Blockchain-Based E-Voting System with Face Recognition

V. Sathya Preiya[1], V. D. Ambeth Kumar[2], R. Vijay[3*], Vijay K.[4], N. Kirubakaran[5]

[1]Department of Computer Science and Engineering, Panimalar Engineering College, Chennai, 600123, India
[2] Department of Computer Engineering, Mizoram University, Aizawl 796004. India
[3]Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Avadi, 600062, Chennai, India
[4]Department of Computer Science and Engineering, Rajalakshmi Engineering College, Chennai, 602105, India
[5]Department of Computer Science and Engineering, Chennai Institute of Technology
Chennai. 600069, India

Emails: sathyapreiya@yahoo.com; ambeth@mzu.edu.in; vijaytamil@hotmail.com; vijayk.btech@gmail.com; drkiru70@gmail.com

Abstract

Given the increasing importance of technology in meeting human needs, its utilization has become crucial. In contemporary democracies, where public trust in governments is declining and elections play a pivotal role, the widespread adoption of technology has led to new challenges. Elections hold significant importance as they determine the future leaders of countries or organizations. However, certain computerized voting systems have faced criticism for their lack of transparency. Establishing public trust in the government is a formidable task due to the lack of transparency and susceptibility to exploitation in existing voting procedures. Both traditional and current digital voting systems are ineffective due to their vulnerabilities. The main objective is to address issues in conventional and electronic voting systems, including errors and unfairness that may arise during the voting process. Integrating blockchain technology into the electoral process can ensure fair elections and reduce unfair practices. The computerized voting methods do not meet the necessary standards for widespread usage, and the physical voting systems also face numerous issues. This underscores the importance of finding a solution to protect the democratic principles of citizens. By offering a fast and secure voting method, this system has the potential to bring about a revolutionary change in the electoral process. It could lead to higher voter participation and more accurate election results. The proposed approach presents a framework for digital voting using blockchain technology, eliminating the need for physical polling locations. Our suggested design incorporates adaptable consensus algorithms to support a scalable blockchain. Smart contracts ensure secure interactions between users and the network during transaction execution. The security aspects of the blockchain-based voting mechanism have also been addressed, including the use of cryptographic hashes for transaction encryption and prevention of 51% attacks. Furthermore, blockchain technology has been utilized to establish transaction systems throughout the voting process. Performance studies of the proposed system demonstrate its feasibility for deployment in large populations.

Keywords: Blockchain; face recognition; votes validation of votes; Tamper-proof; Deterring fraud; spoofing.

1. Introduction

Blockchain technology has the potential to greatly reduce the time and resources needed for defining polling locations, hiring staff, and addressing security concerns [1]. By conducting elections digitally on the blockchain, it is possible to save costs and decrease the chances of manipulated voting [2]. When utilized correctly, blockchain technology, along with other modern technologies, can provide immense benefits and enhanced security. It offers opportunities to enhance transaction tracing, dependability, and transparency within the voting system [3].

Doi: https://doi.org/10.54216/FPA.120104
Received: May 16, 2023 Revised: June 15, 2023 Accepted: July 07, 2023

In traditional digital voting systems, a voting device is connected to a centralized database, making it vulnerable to tampering if accessed physically. This creates a single point of failure for the entire voting system network [4]. On the other hand, an immutable blockchain would remain unaffected by a single network saboteur since the data is decentralized and continuously verified for accuracy. Even if a node were targeted in a malicious attack, only that specific node would be impacted, while the peer-to-peer network could still provide all necessary services. Blockchain technology has reached a level of security and trustworthiness that makes it suitable for serving as the secure ledger for a voting process [5]. With blockchain, there is a higher level of security and trust compared to earlier systems. This allows for the reduction of staff and security personnel required, as well as the provision of polling locations through the involvement of miners in a traditional voting mechanism [6].

The use of a tangible voting system or module, which is susceptible to hacking, is not relied upon [1]. The system's transparency is its most appealing feature as it provides individuals with confidence that their votes are being cast appropriately. Blockchain technology is more transparent and secure compared to any other database. Its implementation is being considered in critical areas such as cryptocurrency exchange, banking, healthcare, and food safety [6]. Therefore, integrating blockchain technology into the voting process ensures greater reliability, safety, and transparency compared to alternative digital voting methods. By utilizing blockchain technology, a transparent voting process that upholds voter privacy and confidence can be conducted.

In the conventional voting process, a voter needs to inform Identification Authorities (IA) of their intention to vote by sending an SMS [7]. The IA confirms the voter and registers their vote at the designated polling place. To cast their ballot, the voter must physically visit a polling place, where the chosen personnel collect the votes [8]. The staff is responsible for vote counting and reporting to higher authorities. The involvement of employees in the voting process increases the risk of human errors [3]. The authorities double-check the count before announcing the results. However, there are several vulnerabilities in this system where votes can be manipulated [9]. The staff has the ability to tamper with the votes or add fraudulent votes during the tallying process. In some cases, the authorities may declare incorrect results under the influence of a third party [10]. The voter has no assurance that their vote has been considered. The traditional voting process lacks transparency and fails to provide assurance of impartial voting. Simply digitalizing the system or using digital voting devices does not solve the problem [11]. These computerized voting devices can be manipulated by hackers, leading to interference in the voting process [12].

Therefore, there is a need for a decentralized system that can maintain data security even in the presence of a corrupt node. The aforementioned issues highlight the lack of transparency in both traditional and digital voting systems [13]. Even when authorized organizations strive to ensure fair voting within a country [7], they often face blame for any human errors or system inefficiencies. This manuscript's primary objective is to promote a voting system based on blockchain technology to prevent any illicit interference in elections and gain the trust of voters. An essential characteristic of blockchain technology is that once a node is added to the chain, it becomes immutable. This is made possible by the decentralized data storage inherent in blockchain technology. The data is copied and stored on multiple nodes within the chain, preventing simultaneous deletion of data from all nodes at once. This ensures the accuracy of the voting process. Furthermore, each node independently computes the data before combining it, reducing the computational requirements for tallying the results. Voter verification is facilitated through the utilization of Identifying Authorities for online verification. The incorporation of blockchain in the voting system aims to prevent vote manipulation and the occurrence of fraudulent votes. Each ID allows for the casting of a single vote, ensuring transparency and preventing duplicity. The implementation of blockchain safeguards the integrity of the votes stored within the system. Any unauthorized attempt to manipulate or tamper with the chain is blocked by the technology of blockchain.

By eliminating intermediaries, the voting system becomes independent, leading to cost savings and a reduced likelihood of human error. Initially, to validate its effectiveness, the traditional manual voting mechanism will be utilized alongside the blockchain-based Voting Management mechanism (VMS). Once VMS demonstrates positive outcomes, the entire voting process can transition solely to VMS. Prior to widespread implementation, a pilot program can be conducted in a local election. The subsequent section will delve into the relevant literature. Section 3 and Section 4 will provide an analysis of the existing system and the proposed blockchain-based voting system, respectively. Lastly, the discussion will encompass the performance evaluation and future enhancements for the existing system.

2. Related Work

The paper titled "Online Voting System Using Blockchain" presents a voting mechanism built on blockchain technology that aims to enhance the security and accountability of online voting. The authors propose a decentralized system to ensure the accuracy and fairness of the voting process, leveraging the immutability and transparency of blockchain technology. This technology guarantees the accurate counting of votes, prevents tampering or interference, and enables voters to cast their ballots anonymously and securely. The paper describes the system's architecture, which consists of a network of nodes that communicate with each other to validate and record votes on the blockchain. The authors also detail various procedures such as voter registration, ballot creation, ballot casting, and vote tallying, highlighting the use of smart contracts to automate the voting process

Doi: https://doi.org/10.54216/FPA.120104
Received: May 16, 2023 Revised: June 15, 2023 Accepted: July 07, 2023

and enforce secure and transparent election rules. In the final section, the article discusses the advantages of the proposed method, including increased voter turnout, improved security and transparency, and reduced costs and inefficiencies compared to conventional voting systems. The authors acknowledge that several challenges remain to be addressed before widespread adoption of the system, including legal and regulatory considerations, technical viability, and user acceptance [1].

The paper titled "A Proposal of Blockchain-Based Electronic Voting System" introduces an electronic voting system that harnesses the advantages of blockchain technology to ensure secure and transparent voting. The authors emphasize the importance of transparent and secure voting procedures and present a solution to address concerns related to voter privacy, security, and auditability. The paper provides an overview of the proposed design for the e-voting system, which encompasses a web-based front-end, a blockchain network, and a mobile application. The authors delve into the functionality of each step in the voting process, including voter registration, casting votes, and counting. They also highlight the utilization of blockchain technology to enhance the security and transparency of the voting process. The authors argue that the implementation of blockchain technology can safeguard voter privacy, ensure voting accuracy, and prevent fraudulent activities and manipulation of votes. The paper's conclusion discusses the potential benefits of the proposed approach, including heightened security and transparency, improved efficiency and accuracy, and increased voter participation and engagement. However, the authors acknowledge that before widespread adoption of the system, several challenges such as legal and regulatory considerations, technical feasibility, and user acceptance need to be addressed [2].

The paper titled "On the Design and Implementation of a Blockchain-Enabled E-Voting Application Within IoT-Oriented Smart Cities" presents a proposal for an electronic voting system that leverages the benefits of both blockchain technology and IoT-focused smart cities. The authors highlight the importance of efficient and secure voting procedures within smart cities and provide a solution to address concerns regarding privacy, security, and transparency. The paper outlines the architectural design of the proposed e-voting system, which comprises a blockchain network, an IoT device network, and a web-based front end. The authors elucidate the functionality of each step in the voting process, including voter registration, voting, and vote counting. Furthermore, the authors emphasize the use of IoT devices such as smart cards and sensors to enhance the privacy and security of the voting process. They argue that these tools can safeguard voter privacy, mitigate identity fraud, and ensure the integrity of the electoral process. The paper concludes by discussing the potential benefits of the proposed approach, including increased participation and engagement, improved efficiency and accuracy, and enhanced security and transparency. However, the authors acknowledge that several challenges, such as legal and regulatory considerations, technical feasibility, and user adoption, must be addressed before the system can be widely implemented [3].

In the paper titled "Secure E-Voting System using Blockchain Technology and Authentication via Face Recognition and Mobile OTP," the authors propose the implementation of an electronic voting system that incorporates face recognition, mobile OTP, and the security features of blockchain technology. The authors emphasize the importance of security and identification in online voting systems and provide a solution to address issues related to identity fraud and vote tampering. The paper outlines the design of the proposed e-voting system, which includes a mobile authentication system, a blockchain network, and a web-based front end. The authors provide detailed explanations of components such as voter registration, voting, and vote counting. They also highlight the use of mobile OTP and face recognition as authentication methods to ensure that only eligible voters can cast their ballots. The authors argue that these security measures can prevent identity fraud and guarantee the confidentiality and fairness of the voting process. The paper concludes by discussing potential benefits of the proposed approach, including improved security and transparency, reduced costs and inefficiencies, and increased participation and engagement. However, the authors acknowledge that several challenges, including legal and regulatory concerns, technical feasibility, and user adoption, need to be addressed before wide-scale implementation of the system can be achieved [5].

The paper titled "Towards the intelligent agents for blockchain e-voting system" proposes the use of auditable blockchain technology with intelligent agents and multi-agent systems in the voting process to enhance transparency and audibility. The authors highlight the current lack of transparency and audibility in existing voting methods and suggest that blockchain technology can address these issues. The article provides an overview of the architecture of the Auditable Blockchain Voting System (ABVS), which establishes a supervised, end-to-end verifiable system by integrating electronic voting and blockchain technology. The authors explain the role of multi-agent systems and intelligent agents in the ABVS, responsible for overseeing the voting process, verifying voter eligibility, and tallying votes. Additionally, the authors discuss security and privacy considerations in the ABVS, including the implementation of cryptographic methods to ensure data confidentiality and integrity. They argue that the utilization of blockchain technology and intelligent agents can enhance the security, privacy, and promote increased transparency and audibility in the voting process. The potential benefits of the ABVS are discussed in the conclusion of the paper, such as increased participation and engagement, improved accuracy and reliability, and enhanced trust in the voting process. However, the authors

Doi: https://doi.org/10.54216/FPA.120104
Received: May 16, 2023 Revised: June 15, 2023 Accepted: July 07, 2023

acknowledge that several challenges, including legal and regulatory aspects, technical feasibility, and user acceptance, need to be addressed before widespread adoption of the system can be achieved [6].
The study titled "Blockchain Technology Application for Electronic Voting Systems" suggests the utilization of blockchain technology for electronic voting. Alongside highlighting the importance of secure and transparent voting processes, the authors present a solution to address concerns regarding voter privacy, security, and transparency. The paper provides an overview of the proposed design for the e-voting system, comprising a web-based front-end, a blockchain network, and a mobile application. The authors discuss the functionality of each voting step, including voter registration, ballot casting, and result tallying. Emphasizing the use of blockchain technology, the authors highlight its role in ensuring the security and transparency of the voting process. They argue that blockchain technology can effectively safeguard against vote fraud and manipulation, guarantee the fairness of the electoral system, and preserve the privacy of voters. The paper's concluding section delves into the benefits of the suggested approach, including increased participation and engagement, enhanced efficiency and accuracy, and improved security and transparency. However, the authors acknowledge that several challenges related to legal and regulatory aspects, technical feasibility, and user adoption must be addressed before implementing the system on a larger scale [7].

3. Existing System

India has implemented the use of electronic voting as a method of voting. The electorate utilized electronic devices to cast their votes. The voting system comprises a comprehensive arrangement of counters and registers. The voting process itself is characterized by its simplicity and user-friendliness. It provides a multitude of advantages to the electoral commission, including enhanced flexibility, heightened security, and increased independence. However, the contemporary fast-paced lifestyle often presents challenges for individuals to allocate time for voting. Therefore, the primary objective of this essay is to conduct an in-depth examination of the electronic voting process, encompassing a meticulous analysis of the voting procedures employed not only on election day but also in subsequent stages.

4. Proposed System

In contrast to other programming frameworks where data manipulation is possible for administrators, blockchain technology is inherently immutable. When employed in a voting system, any individual with access cannot tamper with or modify the votes, ensuring their integrity. Once a node is added to the blockchain, it becomes permanent and cannot be altered or removed, regardless of the situation. In the event of an attack on a node, the neighboring nodes will detect the intrusion and restore the compromised node, thereby maintaining the immutability of the chain. This decentralized nature of blockchain technology ensures that the voting process remains unaffected even if one or more nodes are targeted or compromised, providing robustness in challenging circumstances. The proposed system involves three key participants: the voters, identification authorities, and the administration authority of the electoral commission.

4.1. Voting Procedure Architecture

The proposed system's high-level architecture is presented in Figure 1, showcasing a blockchain-based e-voting system that incorporates face recognition technology. The system demonstrates the collaborative efforts of key stakeholders, including Voters, VMS (Voting Management System), AA (Authentication Authority), and IA (Identity Authority), to facilitate various voting tasks. Each voter establishes an immediate connection with the VMS through either a mobile application or a web portal. The IA is responsible for verifying the registration of voters within the system. Once the validation process is completed, eligible voters are granted permission to vote through the application. It is crucial to ensure secure and user-friendly front-end security for the application's interface, as it serves as the initial step in the entire system process where users input their login information. The system provides equal and unrestricted access to all users during voting activities and offers traceability once a vote is cast. During the registration process, the voter submits their credentials, which are then verified by the VMS against online IA data using the provided ID information. All voter data is securely stored within the VMS.

Doi: https://doi.org/10.54216/FPA.120104
Received: May 16, 2023 Revised: June 15, 2023 Accepted: July 07, 2023

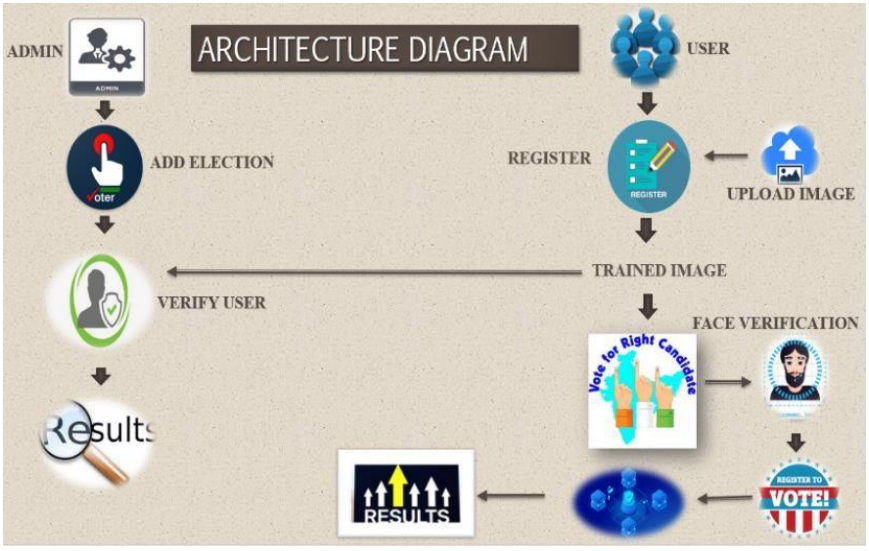

Figure 1: Blockchain-Based E-Voting System with Face Recognition

After successfully completing the registration process of the system, every voter is allocated a single Voting Coin (VC) to prevent multiple voting instances. The subsequent section provides the formal algorithm for implementing the proposed model, which integrates face recognition into a blockchain-based e-voting system. This algorithm encompasses two distinct roles: the administrator and the voter. The responsibilities of the administrator include organizing the elections, determining the election venue, managing candidate registration, and setting the election date. Conversely, the role of the voter involves registering themselves prior to voting, with face recognition utilizing the blockchain technology employed within the system.

Algorithm1: for Blockchain-Based E-Voting System with Face Recognition

Administrator

Input : Voting booth, candidates, voting districts

Output : Election_Result

Begin
1. Add Election Details
2. Start the Election
3. V_Success : = Verify _Voter// Perform user verification using blockchain
4. if V_Success then Allow voter to vote
5. else Voter is invalid and not allowed to vote
6. end if
7. Count Polled Votes
8. Declare Election _Results

End

Verify_Voter

Input: Face Image

Output: Boolean

Begin
1. User detail registration
2. Upload Voter Face Image to model
3. Model uses SHA256 algorithm
4. if match_exists then return true
5. else return false
6. end if

End Verify_Voter

Doi: https://doi.org/10.54216/FPA.120104
Received: May 16, 2023 Revised: June 15, 2023 Accepted: July 07, 2023

4.2. Workflow Of The Proposed Model

The initial phase of the process is Voter Registration, where individuals sign up to participate in voting. During this step, voters provide their name, residence, and a government-issued identification document, such as a passport or driver's license, along with other personal information. Additionally, a facial recognition system captures and records the voter's facial characteristics. Following this, in the Voter Authentication stage, the voter's identity is verified before they are allowed to cast their ballot. Their facial traits are once again captured and compared to the data obtained during the registration process. If a match is found, the voter is successfully authenticated and can proceed to the next stage. Subsequently, the Vote Casting step utilizes an electronic voting method that is based on blockchain technology, allowing the voter to cast their ballot securely.
To ensure the integrity and security of the voting process, the vote data is stored on the blockchain ledger utilizing cryptographic techniques such as the SHA256 algorithm. Following the completion of the voting period, the vote data undergoes tallying. To ensure the legality and accuracy of the results, the vote data can be verified and validated using the blockchain ledger. Lastly, the election results are announced by declaring the outcomes, which can be made publicly available on a website or communicated to relevant authorities.
It is important to note that this workflow model represents only one potential implementation of a blockchain-based electronic voting system incorporating face recognition. Depending on specific requirements and use cases, additional phases and processes may be incorporated. Additionally, rigorous testing and certification should be carried out before deploying the system in real-world scenarios.

4.3. SHA25

Blockchain-based systems, including blockchain-based e-voting systems with face recognition, commonly employ the SHA256 algorithm, which is a cryptographic hash function. In this context, each vote is assigned a digital signature or hash, which is then recorded on the blockchain ledger using the SHA256 algorithm. The workflow of a blockchain-based e-voting system integrated with face recognition technology is depicted in Figure 2. When votes are cast, they are initially transformed from a physical form into a digital representation, such as binary or hexadecimal code. Subsequently, the digital representation of each vote undergoes processing using the SHA256 algorithm, resulting in a unique hash value of fixed length. Along with the hash value, the voter's identity and any relevant additional data are appended to the blockchain record. The assumption made in this context is that a block of 8-bit values, denoted as A, B, C, D, E, F, and G, is being considered. These values are arranged in 32-bit blocks, and the method described in this scenario is used to perform operations on them. The pre-computation step is employed to store the sum value during runtime iterations. For the previous iteration of the $\boldsymbol{\partial'_k}$ value, which is referred to in equations (1), it is derived from equations (2) and (3).

$$\partial'_{\mathrm{k}} = \partial_{\mathrm{k}} + \mathrm{D_k} \quad (1)$$

$$\mathrm{E_{K+1}} = \Sigma_1(\mathrm{E_K}) + \mathrm{IM}(\mathrm{E_K}, \mathrm{F_K}, \mathrm{G_K}) + \partial'_{\mathrm{k}} \quad (2)$$

$$\mathrm{A_{K+1}} = \Sigma_0(\mathrm{A_K}) + \mathrm{HA}(\mathrm{A_K}, \mathrm{B_K}, \mathrm{C_K}) + \Sigma_1(\mathrm{E_K}) + \mathrm{IM}(\mathrm{E_K}, \mathrm{F_K}, \mathrm{G_K}) + \partial'_{\mathrm{k}} \quad (3)$$

The computed values from $\boldsymbol{A_{K+1}}$ and $\boldsymbol{E_{K+1}}$ are stored in registers, while the intermediate state is stored in the buffer using this method. In this context, IM represents the bits in the image, and HA represents the hash value utilized for generating a unique value for each user in the blockchain.

Doi: https://doi.org/10.54216/FPA.120104
Received: May 16, 2023 Revised: June 15, 2023 Accepted: July 07, 2023

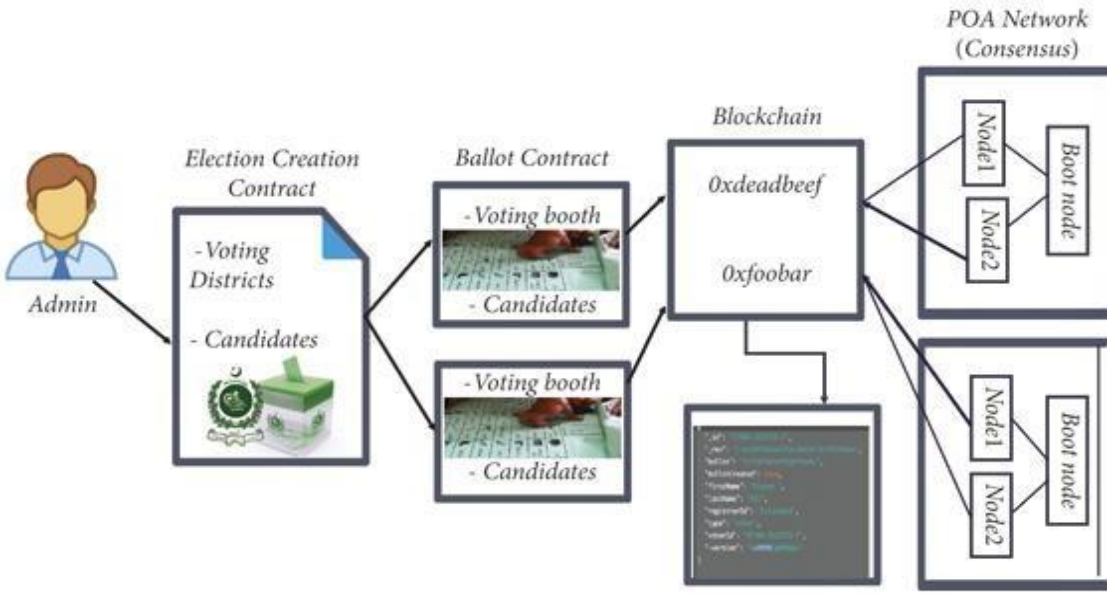

Figure 2: Workflow of Blockchain-Based E-Voting System with Face Recognition

The hash value serves as a cryptographic signature for each vote, ensuring that any tampering or modification goes undetected. Once all votes have been tallied, the SHA256 algorithm is applied to hash all the individual hash values, producing a final hash value that represents the outcome of the election. The SHA256 algorithm is widely recognized for its reliability and security, making it well-suited for utilization in face recognition-based blockchain-based electronic voting systems. By employing this technique to generate digital signatures for each vote, the system ensures a voting process that is transparent, secure, and resistant to unauthorized access.

4.4. K Nearest Neighbor (KNN)

Within blockchain-based electronic voting, the identification of voters can be achieved by analyzing their facial characteristics through the utilization of a machine learning approach known as K Nearest Neighbor (KNN). The implementation of a blockchain-based electronic voting system incorporating the K-Nearest Neighbor algorithm is depicted in Figure 3. By identifying the k-nearest data points within the training set that closely resemble the input data point, the KNN algorithm classifies the input data point based on the majority class of those identified data points. In the context of blockchain-based electronic voting with face recognition, voters can be categorized using the K Nearest Neighbor (KNN) algorithm based on their visual characteristics, such as facial shape, skin tone, and other biometric data. A training set consisting of facial characteristics along with corresponding voter identifications would be collected. When a voter intends to cast a ballot, their facial features are captured and transformed into a digital representation, either in binary code or a set of numeric values. The KNN algorithm is then applied to the digital representation of the voter's facial traits to identify the k-nearest data points in the training set that closely resemble the voter's features. Based on the majority class of those k-nearest data points, the voter is classified according to their identity.

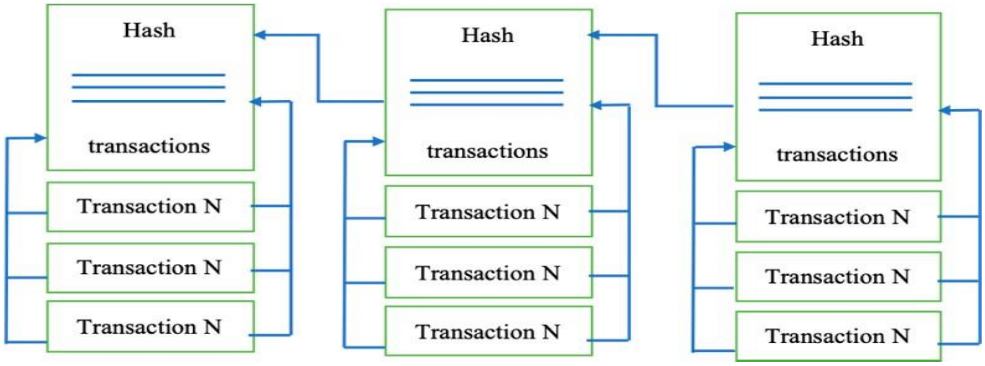

Figure 3: blockchain-based electronic voting using K-Nearest Neighbor Algorithm

Doi: https://doi.org/10.54216/FPA.120104
Received: May 16, 2023 Revised: June 15, 2023 Accepted: July 07, 2023

Figure 4 illustrates a flowchart schematic representation of the process for face recognition and authentication within the system.

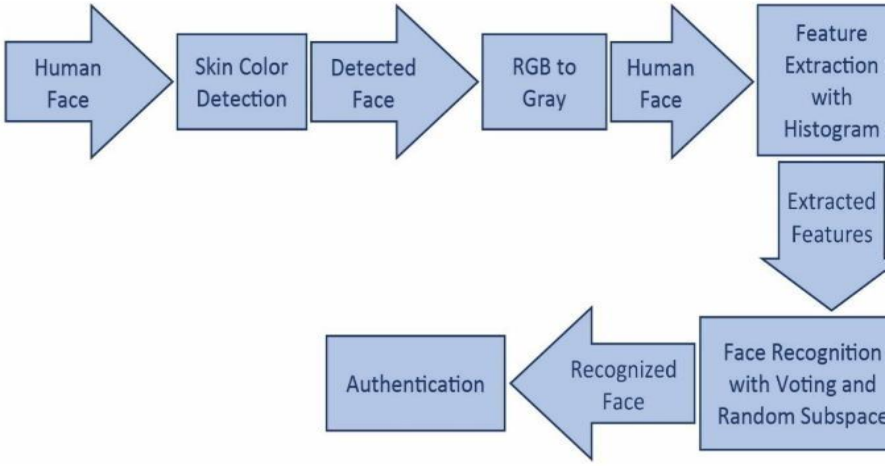

Figure 4: Flowchart Schematic representation for Face Recognition and Authentication

To ensure the confidentiality and integrity of the vote, the SHA256 algorithm or other cryptographic methods would be utilized to record the voter's vote on the blockchain ledger once their identity has been verified. In blockchain-based e-voting with face recognition, the K Nearest Neighbor (KNN) algorithm can be beneficial due to its ability to efficiently and accurately classify voters based on their facial characteristics. However, it is important to note that the accuracy of the KNN algorithm relies on the quality and quantity of the training data, as well as the selection of the value for k in the classification process. Therefore, careful consideration and rigorous testing are necessary when implementing the KNN algorithm in a blockchain-based e-voting system with facial recognition.

5. Performance Analysis

In a blockchain-based electronic voting system that incorporates face recognition, two different algorithms, namely KNN (K-Nearest Neighbors) and SHA256 (Secure Hash Algorithm 256), can be utilized. KNN is a machine learning algorithm commonly employed for facial recognition purposes, whereas SHA256 is a cryptographic hashing algorithm used to ensure the security of transactions on the blockchain.

KNN can be applied in the electronic voting system to verify the identities of voters through facial recognition. It is a widely adopted algorithm for facial identification, where the system compares the facial characteristics of an individual with those stored in a database to establish their identity. The performance of KNN is influenced by factors such as the quality and quantity of the facial database and the accuracy of the algorithm. There are several potential challenges in employing KNN for facial identification, including lighting conditions, facial expressions, and image quality. To ensure the security of transactions on the blockchain, the SHA256 cryptographic hashing method is utilized. Each transaction is assigned a unique hash value by the algorithm, which is subsequently used to verify the integrity and authenticity of the transaction. SHA256 is a widely used algorithm in blockchain systems due to its speed, security, and ability to process a large number of transactions. However, there are potential vulnerabilities associated with SHA256, such as the risk of brute force attacks and collisions, where different inputs produce the same hash value. Figure 5 provides a visual representation comparing the existing approach with the proposed approach.

Doi: https://doi.org/10.54216/FPA.120104
Received: May 16, 2023 Revised: June 15, 2023 Accepted: July 07, 2023

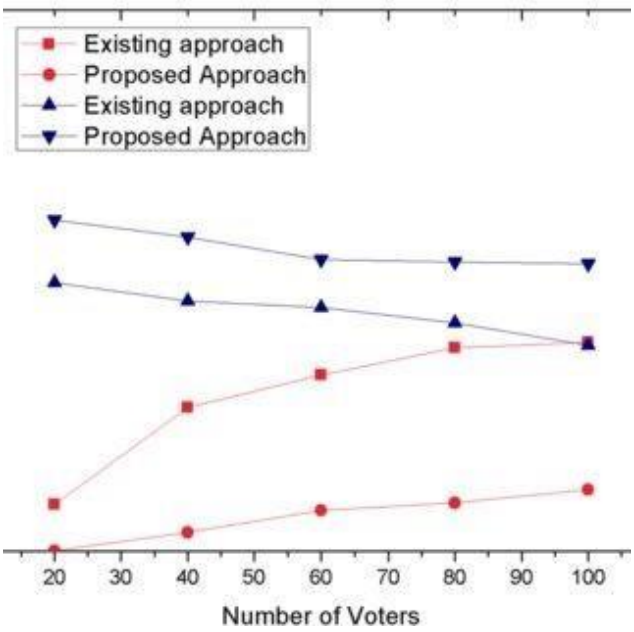

Figure 5: Graphical Representation of existing and proposed approach

The overall performance of a blockchain-based e-voting system with face recognition is influenced by various factors. These factors include the accuracy of the facial recognition system, the security strength of the hashing algorithm employed, and the effectiveness and scalability of the underlying blockchain infrastructure. The successful integration and synchronization of these elements contribute to the overall performance and reliability of the e-voting system.

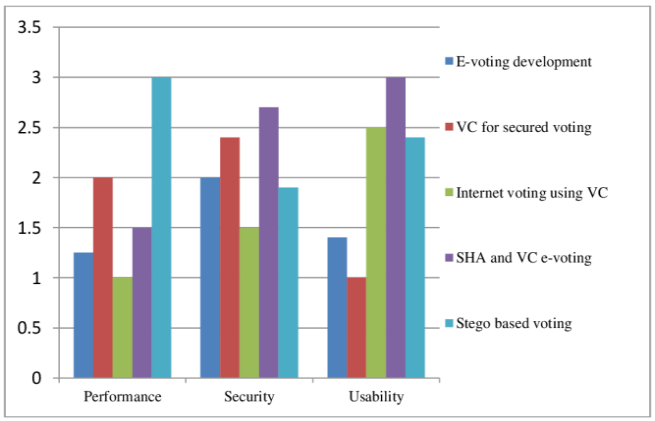

Figure 6: Relative measures of the system

A comparative evaluation of advancements in e-voting, including alternative voting algorithms, is illustrated in Figure 6. The proposed system demonstrates outstanding performance and enhanced security compared to other existing systems. Additionally, Figure 7 provides a comparative analysis between the proposed system and alternative approaches, highlighting the superior speed and cost-effectiveness of the proposed methods in contrast to alternative systems.

Doi: https://doi.org/10.54216/FPA.120104
Received: May 16, 2023 Revised: June 15, 2023 Accepted: July 07, 2023

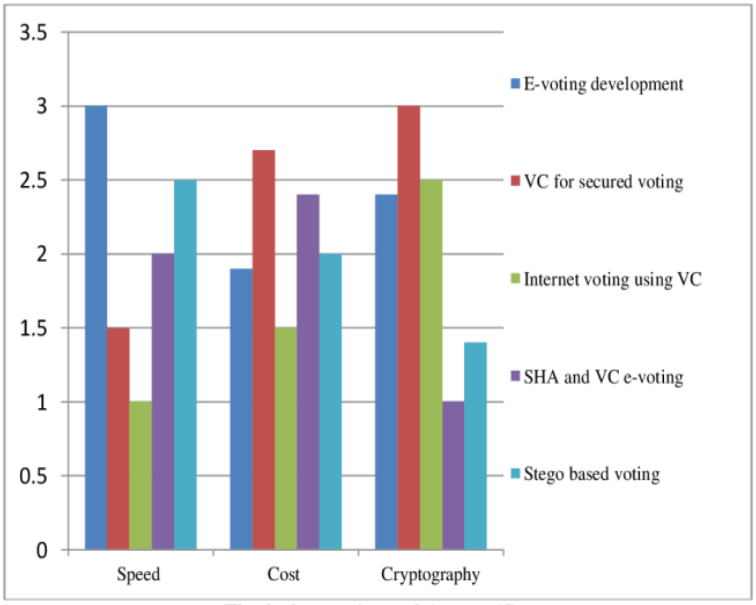

Figure 7: Comparison of the proposed approach

The integration of KNN can enhance the accuracy of facial recognition systems, while the utilization of SHA256 can provide robust security for blockchain transactions. By combining these two algorithms, a dependable and efficient blockchain-based facial recognition e-voting system can be achieved.

6. Future Enhancements

In the future, integrating the e-voting platform with mobile devices can potentially increase voter turnout, considering the widespread use of mobile devices for daily tasks. This would allow voters to conveniently cast their ballots anytime and anywhere. Furthermore, incorporating AI-based face recognition technology can enhance the precision and effectiveness of face verification, even in challenging conditions like dim lighting or when voters are wearing masks. To further enhance the security and accuracy of the voter identification process, the system can be integrated with additional biometric information such as voice or fingerprint recognition. Implementing decentralized identity management can provide voters with better control and protection over their personal data, as they would have the ability to manage their own identity information. Real-time results monitoring can also enhance the accountability and transparency of the e-voting system, allowing voters and interested parties to observe the tallying of results. Additionally, the concept of hybrid voting systems, which utilize both paper ballots and blockchain technology, can make the system more accessible to voters who are not accustomed to electronic voting and serve as a backup in case of any issues with the electronic system. Overall, these future developments have the potential to strengthen the security, usability, and transparency of the blockchain-based face-verified e-voting system, making it a more reliable and trustworthy solution for conducting elections.

7. Conclusion

In conclusion, a blockchain-based face-recognition e-voting system has the potential to offer a secure, effective, and transparent method for conducting elections. By leveraging blockchain technology, the system can ensure the immutability and integrity of the voting process, effectively preventing any fraudulent activities. Incorporating face recognition enhances system security by verifying the identities of voters and ensuring that only authorized individuals can participate. However, before implementing blockchain-based electronic voting with face recognition, careful consideration must be given to the accuracy of the facial recognition algorithm, the scalability of the blockchain network, and the system's usability. While cryptographic hashing techniques like SHA256 can provide a high level of security for blockchain transactions, the use of machine learning algorithms like KNN can improve the accuracy of the facial recognition system. Overall, a face-recognition blockchain-based e-voting system holds promise in delivering a secure and efficient means of conducting elections. Thorough implementation is crucial to ensure the system's correctness, security, and usability. Further research and development are necessary to address challenges and limitations and fully unleash the system's potential as a tool for democratic decision-making.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

Doi: https://doi.org/10.54216/FPA.120104
Received: May 16, 2023 Revised: June 15, 2023 Accepted: July 07, 2023

References

[1] Mahima Churi, Anmol Bajaj, Gurleen Pannu and Megharani Patil Blockchain-Based E-Voting System-In book: Intelligent Computing and Networking, Accessed: March 2023 DOI:10.1007/978- 981-99-0071-8_11

[2] Prof. Ashwini Taksal, Kishor Sandbhor,Yash Dhamak and Ajinkya Sudrik Online Voting System using Face Recognition and Blockchain- Accessed: February 2023 DOI:10.48175/IJARSCT-8547

[3] Hanane Echchaoui, Boudrali Roumaissa and Boudour Rachid A Proposal of Blockchain and NFC-Based Electronic Voting System-In book: Advanced Computational Techniques for Renewable Energy Systems (pp.66-75) Accessed: February 2023 DOI:10.1007/978-3-031- 21216-1_7

[4] Ali Alshehri, Mohamed Baza, Gautam Srivastava and Wahid Rajeh Privacy- Preserving E-Voting System Supporting Score Voting Using Blockchain-Applied Sciences 13(2):1096 Accessed: January 2023 DOI:10.3390/app13021096

[5] Maria-Victoria Vladucu,Ziqian Dong,Jorge Medina and Roberto Rojas- Cessa E-voting Meets Blockchain: A SurveyIEEE Access PP(99):1-1 Accessed: January 2023 DOI:10.1109/ACCESS.2023.3253682

[6] K. Varaprasada Rao and Sandeep Kumar Panda Secure Electronic Voting (E- voting) System Based on Blockchain on Various Platforms In book: Computer Communication, Networking, and IoT Accessed: October 2022 DOI:10.1007/978- 981-19-1976-3_18

[7] Saba Abdul-Baqi Salman,Sufyan T. Faraj Al-Janabi and Ali M Sagheer Valid Blockchain-Based E-Voting Using Elliptic Curve and Homomorphic Encryption International Journal of Interactive Mobile Technologies (iJIM) Accessed: October 2022 DOI:10.3991/ijim.v16i20.33173

[8] Young-Sung IHM and Seung-Hee Kim Development of a Blockchain-Based Online Secret Electronic Voting System-IEICE Transactions on Information and Systems,E105.D(8):1361-1372 Accessed: August 2022 DOI:10.1587/transinf.2021EDK0005

[9] Yousif Mohammed Wahab, Alaan Ghazi, Al- Qalam university College, Aras Al-Dawood and Muthana Alisawi A Framework for Blockchain-Based E-Voting System-International Journal of Interactive Mobile Technologies (iJIM) 16(10):210-222 Accessed: May 2022 DOI:10.3991/ijim.v16i10.30045

[10] G Revathy, K Bhavana Raj, Institute of Public Enterprise, Anil Kumar and Spurthi Adibatti Investigation of E-Voting System using Face Recognition using Convolutional Neural Network (CNN)Theoretical Computer Science Accessed: May 2022 DOI:10.1016/j.tcs.2022.05.005

[11] J. Huang, D. He, M. S. Obaidat, P. Vijayakumar,M. Luo, and K.-K.-R. Choo, ‘‘The application of the blockchain technology in voting systems: A review,’’ ACM Comput. Surv., vol. 54, no. 3, pp. 1–28, Apr. 2022, DOI: 10.1145/3439725.

[12] A. Barnes, C. Brake, and T. Perry. Digital Voting with the use of Blockchain Technology Team Plymouth Pioneers-Plymouth University. Accessed: Feb. 14, 2022.

[13] Deepak, N. R., Taj, S., Khizer, S., Waqeer, S., & Fathima, T. (2021). E-voting system using fingerprint and Face recognition authentication with blockchain. Journal of Advances in Computational Intelligence Theory, 3(3). http://hbrppublication.com/ OJS/ index.php/ JACIT/ article/view/2157

[14] Rohit Rastogi, Priyanshu Arora, Luv Dhamija and Rajat Srivastava Statistical Analysis of Online Voting System Through Blockchain and ML Techniques-A Sustainable Approach for 21st Century Life Style and Smart Cities International Journal of Cyber Behavior Accessed: January 2022 DOI:10.4018/IJCBPL.313947

[15] Janardan Krishna Yadav,Srinivas Jangirala,O.P. Jindal Global University,Deepika Chandra Verma and Shashi Kant Srivastava Blockchain for Fool-Proof E- Voting System-In book: ICT Analysis and Applications (pp.455-466) Accessed: January 2022 DOI:10.1007/978-981-16-5655-2_44

[16] Ali Alshehri, Mohamed Baza, Gautam Srivastava and Wahid Rajeh Privacy-Preserving E-Voting System Supporting Score Voting Using Blockchain-Applied Sciences 13(2):1096 Accessed: January 2023 DOI:10.3390/app13021096.

[17] C. S. Manigandaa,V. D. Ambeth Kumar,G. Ragunath,R. Venkatesan,N. Senthil Kumar. "De-Noising and Segmentation of Medical Images using Neutrophilic Sets." Fusion: Practice and Applications, Vol. 11, No. 2, 2023 ,PP. 111-123.

[18] S. Hemamalini ,V. D. Ambeth Kumar ,R. Venkatesan,S. Malathi. "Relevance Mapping based CNN model with OSR-FCA Technique for Multi-label DR Classification." Fusion: Practice and Applications, Vol. 11, No. 2, 2023 ,PP. 90-110

Doi: https://doi.org/10.54216/FPA.120104
Received: May 16, 2023 Revised: June 15, 2023 Accepted: July 07, 2023