is a critical credential, for this shall then be used later by the voter to access his/her personal dashboard on the election day.

Voter enters ballot page through an account when he registers and confirms. The ballot page is the place and center where a voter performs all the tasks of voting. From this system, every voter's vote will be well informed in a way of giving back the information on each candidate to the voter at the ballot page itself. Participants in the system can then proceed further into interacting with the system, even after they have cast a vote. This was thought of as a reassurance step for better transparency, to ensure that voters can claim with their own eyes that the vote was cast in their favor. Also, they could be eve updated by the second on the electoral results using the same platform, created to securely post results. The ability to oversee the results as they are being aggregated, therefore, makes the entire process more credible and transparent, since viewers can see the effects of their participating actions on a real-time basis.

In addition, this ability of data being presented in real-time ensures that by the time votes are put into the system, the votes are thereafter cast in stone with no way of changing, thus securing and ensuring that an election remains fair and accurate (*Supporting Private Data on Hyperledger Fabric With Secure Multiparty Computation, 2019*). Each participant is able to keep a check on the piling up or waning trend of votes in favor of each candidate, ensuring the transparency of the process and thereby identify immediately any kind of anomaly in the process or error processes occurring in vote counting.

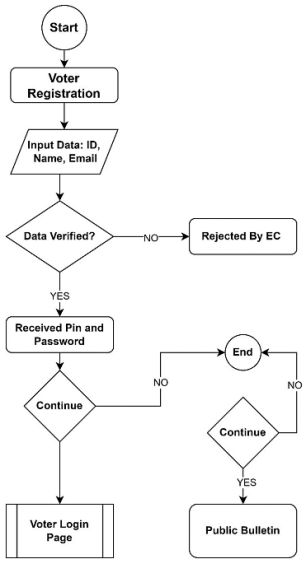

Figure 3. Voter's portal architecture for registration

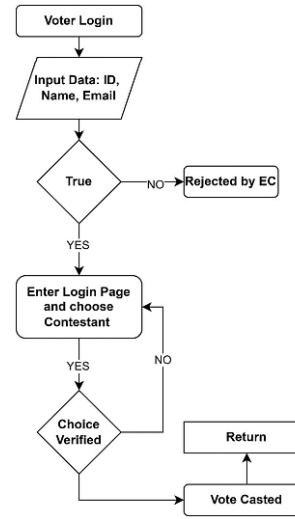

Figure 4. Voter's portal architecture for login

Indeed, the voters' logic in this system is very strong, and it was actually devised to avoid fraud, from registration straight up to the counting process whereby everything done is executed with the highest integrity and transparency. Such a technically elaborate yet effective system with a deep commitment to democratic principles is designed to ensure that every eligible voter can securely and confidently take part in the electoral process.

Voting Process—Next, the intricacies of voting are thoroughly examined and illustrated in the accompanying figure 4, The voting experience is made secure, transparent, and rapid by combining advanced technologies such as blockchain, Zero-Knowledge Proofs, and biometric authentication. It sets a time limit for the election. It makes sure that all the voting activities occur within a certain already speculated time. It brings order and structure to the entire electoral process. The same time limit will control the attempt of voting at any other time rather than the one specified. Once the time for elections has been set, then the voters activate participation in the election by registering their National ID numbers with the system. The essence of this registration is to anchor the identity of a voter so that only eligible voters will participate in the election. If this is successfully carried out, each voter will be given a Personal Identification Number and a password. Such details are always encrypted to make sure that no one will even try to alter or try a shortcut to get into the system.

Now, having done all that, the next step is where the voters log into the web application. Login details in this case include the National ID number, the PIN, and password-also encrypted for their safety. It then matches such credentials against the database where the security features of each registered voter include Inter alia, their National ID number, PIN, password and their biometric data. Such verification is therefore very vital in verifying the voter's identity and his or her eligibility. After effective validation, access is provided for the voter onto the voting page.

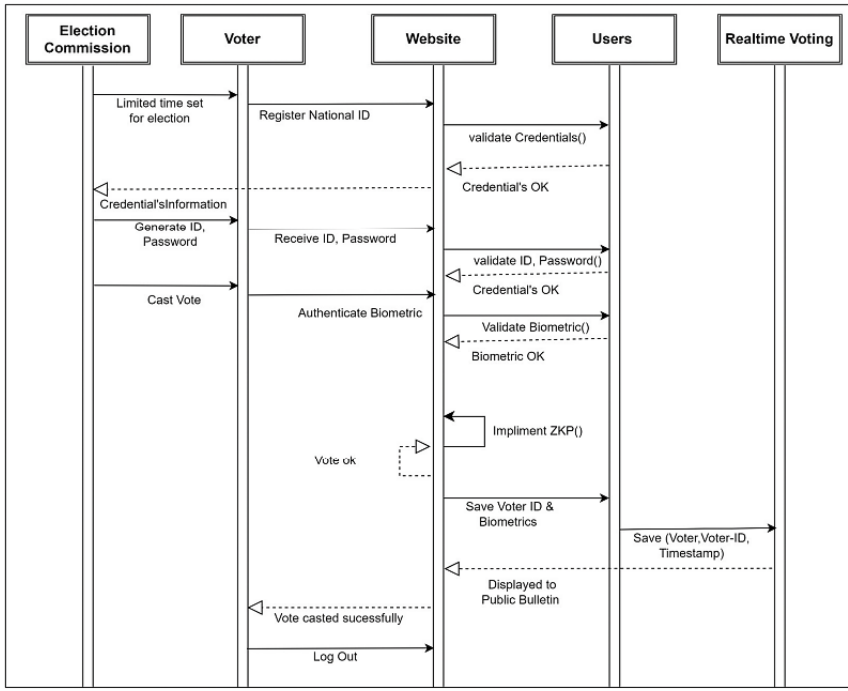

Figure 5. Represents entire voting process

There is the voting page. It contains the list of candidates. In this interface, the system obliges the voter to make an informed decision since all the information required about the candidates is given here. The voter selects the most preferable candidate in his or her eye, and it goes through another security check.

At this level, the voting system incorporates biometric verification for increased security in the electoral process. A voter is required to give, say, a biometric identifier such as a fingerprint. The system then verifies the given biometric data against the data in the database. The biometric verification component would ensure that no individual would vote with somebody else's name through identity theft; that is, every vote would be by a genuine and unique voter[7]. Biometrics further increase the security of the voting process, as any successful biometric verification provides a further strong line of verification. ZKPs encrypt the vote cast by the user, through cryptographic means, and verify the authenticity of this encrypted vote, without actually exposing the contents of the vote. Thus, the voting remains secret and the election result is correct. They may be used to ensure proper counting of votes while not eroding people's privacy with respect to voting[20]. It thereafter verifies the vote finally, after encrypting it with ZKPs. This is to verify that it is not tampered with in any way and that it is a valid vote. The final tally verification will thus guarantee a valid process to pass an election. Upon successful validation, the vote is securely encrypted and sent into the blockchain ledger along with its unique vote ID and timestamp. The blockchain ledger, built over Hyperledger Fabric gives everyone a

decentralized and transparent record of all the votes[23]. The nature inherent in the technology applied in blockchain gives an assurance that data, in this case, today's voting, cannot be altered or deleted at a later stage. This determination, thus, is very important to avoid fraud and to ensure results from the election reflect the true will of the people. The ledger through blockchain is tamper-proof, and thus the process is transparent and accountable. After a vote is securely recorded in the blockchain, the system sends a message of confirmation to a voter. The voter would get a message that his or her vote is well recorded and counted. A confirmation message at the end assures the voter that he or she has participated in the election and the security of their vote.

All of the stages in this whole process are very carefully designed to create an overall effect of maximum security, transparency and integrity. Infusion of blockchain will ensure a reliable decentralized ledger. Biometric authentication and ZKPs create additional layers of security for the protection of voter identity and vote. The system will, therefore, by realizing and exploiting the technologies to their potential, help address adeptly all of the insufficiencies in the traditional and electronic means previously discussed in this paper but will also have the ability to add a new meaning to safe, reliable, and secure electoral processes to cater for "every vote counts." It means taking care of each step of the democratic process and preserving every principle surrounding it to the best possible with integrity and trust[24].

Biometric and Zero-Knowledge Proofs (ZKPs)—On this voting machine, a novel feature has been added, representing a significant step forward in both security and user convenience. This voting machine incorporates two new features: Zero-Knowledge Proofs (ZKPs) and Biometric Authentication, enhancing security to reduce double transactions or fraudulent transactions and minimizing incorrect data usage. These added features are designed to be straightforward and user-friendly. Here are the purposes of each added feature:

Biometric Authentication—is used to ensure that only authorized voters can cast their votes on the website. This Voting Machine uses fingerprints as the voter's identity, which are already registered when voters complete their registration at the Civil Registry Service Office.

Zero-Knowledge Proofs (ZKPs)—are employed to protect voter privacy by proving the validity of a vote without revealing the voter's choice. This ensures that the vote is valid and can be verified without compromising voter anonymity. ZKPs on this Voting Machine work with the following conditions:

Correctness—For any true statement, a prover is able to convince the verifier that it is true.

Soundness—If the statement to be proven is false, then the prover can convince one that it is true only with very small probability. This helps to ensure that a fraudulent prover is unable to convince the verifier that a false statement is true.

Zero-Knowledge—In all these cases, when the statement is true, no information gained by the verifier is produced other than the validity of the statement. In other words, he only learns the validity of the statement himself. Given Below is the workflow explanation of the system diagram shown in Figure 5.

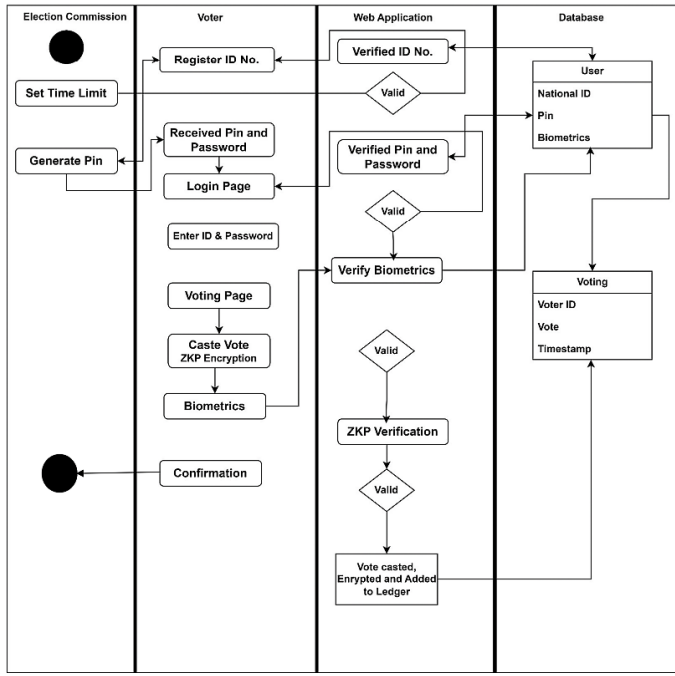

Figure 6. Sequential diagram of the E. Voting system

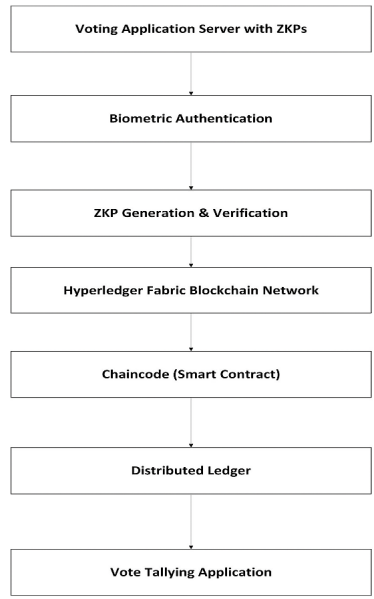

Figure 7. Integration of ZKPs and Biometric to the Voting System

4. Results And Discussion

Several results and findings are posted in this section from the period of implementation to the other core aspects of the application.

Running the Application—These are the results when the Electronic Voting System application is executed from start to finish. Figure 6 shows how the process in the voting exercise has proceeded to the Biometric entry stage, and that the results will be fetched. The participants must first register with a valid ID number before taking the process. A post registration, the participant is issued with a PIN and password. This is an important credential because much later, candidates will be chosen by vote.

While voting, following the participants' selection of their candidate of choice, the next stage is the introduction of their fingerprint. The fingerprint is a guarantee of the participant's identity, as in figure 6. The identification details are taken with the taking of civil records during the registration at the civil registry office. The biometric data is then used as a supporting document that he or she is really an Indonesian.

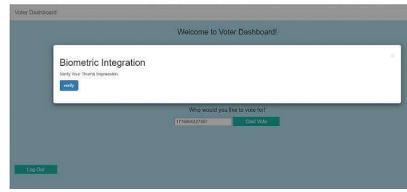

Figure 8. Voters Login Biometric System

The results are then displayed on a public bulletin once the participants are through with selecting the candidates of their choice. The system will indicate that a vote was cast and for which candidate number the vote was cast, as shown in the figure. The system is developed such that it is operated in real-time for ensuring data integrity and security. In order to guarantee anonymity, the security infrastructures also leverage blockchain technology to dislocate timestamps and votes from the network, which makes virtually impossible any attempt of data manipulation. In addition, all votes take place at the same time on the general bulletin and are displayed in real time, as can be seen in Figure 7 below.

Figure 9. Election Results

ZKPs Implementation—The use of Zero-Knowledge Proofs is further applied in the page to be referred to as the "Current Voter Turnout." This page is illustrated by the image in Figure 8, and it houses all the outputs from the algorithm that have been validated. Zero-Knowledge Proofs come into play when the voters have already cleared the biometrics validation step. These are squares where the ZKPs apply the "current voter turnout" by applying the ZKP logic at this step.

In case of any slight anomaly, the voting will not go through, and this will not be intensely included in the public bulletin. A Figure 4 Voting Process number of conditions have to be met for a vote to be accepted: the PIN and password corresponding to the number of a valid ID shall not be used before, the data shall be accurate, and the data shall not be manipulated. When all of the above conditions are met, the cast vote will be valid at its place of submission, and as Fig. illustrates, therefore, the tally at all the got places of votes could never be larger than the number of voters using this approach of ZKPs

The total of both the votes cannot exceed the number of members since ZKPs is in use. This is achieved by the following conditions.

The role of ZKP logic is to check the authenticity plus custody of any vote. It checks that all the necessary assumed identities are precisely unique with no alteration whatsoever. This implies that all the PIN and password combinations must be cross checked against the database to ensure they are not being used earlier and then condemning ragging for purposes of re-voting or voting duplication. Biometrics is another way to check the system security. If any discrepancies are found during this check, such votes will be invalidated on the spot and not included in the publicly projected tally of votes. This allows the system to be secured with a large amount of security and trustworthiness by using ZKPs. Through real-time validation and immediate summaries of the votes, transparency and accountability are ensured, and thereby it is pretty much impossible for the undertaking of any kind of fraud-perpetrating actions. The final voting results are, therefore, accurate and only indicative of legitimate votes that were cast by legitimate voters. This can be seen in Figure 8.

Comparison with Existing Paper—For example, the distinction between the earlier one and the current one is that the current process is very simple and user friendly but still secures the application. As can be seen in Table 1 below some notable differences do exist between a number of the existing study by comparing those highly simplistic to those too complicated. Comparing these two papers with that which is going to be outlined in this study, it can be seen that the output of this study exhibits a more complete set of features. The process has been made to be more concise, and more integrity, security, and transparency have been preserved. Table 1 below presents a comparative analysis that shows how the current study has greatly improved over the past studies, yet the security features are as strong and vital. The comparative elements considered include the interface design, process flow, and security protocols. Earlier instances of such system either tended to be too elementary, just sending them out into the world with not much effort, or too complicated—leaving ways to have them become practical to the users most elusive. Yet, this study balanced well between the features essential in a user-friendly way to avail a system to a more diversified audience.

All these come together to professionally balance out that users should be able to work effortlessly with the application yet be able to benefit from it to the fullest. This adds an overall feature set to a project in a scoreboard way, and it does not compromise security at any one point. We have put the right security protocols in place for us to only accord access warranted by the system to user data and to keep the sanctity of the voting process snow-white. Some of the main components further enhancing the security framework in technology for the said application to be tamper-proof and reliable include Zero Knowledge Proofs (ZKPs) and biometric verification. In addition to security and user-friendliness, the system places emphasis on the issue of transparency. The system has simply been made in a way that all the various voting transactions, complete with real-time validation and the posting of votes immediately to the public, are transparent and open to scrutiny by the stakeholders. This way, it builds the trust of the users in the system and encourages more people to participate, knowing that their votes will be rightly and securely considered.

Table 2. Represents comparison of the System and Existing Paper

Paper 1	Project	Paper 2
Voter take a Registration	Voter takes a Registration	Provide credentials from EC (username)
Verifying ID Voters	Verifying KTP Number with the Database	Registration with Username from EC
Save Data Voter	Receive Pin and Password	Verifying the username with the database
Go to the Login Page for Voting	Go to the login Page for Voting	Reset Password
Get Token	Get Token	Login using username and new password
Voting Candidates	Voting Candidates	Got token from EC
Submit Vote	Biometric Verifying	Request PIN in the application using token and password
-	ZKPs Verifying	Receive the PIN
-	Submit Vote	Vote the candidates using PIN and token
-	-	Verifying token and PIN
-	-	Submit Vote

From Table 1 above, there are some good differences noticed between the existing papers and the system currently. Paper 1 employs very simple steps, although with lapses in unique features to guarantee integrity and security, hence there are chances of double transactions and attacks. On the other hand, Paper 2 has more extensive and secure steps, but it is overly complex and unfriendly to first timers who lack prowess in social media or smartphones. This could actually serve as a drawback for

participation and a barrier to the accessibility of a system. of simple approaches found in existing papers. This innovative approach, in essence, immeasurably augments the level of accessibility of the electronic voting system and gains in reliability and trust. The aim of this system is to strike a balance in making a user-friendly system while being secure. We blend security by maintaining high levels of voting simplicity for easy use, accessibility to a wider audience of voters, and over and above, this system incorporates innovative security protocols to ensure integrity and encourage participation. In other words, this system provides the best solution because its platform is the most user-friendly and secure, taking into account all the limitations discussed above.

Latency Calculations:

i) Hyperledger Fabric Alone:
Average Block Time: 2 seconds
Calculation: For instance, if the voting system contains 10,000 transactions per block, then it would take approximately 2 seconds to create and validate a block.

Total Latency: 2 seconds

ii) Hyperledger Fabric with ZKP:
   a) Overhead of ZKP: Typically, ZKP adds certain computational delay for proof generation and verification. Assume a creation time per proof of 0.1 seconds per transaction.
   b) Average block time: Base Block Time + (ZKP Time per Transaction × Number of Transactions)

Calculations:

- ZKP Time per Transaction: 0.1 seconds
- Number of Transactions per Block: 10,000
- ZKP Overhead: 0.1 x 10,000 = 1,0000.1 \times 10,000 = 1,0000.1 x 10,000 = 1,000 seconds
- Total Block Time: 2 + 1,000 = 1,0022 + 1,000 = 1,0022 + 1,000 = 1,002 seconds
  Total Latency: 1,002 seconds

iii) Hyperledger Fabric with ZKP and Biometrics:
   a) Biometric Overhead: Biometric verification time is assumed to be 0.05 seconds per transaction.
   b) Average block time: Base Block Time + (ZKP Time per Transaction+Biometric Time Per Transaction) × (Number of Transaction)

Calculations:

- ZKP Time per Transaction: 0.1 seconds
- Biometric Time per Transactions: 0.05 seconds
- Combined Overhead: (0.1 + 0.05) x 10,000 = 1,500(0.1 + 0.05) \times 10,000 = 1,500(0.1 + 0.05) x 10,000 = 1,500 seconds
- Total Block Time: 2 + 1,500 = 1,5022 + 1,500 = 1,5022 + 1,500 = 1,502 seconds

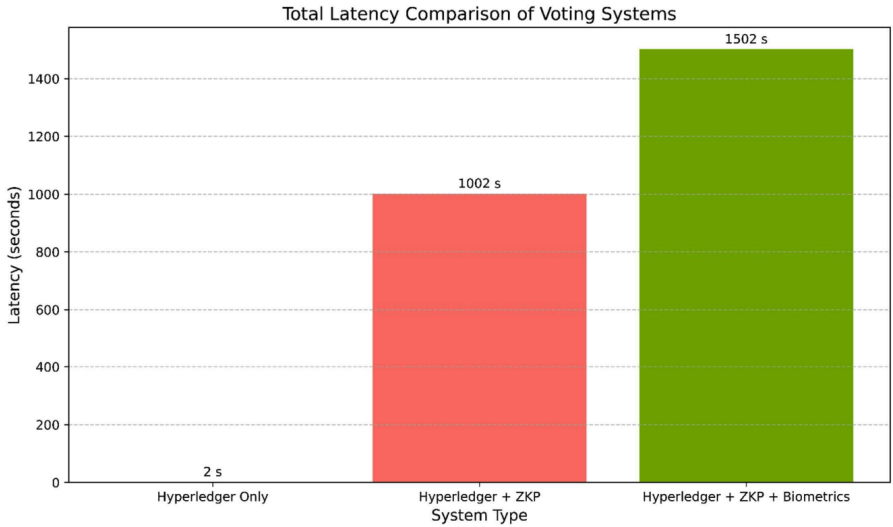

Figure 10. Represents comparison of total system latency (in seconds) for three blockchain-based electronic voting system configurations including: baseline Hyperledger Fabric, with Zero-Knowledge Proofs (ZKP), and with both ZKP and biometric authentication. The trade-off between enhanced security and latency is clearly verified.

5. Conclusion

In this study, a secure and transparent voting system was developed, one which basically addresses Election fraud and vote manipulation. The system proposed an immune-to-manipulation, tamper-proof, and auditable system for elections by leveraging the potential of Hyperledger Fabric blockchain technology. Core Hyperledger Fabric integration with chain code-based smart contracts in Electronic Voting Machines helps set the base for proper infrastructure which can help handle the whole entire electoral process. This integrated approach helps authenticate voters and candidates, provide a secure registration process, ensure transparent voting, and verifiable results, eliminating major issues uncovered in the traditional voting system. The addition of biometric features, such as fingerprints or facial recognition, and Zero-Knowledge Proofs provide more security and guarantee the integrity of the system. Zero-Knowledge Proofs enable confidentiality and correctness of voting without actually revealing the details of vote content, hence maintaining voter privacy. With the biometric identification done, a voter is confirmed using his or her ID, therefore nullifying tricky acts such as double voting and identity theft. All together, these new technologies provide a voting system that is both trustable and secure, thus living up to all present requirements for transparent and safe election processes. This project represents the foundation of when all parts of the democratic process are secure, transparent, and accessible to all eligible voters, regardless of time or place.

References

[1] I. K. Hartono and D. L. Kusumastuti. "The Blockchain Conceptual Model to Prevents Fraud and Increase Transparency In The Presidential Election In Indonesia". In: *2023 IEEE 9th International Conference on Computing, Engineering and Design (ICCED)*. IEEE, 2023, pp. 1–6.

[2] N. B. Al Barghuthi et al. "An analytical view on political voting system using blockchain technology-uae case study". In: *2019 Sixth HCT Information Technology Trends (ITT)*. IEEE, 2019, pp. 132–137.

[3] H. Harpreet Virk et al. *A Blockchain based Distributed E-Voting application implemented on Hyperledger Fabric*. Unpublished manuscript. 2020.

[4] R. Sharad Mangrulkar and P. Vijay Chavan. "Hyperledger". In: *Blockchain Essentials: Core Concepts and Implementations*. Ed. by R. S. Mangrulkar and P. Vijay Chavan. Berkeley, CA: Apress, 2024, pp. 167–201. DOI: 10.1007/978-1-4842-9975-3_5.

[5] S. Brotsis et al. "On the Security and Privacy of Hyperledger Fabric: Challenges and Open Issues". In: *2020 IEEE World Congress on Services (SERVICES)*. 2020, pp. 197–204. DOI: 10.1109/SERVICES48979.2020.00049.

[6] J. Wishwasara. *Zero Knowledge Proofs: A Comprehensive Review of Applications, Protocols, and Future Directions in Cybersecurity*. 2023. DOI: 10.13140/RG.2.2.11606.22080.

[7] S. Kloppenburg and I. Van der Ploeg. "Securing identities: Biometric technologies and the enactment of human bodily differences". In: *Science as Culture* 29.1 (2020), pp. 57–76.

[8] "Permissioned Blockchain Approach". In: *2023 OITS International Conference on Information Technology (OCIT)*. 2023, pp. 539–546. DOI: 10.1109/OCIT59427.2023.10431056.

[9] E. Z. Meza and D. S. R. Supe. "Vulnerabilities and securities in the electronic voting: a review". In: *Revista Odigos* 2.1 (2021), pp. 55–67.

[10] V. Agate et al. "SecureBallot: A secure open source e-Voting system". In: *Journal of Network and Computer Applications* 191 (2021), p. 103165.

[11] E. Z. Meza and D. S. R. Supe. "Vulnerabilities and securities in the electronic voting: a review". In: *Revista Odigos* 2.1 (2021). Duplicate of entry `meza2021vulnerabilities`, pp. 55–67.

[12] N. Ranjan. *Enhancing Voting Security and Efficiency: An Electronic Voting Machine (EVM) System Integrated With Biometric Identifiers*. Unpublished manuscript or technical report. 2023.

[13] M. Morana et al. "Secure e-Voting in Smart Communities". In: *CEUR Workshop Proceedings*. Vol. 2597. Online. 2020, pp. 1–11. URL: http://ceur-ws.org/Vol-2597/paper01.pdf.

[14] A. Riera and P. Brown. "Bringing Confidence to Electronic Voting". In: *Electronic Journal of eGovernment* 1.1 (2003). Online. URL: https://academicpublishing.org/index.php/ejeg/article/view/396.

[15] P. J., A. K. M., and S. T. "Immutable and Transparent Electronic Voting Platform Leveraging Blockchain Technology". In: *International Journal For Multidisciplinary Research* 6.3 (May 2024). DOI: 10.36948/ijfmr.2024.v06i03.19520.

[16] R. Lavin et al. *A Survey on the Applications of Zero-Knowledge Proofs*. 2024. arXiv: 2408.00243.

[17] A. Shetty et al. "Secure Vote - Augmenting Democracy with Aadhar linked Biometrics". In: *International Journal of Advanced Research in Computer and Communication Engineering* (2024). DOI: 10.17148/ijarcce.2024.134218.

[18] K. Desai, D. Gosar, and R. Pachorkar. "Blockchain based e-voting system". In: *International Journal of Engineering Applied Sciences and Technology* 7.12 (2023), pp. 21–30. DOI: 10.33564/ijeast.2023.v07i12.004.

[19] C. Jain et al. "Securing E-Voting using Hyperledger Fabric: A Permissioned Blockchain Approach". In: *2023 OITS International Conference on Information Technology (OCIT)*. 2023, pp. 539–546. DOI: 10.1109/ocit59427.2023.10431056.

[20] Maria-Victoria Vladucu et al. "E-voting meets blockchain: A survey". In: *IEEE Access* 11 (2023), pp. 23293–23308.

[21] Jun Huang et al. "The application of the blockchain technology in voting systems: A review". In: *ACM Computing Surveys (CSUR)* 54.3 (2021), pp. 1–28.

[22] Ali Benabdallah et al. "Analysis of blockchain solutions for E-voting: a systematic literature review". In: *IEEE Access* 10 (2022), pp. 70746–70759.

[23] M. L. Sowmya et al. "Blockchain Voting: A Solution to the Challenges of Traditional Electoral Systems". In: *IEEE SSIT Conference*. 2024, pp. 1–8. DOI: 10.1109/ssitcon62437.2024.10796778.

[24] F. Benhamouda, S. Halevi, and T. Halevi. "Supporting private data on hyperledger fabric with secure multiparty computation". In: *IBM Journal of Research and Development* 63.2/3 (2019), pp. 1–3.