A Project Report On

"DECENTRALIZED ELECTORAL SYSTEM"

UNIVERSITY INSTITUTE OF TECHNOLOGY
THE UNIVERSITY OF BURDWAN

DEPARTMENT OF COMPUTER SCIENCE

AND ENGINEERING [BATCH 2021-2025]

SUBJECT CODE: **PROJ-CSE 891**

Submitted By:

ROUNAK KUNDU (ROLL NO: T20211092 | REG. NO: 202130000199 OF 2021-22)
BIKASH DUTTA (ROLL NO: L20221084 | REG. NO: 20220000008 OF 2022-23)
HIMANGSHU SARKAR (ROLL NO: 20211063 | REG. NO: 202130000119 OF 2021-22)

A project under the guidance of

Mr. SOUMIK GHOSH

(ASSISTANT PROFESSOR)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

UNIVERSITY INSTITUTE OF TECHNOLOGY,

THE BURDWAN UNIVERSITY,

GOLAPBAG (NORTH), BURDWAN-713104,

WEST BENGAL, INDIA

ACKNOWLEDGEMENT

We would like to express our deepest gratitude and appreciation to all those who have contributed to the successful completion of our major project on "Decentralized Electoral System". This project has been an invaluable learning experience, and we are indebted to the individuals for their guidance, support and contributions.

First and foremost, we extend our heartfelt thanks to our project guide, Prof. Soumik Ghosh, for his unwavering support and invaluable guidance throughout the project. We also want to express our gratitude towards Dr. Souvik Bhattacharya, In-charge, Assistant Professor, Department of Computer Science and Engineering for providing us an opportunity to work on this topic. We are also grateful to the faculty members of University Institute of Technology, Burdwan University for providing us with the necessary resources and our family and friends for their continuous support and encouragement.

In conclusion, this project would not have been possible without the collective efforts and contributions of the individuals mentioned above. We are deeply grateful for their guidance, support, and dedication. Their involvement has enriched our learning experience and has been invaluable in shaping the success of this project.

Thanking you,

Team members:

_____

(ROUNAK KUNDU) [ROLL NO: T20211092 | REG. NO: 202130000199 OF 2021-22]

_____

(BIKASH DUTTA) [ROLL NO: L20221084 | REG. NO: 202230000008 of 2022-2023]

_____

(HIMANGSHU SARKAR) [ROLL NO: 20211063 | REG. NO: 202130000119 OF 2021-22]

University Institute of Technology,
The University of Burdwan

CERTIFICATE OF APPROVAL

This is certified that the project proposal entitled "DECENTRALIZED ELECTORAL SYSTEM" which is submitted by **Rounak Kundu**, **Bikash Dutta** and **Himangshu Sarkar** as partial fulfillment for the award of degree of **Bachelor of Engineering, Computer Science and Engineering** at **UNIVERSITY INSTITUTE OF TECHNOLOGY, THE UNIVERSITY OF BURDWAN** is the record of the word of the student which have been carried out under my supervision.

Date: 10 July, 2025

Place: **BURDWAN, WEST BENGAL**

_____

(Soumik Ghosh)
Project Supervisor
and Assistant Professor,
Department of
Computer Science and Engineering,
University Institute of Technology,
The University of Burdwan

TABLE OF CONTENTS

ABSTRACT

The advancement of technology has revolutionized various sectors, including the electoral process. This project proposes a decentralized electoral system utilizing the extensive network of ATMs across India as polling booths. By implementing iris verification for voter authentication and blockchain technology for secure vote recording, the system aims to enhance the accessibility, security, and efficiency of voting.

Iris verification will be used to ensure that each vote is legitimate, significantly reducing instances of fraud and impersonation. The Ethereum blockchain will secure voting data, providing transparency, immutability, and trust in the electoral process. The entire voting process will be automated, including instant vote counting, thereby minimizing human intervention and errors. This approach will also reduce election costs by utilizing existing ATM infrastructure and decreasing the need for traditional polling stations and associated resources. Furthermore, it will alleviate disruptions to educational institutions, which are often used as polling stations, allowing them to continue their activities without interruption.

Throughout the project, it became clear that the suggested implementation has essential tradeoffs and would not work in practice. The study concretizes what needs to be improved in order to use a voting system built on blockchain technology. This report concludes that there is still work to be done in order to use this technology in crucial elds such as voting. And suggests using a private blockchain in order to implement the specified voting system, DeVote.

GENERAL TERMS AND ABBREVIATIONS

API: Application Programming Interface.

ATM: Automated Teller Machine.

Back-end: Server-side, refers to things the user can't see e.g. databases and servers.

Bitcoin: World's largest cryptocurrency.

Blockchain: Decentralized data storage.

CI: Continuous Integration, used for automate testing when pushing to master branch.

CLI: Command-line interface.

Consensus Mechanism: Protocol used to synchronize all nodes on the blockchain.

DAPP: Decentralized Applications, e.g. the suggested prototype.

Decentralized System: A system with no central authority.

DeVote: The decentralized voting system that was implemented for this thesis.

DLT: Distributed Ledger Technology.

ECDSA: Elliptic Curve Digital Signature Algorithm.

Ethash: A hashing algorithm used in Ethereum blockchain.

Ethereum: Blockchain based platform.

Smart Contract: Protocol for digitally verifying negotiations of a contract.

Front-end: Client-side, everything involved with what the user sees.

Genesis Block: First block of a blockchain.

GUI: Graphical user interface.

Hash Function: Algorithm that converts data in a one-way manner.

Keccak: A primitive cryptographic family which holds members of the Secure Hash

Algorithm family.

Linter: Software for analyzing code for potential errors.

Mining: Process used to create blocks for the blockchain.

Nonce: Essentially a piece of data that is time consuming to compute but easy to verify.

Peer-to-Peer Network: Non-hierarchical network where nodes communicate directly between each other.

PoS: Proof of stake, compared to the Proof of Work, where the creator of a new block is chosen in a deterministic way, depending on its wealth.

PoW: Proof of Work. Essentially a protocol that by computational power states which block to trust.

Proof of Concept: Realization of an idea, used to demonstrate its utility.

secp256k1 Curve: Parameters of the elliptic curve used in Bitcoins public-key cryptography

Solidity: Programming language used for implementing smart contracts and designed to be used on Ethereum's Virtual Machine.

TTP: Trusted Third Party UTXO Unspent Transaction Outputs is the output of a bitcoin transaction that a user receives and is able to spend in the future.

Webhook: User do need HTTP callbacks.

INTRODUCTION

India is the world's largest democracy with an estimated 23.1 million registered voters. The heart of democracy is voting. In order to ensure a fair and credible election process, security and reliability must be guaranteed in every stage of the process. The success of a democracy depends on the degree of fairness and reliability of its elections.

1.1. Background

Elections have a great power in determining the fate of a nation or an organization. Simple purpose of the election is the channeling of popular sovereignty as a representative democracy. At first, elections in India were conducted using paper ballots. In the paper ballot voting scheme, voters marked their choice of candidates on a piece of paper known as the ballot paper and placed them in the ballot box. Mostly, these ballots were manually counted and this led to a considerable delay in the election process. Also, there was no guarantee of vote secrecy. In some constituencies there were allegations of booth capture and 'ballot stuffing' by party loyalists [1]. In order to overcome these problems, Electronic Voting Machines (EVMs) were introduced by the Election Commission of India in the 1990s. These EVMs have been exclusively manufactured by two government-owned companies: Bharat Electronics Limited (BEL) and Electronics Corporation of India Limited (ECIL). These devices have a simple design and are easy to use. But they were subjected to widespread criticism by various political parties who questioned their reliability and integrity. In addition to this, there has also been an increase in the number of allegations of electoral frauds due to EVMs, such as in the 2009 parliamentary elections [2].

1.2. Purpose

The primary objective of this project is to propose a decentralized electoral system that democratizes access to voting by leveraging existing infrastructure and state-of-the-art technologies. By utilizing ATMs as polling booths and implementing iris verification alongside blockchain technology, the project aims to facilitate a secure, convenient,

and transparent voting process for citizens across India. Through this innovative approach, the project seeks to enhance civic participation, foster trust in democratic institutions, and pave the way for more inclusive and efficient elections.

1.3. Problems and Solutions

The most frequent problem in elections is the issue of data manipulation, security, and transparency. With the development of technology, the use of technology in overcoming the problems that occur becomes important, as well as the intricacies of the collection process [3]. Security is always the biggest concern for an DeVote system. There should be no DeVote system to secure data and should be able to withstand potential attacks. Blockchain technology is one solution that can be used to reduce the problems that occur in voting. Blockchain has been used in Ethereum transaction database systems [4]. Blockchain is a distributed, unchangeable and transparent ledger who can't deny the truth [5]. Consists of several blocks that are linked to each other and in sequence. The block is related because from the previous hash used in the next block making process, the attempt to change the information will be more difficult as it has to change the next blocks [6]. The database was made public, acquired by many users. The circumstances of cheating, the database owned by users who do the cheating will be different from the database owned by other users. Then the existing database on the user is not valid. In the Ethereum system, a mining process is required. In this research, a method that uses turn rules for each node in blockchain creation, with the assured importance of each node joining the blockchain. This research is on the recording of the results of DeVote conducted after the election process is completed. The data corresponding to the results on each node distributed under the blockchain permission protocol.

Blockchain will notably strengthen transparency, revolutionize the national election methods, and ameliorate the conventional way of voting. It also alleviates the labor and the cost to conduct. This system withholds the potential to replace EVMs. The Block-chain based polling system is secure and robust with additional features such as reduced paperwork, manpower, and running cost. One of the main issues faced with the current method of polling is that the voter can only cast the vote in the assigned

polling booth, this makes it impossible for people living out of their native towns. The software-based election would be a good solution for the eligible citizens with voting rights to vote form any part of the country with no constraints for a particular booth. It would provide immense help to the Election Commission of India for faster and easier conduction. The use of the Internet of Things in the biometric scanners outside every booth will stop the forced illegal entry by verification of each biometrics before they step in. The future enabled with a decentralized network of the registered votes will be best served by the Blockchain technology. Apart from giving a solution for current problems, the technology also gives the option to check and verify the vote cast by each voter on the network.

Advantages existing Polling System:

- 10,000 tons of ballots are saved in a national election in India which is around 2 lac trees [7].
- EVM machines are easy to move from one place to another place.
- Shorter vote count time as compared to early machinery.
- The EVMs are run by the batteries, so these machines can be used in those areas whereas there is no electricity.
- EVM reduces the possibilities of fake votes.
- EVM machines can be moved easily from one place to another as compared to the ballot boxes.

Limitations Existing Polling System:

- A candidate can know how many people from a polling station voted for him and might show favoritism or hold a grudge on specific areas [8].
- Manual working increases the time consumption.
- Each voter is restricted to a specific polling station.
- Counting of votes is a tedious, time consuming, and less reliable process.
- EVMs are restricted to 2000 votes and 64 candidates.
- Concerns were raised in the 2019 Lok Sabha elections about the tampering and hacking of EVMs.

- Existing polling systems has set-up as well as maintenance costs.

1.4. Delimitations

While the proposed decentralized electoral system offers numerous benefits, it is essential to acknowledge certain limitations and constraints. Firstly, the implementation of such a system may require significant investment in infrastructure upgrades and technological integration. Additionally, ensuring the security and reliability of iris verification and blockchain technologies will be paramount to the success of the project. Furthermore, while the project aims to enhance accessibility and inclusivity, it may not completely eliminate all barriers to voting, particularly for marginalized or disadvantaged populations. Finally, the scope of the project may be limited to certain geographical regions or demographics, necessitating further research and adaptation for broader implementation.

LITERATURE SURVEY

To finalize an approach for implementing a decentralized electoral system using blockchain technology and iris verification, we reviewed numerous studies and previous works assessing the feasibility, security, and efficiency of these technologies. The goal was to ensure a robust, secure, and accessible voting platform that addresses the limitations of traditional voting systems.

Let's discuss the summery of the research papers and applications we studied.

Paper ID	Author's Name (Publication Year)	Objective	Technologies Used	Advantages	Limitations
[1]	J. Alex Halderman et al. (2010)	To evaluate the security of India's Electronic Voting Machines (EVMs) and identify potential vulnerabilities that could be exploited to alter election outcomes.	Hardware, firmware analysis, tamper detection, side-channel analysis, and simulated attacks tested EVM vulnerabilities in controlled environments.	Increasing awareness about significant security flaws in EVMs, which is crucial for prompting improvements in electronic voting security	Potential public trust issues, logistical and financial challenges in addressing vulnerabilities, and possible complexity or usability problems with improvements.
[2]	Christian (2017)	Design and implement visual cryptography in an DeVote system to enhance voter anonymity.	Visual cryptography for encrypting visual information and integration into an DeVote system.	Enhanced voter anonymity and privacy protection against identity exposure.	Implementation complexity and potential usability issues for end-users.

Paper ID	Author's Name (Publication Year)	Objective	Technologies Used	Advantages	Limitations
[3]	C. Dougherty (2016)	Develop a secure and transparent voting system using blockchain technology to ensure democratic voting integrity.	Blockchain technology for secure and transparent vote recording and verification.	Immutable vote records enhance security and transparency, preventing tampering and fraud.	High computational requirements and potential scalability issues could hinder widespread adoption.
[4]	D. A. Wijaya (2016)	To explore advanced concepts and implementations of Bitcoin, focusing on enhancing understanding and application of cryptocurrency technologies	Bitcoin protocol, blockchain technology, advanced cryptographic techniques, and transaction management within the Bitcoin network.	Provides deeper insights into Bitcoin's technical aspects, improving understanding and potential implementation of advanced cryptocurrency features.	Complexity of advanced topics may be challenging for beginners; technical depth might limit accessibility for non-experts.
[5]	H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. J. Kishigami (2016)	To propose a complete consensus mechanism for blockchain contracts, aiming to enhance reliability and security in blockchain-based agreements.	Blockchain technology, consensus algorithms, and smart contracts to ensure secure and reliable execution of blockchain transactions.	Enhanced security and reliability for executing blockchain contracts, improving trust and transparency in digital agreements.	Potential complexity in implementing and maintaining consensus mechanisms; may involve higher computational overhead and increased resource consumption.

Paper ID	Author's Name (Publication Year)	Objective	Technologies Used	Advantages	Limitations
[6]	P. Vamsikrishna, S. D. Kumar, D. Bommisetty, and A. Tyagi (2016)	To develop a reliable voting system using Raspberry Pi technology to enhance transparency and integrity in democratic voting processes.	Raspberry Pi hardware, software for secure voting applications, and networking for data transmission and vote recording.	Cost,effective, transparent, and reliable technology for improving electoral processes; Raspberry Pi provides an accessible and flexible platform for implementation.	Limited processing power and potential security vulnerabilities; may require additional security measures to ensure robustness against tampering and cyber threats.
[7]	Jagranjosh (2022)	To outline the benefits of using Electronic Voting Machines (EVMs) in elections, highlighting their advantages in improving the electoral process.	Electronic Voting Machines (EVMs) incorporating digital technology for secure and efficient vote recording and counting.	EVMs streamline the voting process, reduce human error, and expedite vote counting, enhancing efficiency and accuracy in elections.	Potential security vulnerabilities, tampering risks, and issues with public trust in electronic systems may affect the overall reliability of EVMs.

Paper ID	Author's Name (Publication Year)	Objective	Technologies Used	Advantages	Limitations
[8]	Wikipedia (2024)	To provide an overview of electronic voting in India, including its adoption, implementation, and impact on the electoral process.	Electronic Voting Machines (EVMs) and Voter Verifiable Paper Audit Trail (VVPAT) for secure and verifiable vote recording and counting.	EVMs improve voting speed, reduce manual errors, and enhance election efficiency; VVPAT ensures vote verification and transparency.	Concerns about EVM tampering, technical glitches, and lack of transparency may affect public confidence and the integrity of the voting process.
[9]	Y. Abuidris, R. Kumar, and W. Wenyong (2019)	To survey and analyze blockchain-based electronic voting systems, exploring advantages, challenges, and implementations for secure voting.	Blockchain technology for secure, transparent, and decentralized voting systems, including smart contracts and cryptographic techniques.	Blockchain provides secure, tamper-proof voting records, enhances transparency, and reduces the risk of election fraud.	Blockchain systems may face scalability issues, high implementation costs, and complex integration with existing electoral processes.
[10]	K. M. Khan, J. Arshad, and M. M. Khan (2020)	To investigate performance constraints of blockchain-based secure electronic voting systems, focusing on issues like scalability, speed, and resource requirements.	Blockchain technology, including distributed ledgers, consensus algorithms, and cryptographic methods for secure voting.	Blockchain enhances security, integrity, and transparency of voting systems while providing a tamper-resistant record of votes.	Performance constraints include scalability challenges, slower transaction processing speeds, and higher computational and resource demands.

Paper ID	Author's Name (Publication Year)	Objective	Technologies Used	Advantages	Limitations
[11]	B. Singhal, G. Dhameja, and P. S. Panda (2018)	To provide a comprehensive introduction to blockchain technology, including fundamental concepts and practical guidance for building blockchain solutions.	Blockchain fundamentals, including distributed ledgers, consensus algorithms, cryptographic techniques, and smart contracts.	Offers a clear, accessible introduction to blockchain technology, making it easier for beginners to understand and implement blockchain solutions.	Focused on foundational knowledge; may not cover advanced topics or address complex real-world blockchain implementation challenges.
[12]	G. M. C. Sravani (2019)	To propose a secure electronic voting system integrating blockchain and homomorphic encryption to enhance voter privacy and election integrity.	Blockchain technology for transparent vote recording, and homomorphic encryption for privacy-preserving computation on encrypted data.	Enhances security and privacy by combining blockchain's transparency with homomorphic encryption's ability to process encrypted votes without decryption.	Complex integration of blockchain and encryption technologies may introduce implementation challenges and performance overhead.
[13]	Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten (2007)	To conduct a security analysis of the Diebold AccuVote-TS voting machine, identifying vulnerabilities and assessing the machine's security risks.	Diebold AccuVote-TS voting machine hardware and software, including analysis of security flaws in the voting system.	Uncovers critical security vulnerabilities, contributing to improvements in voting machine security and election integrity.	Reveals weaknesses that may undermine public confidence in electronic voting systems; addressing these flaws can be complex and costly.

Paper ID	Author's Name (Publication Year)	Objective	Technologies Used	Advantages	Limitations
[14]	Vitalik Buterin (2013)	To introduce Ethereum, a blockchain platform designed to enable smart contracts and decentralized applications (DApps), expanding blockchain functionality beyond Bitcoin.	Ethereum blockchain, smart contracts, decentralized applications (DApps), and Ethereum Virtual Machine (EVM).	Supports flexible and programmable contracts, enabling a wide range of decentralized applications and complex transactions beyond simple cryptocurrency transfers.	Scalability issues and higher complexity compared to simpler blockchain systems; can also face security challenges related to smart contract vulnerabilities.
[15]	H. Agarwal and G. N. Pandey (2013)	To design an online voting system for India using AADHAAR ID to enhance voter authentication and streamline the voting process.	AADHAAR ID for voter verification, online voting platforms, and secure authentication methods to ensure accurate and reliable voting.	Improves voter authentication, reduces fraud, and streamlines the voting process, making it more accessible and efficient.	Dependency on AADHAAR ID may exclude some eligible voters; online systems face security risks and may require robust infrastructure
[16]	Ankit Anand and Pallavi Divya (2012)	To propose an efficient online voting system that enhances the voting process through improved security and user convenience.	Online voting platform, secure authentication mechanisms, and data encryption techniques to protect vote integrity and privacy.	Increases voting efficiency, accessibility, and security by leveraging online technology and encryption methods for safe and user-friendly voting.	May face challenges related to cybersecurity, including potential hacking risks and the need for robust infrastructure to ensure system reliability.

Paper ID	Author's Name (Publication Year)	Objective	Technologies Used	Advantages	Limitations
[17]	D. Ashok Kumar and T. Ummal Sariba Begum (2011)	To design a novel electronic voting system that incorporates fingerprint recognition technology for enhanced voter authenticatio n and system security.	Fingerprint recognition for biometric authentication, electronic voting system hardware and software for secure and accurate vote processing.	Enhances security and accuracy of voter identification, reducing fraud and ensuring that each vote is cast by a legitimate voter.	Requires reliable biometric hardware and may face challenges related to fingerprint recognition accuracy and data privacy.
[18]	Ahmed Ben Ayed (2017)	To propose a conceptual secure electronic voting system based on blockchain technology to enhance security, transparency, and integrity in voting processes.	Blockchain technology for secure, transparent, and immutable vote recording, with cryptographic methods to ensure data integrity and confidentiality.	Provides a secure and tamper-proof voting system with enhanced transparency and traceability, reducing risks of election fraud.	Conceptual design may face practical implementati on challenges, including scalability issues and the need for robust infrastructure to support blockchain technology.
[19]	R. Bremananth (2016)	To develop a robust method for detecting eyelashes and eyelids in iris recognition systems to enhance accuracy and security in biometric applications.	Iris recognition technology with algorithms for detecting eyelashes and eyelids, applied within a Localized Random Coefficient (LRC) security system framework.	Improves accuracy of iris recognition by addressing challenges related to eyelashes and eyelids, enhancing biometric system security.	Complexity in processing and potential computationa l overhead; may require significant adjustments to existing iris recognition systems.

Paper ID	Author's Name (Publication Year)	Objective	Technologies Used	Advantages	Limitations
[20]	H. Hofbauer, E. Jalilian, and A. Uhl (2019)	To enhance iris recognition accuracy by utilizing superior Convolutional Neural Network (CNN)-based iris segmentation techniques.	Convolutional Neural Networks (CNNs) for advanced iris segmentation, pattern recognition algorithms for improved accuracy in iris recognition.	Achieves higher recognition accuracy by leveraging advanced CNN-based segmentation, improving the reliability and precision of iris biometric systems.	CNN-based methods may require extensive computational resources and large datasets for training, potentially increasing complexity and processing time.
[21]	S. Chaudhary and R. Nath (2015)	To propose a new template protection approach for iris recognition to enhance security and privacy by safeguarding iris templates.	Template protection techniques for iris recognition, including cryptographic methods and secure storage solutions for biometric data.	Improves security and privacy of iris recognition systems by protecting sensitive biometric templates from unauthorized access and potential misuse.	Deployment complexity and potential performance trade-offs; may require sophisticated techniques that could impact system efficiency and user experience.
[22]	Z. Hussain and D. Agarwal (2019)	To perform a comparative analysis of various edge detection techniques applied to flame image processing, evaluating their effectiveness and performance.	Edge detection techniques such as Sobel, Canny, and Prewitt filters applied to flame images for identifying boundaries and features.	Provides insights into the effectiveness of different edge detection methods for flame image processing, helping improve accuracy.	May require extensive computational resources and could face challenges in differentiating between flame edges and noise or other similar features.

Paper ID	Author's Name (Publication Year)	Objective	Technologies Used	Advantages	Limitations
[23]	Follow My Voatz,Inc. (2023)	Enhance voting transparency, security, and accessibility using blockchain technology for governmental and corporate elections.	Uses blockchain for an immutable vote ledger, encryption, two-factor authentication, distributed ledger, blockchain nodes, secure databases, and APIs for communication.	Increased transparency, enhanced security through encryption, and improved accessibility for remote and disabled voters.	Scalability challenges, user adoption issues, and the need for regulatory compliance across jurisdictions.
[24]	Voatz (2014)	Enable secure, accessible voting via smartphones and tablets using blockchain technology.	Blockchain Technology: Secure, immutable vote recording. Biometric Authentication: Fingerprint and facial recognition. End-to-End Encryption: Secure data transmission. AES: Strong data encryption. RSA: Secure key exchanges. Blockchain Cryptography: Ensures data integrity.	Provides secure, immutable vote records with blockchain, biometric authentication, and end-to-end encryption.	Faces security concerns, transparency issues, scalability challenges, and regulatory hurdles.

2.1. Global Experiments

Decentralized voting systems, particularly those leveraging blockchain technology, have been an area of active research and experimentation around the world. These systems aim to enhance the transparency, security, and efficiency of voting processes.

2.1.1. Past Work

Here are some notable examples of past work and experiments in decentralized voting:

Estonia

Estonia has been a pioneer in electronic voting (e-voting), starting its implementation in 2005. While not decentralized, its i-Voting system serves as a foundational experiment in digital voting. The system uses strong cryptographic methods to secure votes and has evolved to include features that could integrate blockchain in the future for enhanced security and transparency.

Switzerland

Switzerland has experimented with blockchain-based voting. In 2018, the Swiss city of Zug conducted a blockchain-based municipal vote. The trial involved 72 citizens and demonstrated the feasibility of using blockchain for secure, transparent, and tamper-proof voting processes.

Sierra Leone

In 2018, Sierra Leone conducted a blockchain-based voting pilot during its presidential elections. The project, run by Agora, a Swiss-based blockchain startup, aimed to provide a transparent and secure method of tallying votes. While not the primary method used for the official count, the pilot demonstrated the potential of blockchain technology in a real-world electoral process.

West Virginia, USA

West Virginia piloted a blockchain voting system for overseas military personnel during the 2018 midterm elections. The pilot used a mobile voting platform developed

by Voatz. Despite some security concerns raised by experts, the pilot was considered successful and demonstrated the practicality of using blockchain for absentee voting.

Japan

Tsukuba City in Japan tested a blockchain-based voting system in 2018 for local administrative processes. The system allowed residents to vote on social development programs, showcasing blockchain's application in participatory governance.

Moscow, Russia

Moscow has implemented several blockchain-based voting pilots, particularly for its Active Citizen program, which involves voting on civic issues. These pilots have highlighted the potential of blockchain to increase voter engagement and trust in the voting process.

Spain (Catalonia)

Catalonia has explored blockchain voting for its regional independence referendum. Though the political context was contentious, the technical experiments underscored blockchain's potential in managing secure and transparent voting processes even in politically sensitive scenarios.

2.1.2. Security Concerns

West Virginia (Voatz): Vulnerabilities in the Voatz mobile app raised manipulation concerns.

Sierra Leone (Agora): Doubts surfaced about the integrity and security of Agora's blockchain-based system.

Moscow, Russia (Active Citizen): Security vulnerabilities in the voting platform highlighted potential compromises.

General Concerns: Vulnerabilities in supporting infrastructure, data privacy, and end-to-end security pose significant challenges.

2.1.3. Conclusion

Decentralized voting systems leveraging blockchain technology show promising

potential in enhancing the security, transparency, and efficiency of voting processes. However, widespread adoption requires overcoming technical, regulatory, and security challenges. Continued experimentation and research are essential to address these issues and realize the full potential of decentralized voting.

METHODOLOGIES

To develop a secure and efficient DeVote system, a combination of methodologies derived from various research studies can be implemented. This comprehensive approach integrates blockchain technology, advanced cryptographic techniques, biometric authentication, and rigorous security analysis to ensure the integrity and transparency of the voting process.

3.1. Blockchain-Based Framework

A blockchain-based framework is essential for ensuring immutability and transparency in DeVote systems. As discussed by Watanabe et al. in "Blockchain contract: A complete consensus using blockchain" and Ayed in "A Conceptual Secure Blockchain-Based Electronic Voting System," blockchain technology can securely record votes in an immutable ledger [5]. This decentralized approach ensures that no single entity can alter the voting records. Ethereum smart contracts, as described by Vitalik Buterin in the "Ethereum White Paper," automate the vote counting process by executing predefined rules and updating the blockchain ledger with each vote [14]. This eliminates the need for manual intervention and minimizes the risk of errors or fraud. The peer-to-peer transaction validation mechanism similar to Bitcoin, as outlined by Nakamoto in "Bitcoin: A Peer-to-Peer Electronic Cash System," ensures that votes are validated by multiple nodes in the network, enhancing the security and reliability of the voting system.

3.2. Cryptographic Techniques

To enhance voter anonymity and vote security, various cryptographic techniques are employed. Christian's study on visual cryptography, "Desain Dan Implementasi Visual Cryptography Pada Sistem DeVote Untuk Meningkatkan Anonymity," highlights a method where votes are split into visually encrypted shares [2]. These shares can only be combined to reveal the vote, thus maintaining voter anonymity. Sravani’s research in "Secure electronic voting using blockchain and homomorphic encryption"

introduces homomorphic encryption, which allows encrypted votes to be processed without decrypting them [12]. This ensures that the confidentiality of votes is preserved throughout the counting process. Furthermore, robust cryptographic schemes for protecting biometric data, such as iris templates, are implemented to secure sensitive voter information. Chaudhary and Nath's approach in "A new template protection approach for iris recognition" provides a method to protect biometric data against unauthorized access or tampering [21].

3.3. Biometric Authentication

Biometric authentication strengthens the security of the DeVote system by ensuring that only eligible voters can cast their ballots. Fingerprint authentication, as detailed by Kumar and Begum in "A Novel design of Electronic Voting System Using Fingerprint," utilizes the uniqueness of fingerprints to verify voter identity, preventing unauthorized voting [17]. Iris recognition, employing advanced CNN-based segmentation techniques as described by Hofbauer et al. in "Exploiting superior CNN-based iris segmentation for better recognition accuracy," provides an additional layer of security [20]. This method improves the accuracy and reliability of voter authentication, making it difficult for unauthorized individuals to spoof the system. In India, the integration of Aadhaar ID, as suggested by Agarwal and Pandey in "Online voting system for India based on AADHAAR ID," offers a robust solution for voter identification, leveraging the widespread use of Aadhaar for a secure and scalable authentication process [15].

3.4. Distributed Ledger

The DeVote system leverages the power of distributed ledger technology (DLT) to revolutionize the voting process. A distributed ledger, often referred to as blockchain, is a decentralized database that is shared across multiple locations or nodes. This technology ensures that all transactions, in this case, votes, are recorded in a secure, transparent, and immutable manner. The use of DLT in our project addresses several critical issues inherent in traditional voting systems, such as security, transparency, and trust.

In DeVote, every vote is recorded as a transaction on the blockchain. This decentralized approach eliminates the need for a central authority to manage and verify votes, thereby reducing the risk of manipulation and fraud. Since the ledger is distributed across numerous nodes, any attempt to alter the voting data would require simultaneous manipulation of the majority of these nodes, making tampering virtually impossible. This inherent security feature of DLT ensures that the integrity of the voting process is maintained, and the results are trustworthy [23].

Transparency is another significant advantage of using a distributed ledger. In traditional voting systems, the process of vote counting and result tabulation is often opaque, leading to suspicions and allegations of fraud. With DeVote, every transaction is recorded on the blockchain, which is publicly accessible and can be audited by anyone. This transparency allows for real-time monitoring of the voting process, ensuring that all stakeholders, including voters, candidates, and election officials, can verify the accuracy of the results [24].

Furthermore, DLT enhances the efficiency of the voting process. Traditional systems involve manual counting and consolidation of votes, which is time-consuming and prone to human error. In contrast, DeVote automates these processes through smart contracts. These self-executing contracts, encoded on the blockchain, automatically verify voter eligibility, record votes, and tally results, ensuring a swift and accurate conclusion to the election. This automation not only speeds up the process but also minimizes the potential for human error and bias.

Privacy is also a critical concern in any voting system. DeVote addresses this by using advanced cryptographic techniques to ensure that votes are anonymous and cannot be traced back to individual voters. Each vote is encrypted before being recorded on the blockchain, and only authorized entities can decrypt and access the data. This ensures that voter privacy is maintained while still providing a transparent and verifiable record of the election.

The decentralized nature of DLT also enhances the resilience of the voting system. Traditional systems can be vulnerable to single points of failure, where a disruption at a central node can affect the entire system. In contrast, DeVote's distributed ledger is replicated across multiple nodes, ensuring that the system remains operational even if some nodes fail. This resilience is crucial for maintaining the continuity and reliability of the voting process, especially in large-scale elections.

In summary, the use of distributed ledger technology in the DeVote system provides a robust solution to the challenges faced by traditional voting systems. By ensuring security, transparency, efficiency, privacy, and resilience, DLT enables a more trustworthy and accessible electoral process. This innovative approach not only addresses current issues but also sets the stage for future advancements in democratic participation.

3.5. Security Analysis and Audits

Regular security analysis and audits are crucial for maintaining the integrity of the DeVote system. Wolchok et al. in "Security Analysis of India’s Electronic Voting Machines" and Feldman et al. in "Security Analysis of the Diebold AccuVote-TS Voting Machine" emphasize the importance of reverse engineering and penetration testing to uncover and address potential vulnerabilities [1][13]. These analyses involve examining both hardware and software components to identify weaknesses that could be exploited. Regular security audits and performance evaluations, as highlighted by Khan et al. in "Investigating performance constraints for blockchain based secure DeVote system," ensure that the system remains resilient against emerging threats [10]. Continuous monitoring and updating of security protocols are essential to maintaining trust in the DeVote process.

3.6. Transparency and Auditability

Maintaining transparency and auditability is vital for public trust in the DeVote system. The decentralized ledger, as discussed by Watanabe et al. and Ayed, allows for public verification of votes, ensuring that the voting process is transparent and tamper-proof [5][18]. Each vote recorded on the blockchain is publicly verifiable, enabling voters

and independent auditors to confirm the integrity of the election results. This level of transparency helps build confidence in the electoral process and ensures that any discrepancies can be quickly identified and addressed.

3.7. Performance and Scalability

To handle large-scale elections, the DeVote system must be both performant and scalable. Efficient edge detection algorithms for biometric image processing, as analyzed by Hussain and Agarwal in "A Comparative Analysis of Edge Detection Techniques Used in Flame Image Processing," enhance the speed and accuracy of voter authentication. Optimizing these algorithms ensures quick and reliable verification of voter identities [22]. Additionally, addressing performance constraints in blockchain-based systems, as discussed by Khan et al., involves implementing scalability measures to handle high volumes of transactions without compromising security or performance. This includes optimizing cryptographic processes and ensuring that the blockchain framework can efficiently manage peak voting periods.

PROBLEM STATEMENT

The integrity and efficiency of electoral processes are crucial to maintaining public trust in democratic systems. However, traditional voting methods face significant challenges that compromise the security, transparency, and accessibility of elections. As technology evolves, it becomes essential to address these issues through innovative solutions. Here are the key problems associated with traditional voting systems:

- **Data Manipulation:** One of the foremost issues in traditional voting systems is data manipulation. This problem manifests in various forms, including the altering of vote counts, deletion of legitimate votes, and the addition of fraudulent votes. Data manipulation undermines the integrity of the electoral process and erodes public trust in democratic institutions. When the accuracy of the vote tally is compromised, the legitimacy of the elected officials and the democratic process itself is called into question. Historical instances of data manipulation have led to political instability, protests, and even violence, as seen in various parts of the world.
- **Security Concerns:** Security is a critical concern in traditional voting systems, which are vulnerable to multiple types of attacks. Physical tampering with voting machines, cyberattacks on electronic voting systems, and insider threats all pose significant risks. Physical tampering can involve altering the internal mechanisms of voting machines to change the outcome. Cyberattacks can be orchestrated by hackers to infiltrate election systems, steal data, or alter vote counts. Insider threats involve individuals within the election system who have access to sensitive information and can manipulate results from within. These vulnerabilities make it challenging to ensure the confidentiality, integrity, and availability of the voting process, which are essential for a secure election.
- **Transparency Issues:** Transparency in the voting process is crucial for maintaining public confidence in the electoral system. Traditional voting methods often lack the necessary transparency, leading to suspicions of foul play. The processes and technologies used in elections are not always clear to

the public, which can result in a lack of trust in the outcomes. Transparency issues also arise from the inability to independently verify the accuracy of the vote count. Without a transparent system, it is difficult for third-party observers to audit the election process and ensure that the results are accurate and free from manipulation.

- **Geographical Constraints:** Traditional voting systems require voters to cast their ballots at designated polling stations. This requirement can be inconvenient for voters who live far from their assigned polling places, particularly in rural areas where polling stations may be sparse. Geographical constraints can significantly impact voter turnout, as individuals may be unable or unwilling to travel long distances to vote. This issue disproportionately affects marginalized communities, including the elderly, people with disabilities, and those without reliable transportation. Consequently, the geographical limitations of traditional voting systems can lead to lower participation rates and a less representative electoral outcome.
- **Resource Utilization:** The setup and operation of polling stations require significant resources, including manpower, equipment, and facilities. The logistical complexity and financial burden of establishing and maintaining these stations can be substantial. For instance, in large countries with vast and diverse populations like India, the logistical challenges are immense. Elections require the deployment of thousands of polling stations, each staffed with trained personnel and equipped with voting machines. Additionally, securing these locations and ensuring they are accessible to all voters adds to the resource demands. These factors contribute to the high cost of conducting elections and can strain public resources.
- **Manual Processes:** Many traditional voting systems still rely heavily on manual processes for vote counting and verification. Manual vote counting is labor-intensive and prone to human error, which can delay the reporting of election results and increase the likelihood of inaccuracies. Human involvement in vote counting also opens up opportunities for intentional manipulation or bias, further compromising the integrity of the election. The delays and potential

errors associated with manual processes can diminish public confidence in the electoral system and its ability to deliver timely and accurate results.

- **Complexity and Accessibility:** The complexity of the voting process can also be a barrier to participation. Voters may encounter difficulties in understanding how to use voting machines, complete paper ballots correctly, or navigate the logistics of casting their vote. This complexity can be particularly challenging for first-time voters, individuals with low literacy levels, and those with disabilities. Ensuring that the voting process is straightforward and accessible to all eligible voters is essential for promoting higher participation rates and ensuring that every voice is heard.
- **Lack of Real-Time Updates:** Traditional voting systems often lack the capability to provide real-time updates on voter turnout and voting progress. This limitation makes it difficult for election officials to monitor and respond to issues as they arise. Real-time data can be invaluable for identifying and addressing problems such as long wait times, technical malfunctions, or security breaches. Without real-time updates, election officials are operating with limited information, which can hinder their ability to ensure a smooth and efficient voting process.

In summary, traditional voting systems face numerous challenges, including data manipulation, security vulnerabilities, transparency issues, geographical constraints, resource demands, reliance on manual processes, complexity, and a lack of real-time updates. Addressing these problems is crucial for enhancing the integrity, efficiency, and accessibility of the electoral process. Advanced technologies such as blockchain and biometric verification offer promising solutions to these longstanding issues, providing a pathway to more secure, transparent, and inclusive elections.

PROPOSED METHODOLGY

The DeVote system aims to transform the voting process by integrating blockchain technology and iris verification into the existing ATM infrastructure across India. This methodology outlines the detailed steps and components required to implement DeVote, ensuring a secure, transparent, and accessible voting platform that addresses the shortcomings of traditional voting systems.

5.1. Technical Background

This section introduces and establishes the fundamental technical theory of blockchain technology; particularly Ethereum which was the central framework implemented in order to build a minimum valuable decentralized voting system. Basically, all relevant concepts and terms regarding blockchain technology and the necessary surrounding technicalities are explained.

5.1.1. Blockchain

Blockchain technology is a decentralized digital ledger that records transactions across multiple computers in a way that ensures security, transparency, and immutability. It is the underlying technology behind cryptocurrencies like Bitcoin and Ethereum and is increasingly being applied in various fields, including finance, supply chain management, and voting systems [1][2][3].

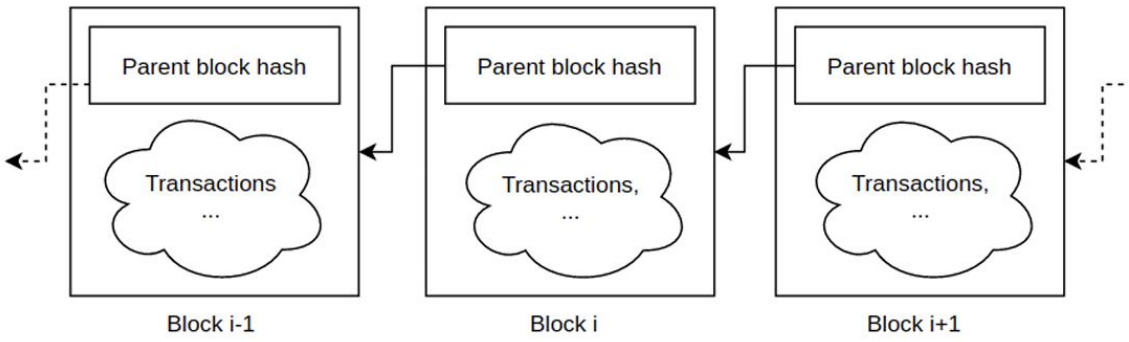

Figure 1: Abstract blockchain visualization, where each cloud represents digital information about transactions. Fundamentally, this information varies and is stored

and represented in different forms of data structures. Depending on the blockchain, this might vary from more basic Bitcoin blocks to complex Ethereum blocks.

5.1.1.1. Transactions

In a blockchain, a transaction is a transfer of value or information between participants. Each transaction is digitally signed by the sender's private key, ensuring its authenticity and integrity. Transactions are grouped into blocks, which are then added to the blockchain in a linear, chronological order. Once a transaction is recorded in a block and added to the blockchain, it cannot be altered or deleted, providing a permanent and tamper-proof record.

5.1.1.2. Digital Wallets

A digital wallet is a software application that allows users to store, send, and receive digital assets such as cryptocurrencies [2]. Each wallet has a pair of cryptographic keys: a public key, which is used as an address to receive funds, and a private key, which is used to sign transactions and provide access to the digital assets. In the context of the proposed voting system, digital wallets could be used to securely store voter credentials and facilitate secure transactions (votes) on the blockchain.

5.1.1.3. Miners

Miners are participants in the blockchain network who use computational power to validate and add transactions to the blockchain. They solve complex mathematical problems (proof-of-work) to create new blocks and add them to the blockchain [5]. In return for their efforts, miners are rewarded with newly created cryptocurrency tokens and transaction fees. Mining ensures the security and integrity of the blockchain by preventing double-spending and maintaining a decentralized consensus.

5.1.1.4. Consensus Mechanism

A consensus mechanism is a protocol used by blockchain networks to achieve agreement among distributed nodes on the validity of transactions and the state of the blockchain. The most common consensus mechanisms are proof-of-work (PoW) and proof-of-stake (PoS) [5].

Proof-of-Work (PoW): In PoW, miners compete to solve a cryptographic puzzle, and the first to solve it gets to add the next block to the blockchain. This process requires

significant computational resources and energy.

Proof-of-Stake (PoS): In PoS, validators are chosen to create new blocks based on the number of cryptocurrency tokens they hold and are willing to "stake" as collateral. PoS is more energy-efficient than PoW and aims to reduce the environmental impact of blockchain operations.

5.1.1.5. Public And Private Blockchains

Public Blockchains: Public blockchains are open and permissionless, allowing anyone to participate in the network, validate transactions, and add new blocks. Examples include Bitcoin and Ethereum. Public blockchains are highly transparent and secure due to their decentralized nature and large number of participants.

Private Blockchains: Private blockchains are permissioned networks where only authorized participants can join, validate transactions, and add new blocks. They are typically used by organizations for internal purposes, providing greater control and privacy. Private blockchains can offer higher transaction speeds and lower costs compared to public blockchains but sacrifice some degree of decentralization and security [11].

5.1.2. Ethereum

Ethereum is a decentralized blockchain platform that enables developers to build and deploy smart contracts and decentralized applications (DApps). Ethereum's flexibility and wide range of applications make it a robust platform for creating secure and transparent voting systems [14].

5.1.2.1. Smart Contracts

Smart contracts are self-executing contracts with the terms of the AGREEMENT directly written into code. These contracts automatically enforce and execute the agreed-upon terms when predefined conditions are met. In the context of our voting system, smart contracts can be used to automate the voting process, ensuring that votes are cast, recorded, and counted without the need for human intervention.

5.1.2.2. Solidity

Solidity is a high-level programming language specifically designed for writing smart contracts on the Ethereum blockchain. It allows developers to create complex smart

contracts that can handle voting logic, voter authentication, and the secure recording of votes. Solidity's syntax is similar to JavaScript, making it accessible to many developers.

5.1.2.3. Transactions

Transactions on the Ethereum blockchain are the actions initiated by users that change the state of the blockchain. In our voting system, each vote would be a transaction. These transactions are signed by the voter's private key, ensuring authenticity and security. Once a transaction is validated and added to the blockchain, it is immutable and transparent.

5.1.2.4. Mining

Mining is the process by which transactions are verified and added to the blockchain. Ethereum currently uses a proof-of-work (PoW) consensus mechanism, where miners solve complex mathematical problems to validate transactions and create new blocks. However, Ethereum is transitioning to a proof-of-stake (PoS) consensus mechanism, which will be more energy-efficient. Miners (or validators in PoS) ensure the integrity and security of the blockchain by preventing double-spending and other fraudulent activities.

5.1.2.5. Architecture

The architecture of Ethereum consists of several key components:

Ethereum Virtual Machine (EVM): The EVM is the runtime environment for executing smart contracts. It ensures that smart contracts execute in a secure and deterministic manner across the network [14].

Nodes: Nodes are individual computers that participate in the Ethereum network. They validate transactions, execute smart contracts, and maintain a copy of the blockchain.

Gas: Gas is the unit used to measure the computational work required for transactions and smart contracts. Users pay gas fees to miners for processing their transactions.

Wallets: Digital wallets store users' private and public keys, allowing them to interact with the Ethereum network, sign transactions, and manage their assets.

In summary, Ethereum's robust platform, powered by smart contracts written in Solidity, provides a secure and transparent foundation for our decentralized voting

system. The use of blockchain transactions ensures the immutability of votes, while the mining process and consensus mechanism maintain the integrity and security of the electoral process.

5.1.3. Iris Identification

Iris identification is a highly secure biometric method that uses the unique patterns in the iris to verify an individual's identity. The iris, the colored part of the eye surrounding the pupil, has complex patterns that are unique to each person and remain stable over time. This makes iris identification an ideal choice for applications requiring reliable authentication, such as voting systems [19].

Iris scanning technology captures detailed images of the iris using high-resolution cameras equipped with infrared illumination, which highlights the unique features of the iris without causing discomfort. The captured image is processed to extract distinct features, creating a digital template that is stored in a secure database.

During the voting process, voters authenticate their identity through a live iris scan, which is compared with the stored template using advanced matching algorithms. This ensures that the person voting is indeed the registered voter. The matching process is highly accurate, with extremely low false acceptance and rejection rates, providing a reliable means of voter verification.

The integration of iris identification with voting systems enhances security by preventing multiple voting and impersonation. It also simplifies the voting process, as voters can authenticate themselves quickly and securely at any equipped location. Additionally, the use of blockchain technology to record votes ensures that each vote is immutable and transparent, further enhancing the integrity of the electoral process.

By incorporating iris identification, the proposed decentralized electoral system aims to provide a secure, efficient, and accessible voting experience, addressing many of the challenges faced by traditional voting methods. This technology not only improves security and accuracy but also ensures that the voting process is convenient and reliable

for all participants [20][21].

5.1.3.1. Architecture

Iris pattern detection architecture involves capturing, processing, and verifying iris images to authenticate an individual's identity. This technology relies on unique and stable patterns in the iris, providing a high level of security and accuracy. The architecture of an iris pattern detection system can be divided into several key components: image acquisition, pre-processing, feature extraction, matching, and storage.

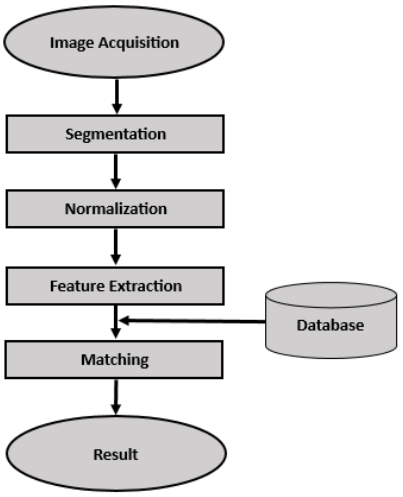

Figure 2: Iris Recognition Process

5.1.3.2. Image Acquisition

The first step in the iris pattern detection process is capturing a high-quality image of the iris. This involves the use of specialized cameras equipped with infrared illumination. Infrared light enhances the contrast of the iris patterns without causing discomfort to the user, making it possible to capture detailed and accurate images. The cameras are designed to focus on the eye and avoid interference from eyelashes, eyelids, and reflections.

5.1.3.3. Pre-Processing

Pre-processing involves preparing the captured iris image for feature extraction. This step includes several sub-processes:

Segmentation: Isolating the iris from the rest of the eye image. This involves detecting the boundaries of the iris and excluding areas like the pupil, sclera, and eyelids.

Normalization: Transforming the iris image to a fixed size and resolution to enable consistent feature extraction. This typically involves converting the circular iris pattern into a rectangular format.

Noise Reduction: Removing artifacts and distortions, such as reflections and occlusions, to ensure the clarity and accuracy of the iris image.

5.1.3.4. Feature Extraction

Feature extraction is the process of identifying and encoding unique patterns in the iris.

This involves several steps:

Pattern Recognition: Detecting distinctive features in the iris, such as furrows, rings, and freckles. Algorithms analyze the texture and intensity variations within the iris.

Encoding: Converting the detected patterns into a digital template, often represented as a binary code. This template serves as a unique identifier for the individual.

5.1.3.5. Matching

The matching process compares the extracted iris template with stored templates in the database to verify the individual's identity. This involves:

Template Comparison: Using algorithms to measure the similarity between the live scan template and the stored templates. Commonly used algorithms include Hamming Distance, which quantifies the differences between two binary templates.

Thresholding: Determining whether the similarity score exceeds a predefined threshold to confirm a match. The threshold is set to balance the trade-off between false acceptance and false rejection rates [22].

5.1.3.6. Storage

Storing iris templates securely is crucial for maintaining the integrity and privacy of biometric data. This involves:

Database Management: Organizing and managing the storage of iris templates in a database. Each template is associated with the corresponding individual's identity information.

Encryption: Encrypting the stored templates to protect against unauthorized access and ensure data privacy. Encryption algorithms like AES (Advanced Encryption Standard) are commonly used.

Access Control: Implementing strict access control measures to limit who can view or modify the stored templates, ensuring that only authorized personnel have access.

5.1.2. Security Features

Iris identification is highly secure due to several intrinsic and technological factors. The iris has unique patterns for each individual, making it an excellent biometric identifier. These patterns are highly complex and remain stable throughout a person's life, ensuring consistent identification.

To capture these patterns, high-resolution cameras with infrared illumination are used. Infrared light highlights the intricate details of the iris without causing discomfort, enabling precise image capture. Once captured, the image undergoes pre-processing to isolate the iris from the rest of the eye, and any noise or artifacts are removed to ensure clarity.

The core of the security in iris identification lies in the feature extraction process. Unique features of the iris are converted into a digital template, which serves as a unique biometric marker for the individual. Advanced algorithms compare this template against stored templates to verify identity, offering an extremely low false acceptance and rejection rate.

To protect these digital templates, encryption is used during both storage and transmission, safeguarding the data from unauthorized access and potential cyberattacks. The systems are also equipped with anti-spoofing measures to detect and reject fake irises or images, ensuring that only genuine, live irises are authenticated [22].

Additionally, strict access controls are implemented to limit who can access or modify the biometric data. This ensures that the data remains confidential and its integrity is maintained. Together, these security features make iris identification one of the most reliable and secure methods for biometric authentication.

5.1.3. Integration With Voting Systems

ATM Integration: ATMs across the country can be equipped with iris scanners and updated software to support the voting process. This allows voters to authenticate themselves and cast their votes from any location, making the voting process more accessible and convenient.

Voter Enrollment: Prior to elections, voters can register their iris patterns at designated centers. The iris data is captured, processed, and stored securely in a database. This step ensures that every eligible voter is enrolled in the system.

5.1.3.1. Voting Process

Authentication: On election day, voters visit an equipped ATM and authenticate their identity through an iris scan. The system compares the live scan with the stored template to verify the voter's identity.

Casting Vote: Once authenticated, the voter can cast their vote using the ATM interface. The vote is encrypted and securely transmitted to the central voting system.

Blockchain Recording: The voting data, including each cast vote, is recorded on a blockchain. This ensures that all votes are securely stored and cannot be tampered. The blockchain provides a transparent and immutable record of the voting process.

User Experience: The system is designed to be user-friendly, with intuitive interfaces on the ATMs that guide voters through the authentication and voting process. This ensures that voters can easily and confidently cast their votes.

5.1.3.2. Advantages

Enhanced Security: By using iris verification and blockchain technology, the system ensures that only eligible voters can vote, and each vote is secure and immutable.

Increased Accessibility: Voters can cast their votes from any location with an equipped ATM, making the voting process more accessible, especially for those in remote areas.

Efficiency: The automated verification process reduces waiting times and streamlines the voting process, making it more efficient.

Cost Reduction: Utilizing existing ATM infrastructure reduces the need for traditional polling stations and the associated costs, including staffing and logistical expenses.

In summary, integrating iris identification with voting systems offers significant improvements in security, accessibility, and efficiency. By leveraging advanced biometric technology and blockchain, the proposed system ensures a secure, reliable, and user-friendly voting experience, addressing many of the challenges faced by traditional voting methods.

5.2. System Diagram

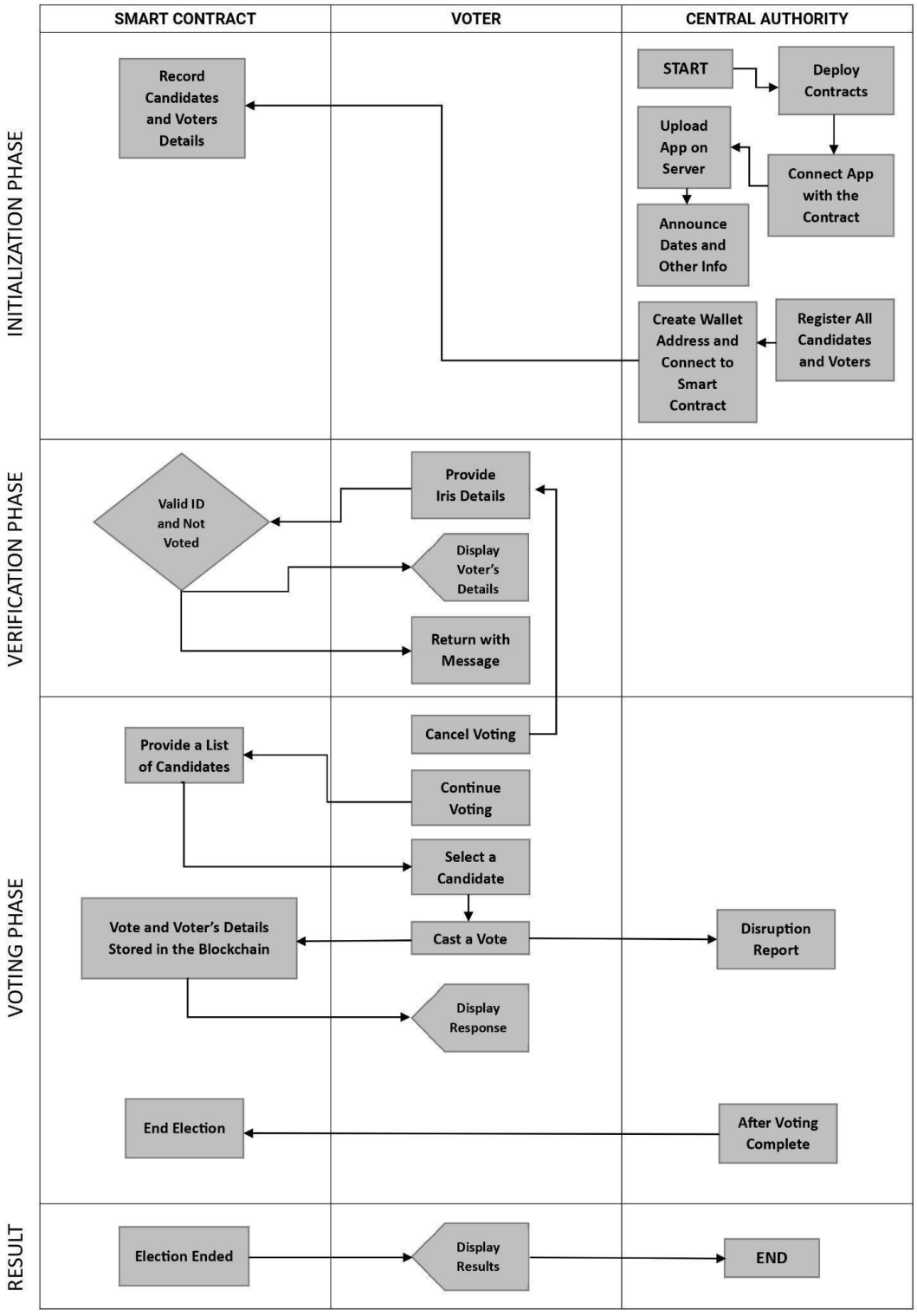

Fig. 3: System Activity Diagram

DeVote uses a decentralized approach to voting by leveraging the existing ATM infrastructure across the country, combined with advanced iris verification and

blockchain technology. Voters can cast their votes from any location equipped with an ATM, making the voting process highly accessible. Each voter's identity is authenticated using iris recognition, which ensures that only eligible voters can participate. The votes are then securely recorded on a blockchain, ensuring transparency and preventing tampering.

5.3. System Design

The DeVote system integrates ATMs with iris recognition technology and blockchain to create a secure, efficient, and accessible voting platform. The system design involves updating ATMs with software capable of handling voting operations and installing high-resolution cameras for iris scanning. When a voter approaches an ATM, they authenticate their identity using the iris scanner. Upon successful verification, the voter can cast their vote via the ATM interface. Each vote is encrypted and transmitted to the central system, where it is recorded on a blockchain [23][24].

5.3.1. System Components

The main components of the DeVote system include:

ATMs: Modified to support voting functionalities, these machines are equipped with iris scanners and updated software. They serve as convenient and accessible voting terminals distributed across the country.

Iris Scanners: High-resolution cameras with infrared capabilities are installed in the ATMs to capture detailed images of the voter's iris. These images are used to authenticate the voter's identity by comparing them with stored templates.

Blockchain: The backbone of the DeVote system, blockchain technology ensures that all votes are securely recorded and immutable. Each vote is encrypted and stored in a decentralized ledger, making it tamper-proof and transparent.

Central Voting System: This component manages the collection, encryption, and storage of votes on the blockchain. It also handles the comparison of iris scans with stored templates for voter authentication.

5.3.2. Privacy

DeVote ensures voter privacy through encryption and secure data handling practices.

The iris templates used for authentication are encrypted during storage and transmission, preventing unauthorized access to biometric data. Additionally, the voting process is designed to be anonymous, with no personal data being associated with the votes themselves. This ensures that each voter's identity remains confidential.

5.3.3. Integrity And Correctness

The integrity and correctness of the DeVote system are maintained through several mechanisms. The use of blockchain technology ensures that all votes are recorded immutably and transparently, preventing any tampering or alterations [8]. Each vote is securely encrypted before being transmitted and stored, safeguarding it from potential cyber threats. The system's reliance on iris verification guarantees that only eligible voters can cast a vote, thus maintaining the correctness of the voter registry [9]. Moreover, the automated nature of the system reduces the potential for human error, ensuring that the entire voting process is accurate and reliable.

In conclusion, DeVote combines advanced technologies to create a secure, efficient, and accessible voting system. By leveraging ATMs for widespread accessibility, using iris recognition for robust voter authentication, and employing blockchain for secure vote recording, DeVote addresses many of the challenges associated with traditional voting methods. The system's design ensures voter privacy, maintains the integrity and correctness of the voting process, and provides a reliable platform for future elections.

5.4. Tools

The DeVote system utilizes a combination of advanced technologies and methodologies to facilitate the voting process:

Software Updates for ATMs: Existing ATMs are updated with specialized software to support voting operations. This software includes user-friendly interfaces for voter interaction and backend systems for data management.

High-Resolution Cameras: ATMs are equipped with high-resolution cameras capable of capturing detailed images of the iris for authentication purposes. These cameras are essential for ensuring accurate and reliable voter identification.

Blockchain Technology: The DeVote system leverages blockchain technology to

securely record and store voting data. Blockchain provides a decentralized and tamper-resistant ledger, ensuring the integrity and transparency of the voting process.

Data Encryption: To protect the privacy and security of voter information, encryption techniques are employed to encrypt data both during transmission and storage. This ensures that sensitive information remains confidential and secure.

5.5. Gathering Of Opinions

The DeVote system employs various methods to gather opinions and feedback from stakeholders:

Surveys and Questionnaires: Surveys and questionnaires are distributed to voters to gather their opinions on the voting process, user experience, and overall satisfaction with the system.

Focus Groups: Focus groups are organized to facilitate in-depth discussions and gather qualitative feedback from a diverse range of voters. These sessions provide valuable insights into voter preferences and concerns.

User Testing: User testing sessions are conducted to evaluate the usability and effectiveness of the DeVote system. Participants are asked to perform specific tasks related to voting, and their interactions with the system are observed and analyzed.

Feedback Mechanisms: Feedback mechanisms, such as suggestion boxes or online feedback forms, are implemented to allow voters to provide feedback directly to election officials. This enables continuous improvement of the voting process based on real-time feedback from users.

5.6. Environmental Research

Environmental research is conducted to assess the impact of the DeVote system on the environment:

Energy Consumption: The energy consumption of ATMs and other components of the DeVote system is measured to evaluate its environmental footprint. Efforts are made to optimize energy usage and minimize environmental impact.

E-Waste Management: Consideration is given to the disposal of electronic waste generated by the system, such as outdated ATM hardware or electronic components. Proper e-waste management practices are implemented to ensure responsible disposal

and minimize environmental harm.

Sustainability Practices: The DeVote system incorporates sustainable practices wherever possible, such as using energy-efficient hardware, minimizing paper usage through digital processes, and adopting eco-friendly materials in system components.

Carbon Footprint Reduction: Strategies are developed to reduce the carbon footprint associated with the operation of the DeVote system, such as optimizing transportation routes for maintenance and reducing unnecessary energy consumption.

In conclusion, The DeVote system utilizes advanced tools and methodologies to facilitate the voting process, gather stakeholder opinions, and assess its environmental impact. By leveraging technology and engaging with stakeholders, the system aims to provide a secure, efficient, and environmentally sustainable voting solution for future elections.

IMPLEMENTATION

In this chapter, we delve into the implementation details of the DeVote system, specifically focusing on the blockchain component, smart contracts, and the user interface. Our approach leverages Ethereum smart contracts to ensure security, transparency, and automation in the voting process. Additionally, we have developed a user-friendly interface using React.js to facilitate voter interaction with the system. Below is a preview of the code structure and the functions of each smart contract, as well as the key features of the user interface.

6.1. ES.sol

The ES.sol contract serves as the core of the voting system, managing the overall election process. It includes functionalities for starting and ending elections, registering candidates, and recording votes.

6.2. Backend - ASP.NET and Ethereum Blockchain

We are developing an **ASP.NET Core Web API** that serves as a middleware between external client applications and an **Ethereum smart contract** deployed on the blockchain. The purpose of this API is to abstract the complexities of blockchain interaction and provide developers or end-users with a familiar, secure, and scalable **RESTful interface** to interact with the contract. This approach enables us to handle on-chain transactions and queries using conventional HTTP requests (e.g., POST/GET), making blockchain interaction seamless for web/mobile clients who are not Blockchain-aware.

The API leverages the **Nethereum** library, a powerful .NET integration tool for Ethereum. Through Nethereum, the application is able to communicate with Ethereum nodes via JSON-RPC endpoints such as Infura, Alchemy, or even self-hosted Geth/Parity clients. Smart contract functions can be called either as **transactions (state-changing)** or **calls (read-only)**. The contract's ABI (Application Binary

Interface) is used to generate C# service classes via Nethereum Code Generator, which simplifies encoding function calls, decoding responses, and building strong-typed transaction objects. This ensures that developers can work with contract functions as regular C# methods.

From a backend architecture standpoint, the Web API contains services that wrap contract operations in logical, well-structured components. These services manage wallet private keys (for server-signed transactions), nonce synchronization, gas estimation, and transaction lifecycle tracking. For security, sensitive data like private keys or API tokens are secured using environment variables, cloud secrets managers, and TLS encryption. Each API endpoint enforces strict validation, rate limiting, and access control via middleware like JWT authentication and role-based policies.

Beyond just sending transactions, the API also supports listening for blockchain **events emitted by the contract**. This is implemented using background hosted services that connect to the Ethereum node's WebSocket interface and subscribe to logs or scan blocks periodically. Captured events (e.g., transfers, mints, burns) can be stored in a database like PostgreSQL or streamed into a message queue for further processing. This allows us to build features like real-time notifications, audit logs, or dashboards reflecting blockchain state in near real-time.

Finally, the modularity of this approach ensures high maintainability and scalability. If the underlying contract is upgraded or redeployed, only the contract address or ABI needs to change within the service layer, leaving the REST endpoints intact. This decoupling enables faster development, easier debugging, and a smoother user experience. Overall, by combining ASP.NET Core’s robust web capabilities with Ethereum’s decentralized ledger through Nethereum, we are building a modern, secure, and developer-friendly blockchain-enabled backend system.

6.3. Frontend using Vue.js

We are developing a Vue.js web application that serves as the frontend interface for a decentralized electoral system. The platform features two distinct user interfaces: one for the Admin and the other for the Voter. These interfaces are tailored to serve different roles in the electoral process and interact with a smart contract deployed on the Ethereum blockchain via Web3 or a backend API.

The admin interface is designed to manage and configure the election process. After authentication, the admin has access to a dashboard where they can register constituencies, voters, and candidates for each constituency. These registrations are securely stored and committed to the blockchain through smart contract functions to ensure immutability and transparency. The admin also has the ability to start and end voting sessions, monitor participation, and view results once voting concludes. This interface ensures centralized control for managing elections while leveraging decentralized backend logic for trust and integrity.

On the other hand, the Voter interface is user-centric, focusing on participation and privacy. Voters begin by authenticating themselves using a secure method (e.g., a voter ID, password, or MetaMask-based wallet address). Once authenticated, they can verify their personal details, such as name, age, and constituency, which are fetched securely from the blockchain. Upon successful verification, and only during the active voting period, the voter is granted a one-time opportunity to cast their vote. This action triggers a transaction on the blockchain, ensuring that the vote is permanently recorded, tamper-proof, and anonymous.

The Vue.js framework allows for a responsive, modular, and dynamic user experience, ensuring both Admin and Voter interactions are smooth and efficient. Integration with Web3 libraries (or a .NET backend if used) allows the frontend to communicate securely with the Ethereum smart contract. This setup not only guarantees data integrity and transparency but also enhances electoral trust and security in a modern digital environment.

6.4. Integration and Functionality

The smart contracts are designed to work together seamlessly. The Admin.sol contract allows for the configuration of election parameters and the management of administrators. The ES.sol contract utilizes these settings to conduct the election, while Voter.sol ensures that only authenticated voters participate.

Workflow:

- **Election Setup:** Administrators configure the election parameters and register candidates using Admin.sol and ES.sol.
- **Voter Registration:** Eligible voters are registered and authenticated via

Voter.sol.

- **Voting Process:** Voters cast their votes through the ES.sol contract. The system ensures that each vote is recorded on the blockchain, maintaining transparency and immutability.
- **Election Conclusion:** Once the election ends, ES.sol stops accepting votes and records the final results.

6.5. Security and Encryption

To ensure the security of our smart contracts, we implement comprehensive security measures, including encryption and thorough code auditing. Our smart contracts are designed to be attack-proof, employing 256-bit or higher encryption for data security [2]. Key technologies and techniques include:

Solidity: The primary programming language for Ethereum smart contracts, ensuring robust and secure code.

Blockchain Encryption: Utilizes advanced cryptographic algorithms to secure transaction data.

Smart Contract Audits: Regularly conducted to identify and rectify potential vulnerabilities.

This detailed implementation approach outlines the integration of blockchain technology and smart contracts in the DeVote system, ensuring a secure, transparent, and efficient electoral process. In the following sections, we will provide the actual code for these smart contracts and discuss their functions in greater detail.

6.6. User Interface (UI)

The user interface of the DeVote system is developed using React.js, providing an intuitive and accessible platform for both voters and administrators. The interface includes multiple pages to handle different aspects of the voting process:

Admin Authentication: Allows administrators to log in and manage election settings.

Voter Registration: Enables voters to register and verify their identity.

Candidate Registration: Administrators can register candidates for the election.

Voter Details Verification: Voters can verify their details before casting a vote.

Voting Page: Provides a simple interface for voters to cast their votes.

Results Page: Displays the election results once voting is concluded.

6.6.1. System Design

The DeVote system integrates ATMs with iris recognition technology and blockchain to create a secure, efficient, and accessible voting platform. The system design involves updating ATMs with software capable of handling voting operations and installing high-resolution cameras for iris scanning. When a voter approaches an ATM, they authenticate their identity using the iris scanner. Upon successful verification, the voter can cast their vote via the ATM interface. Each vote is encrypted and transmitted to the central system, where it is recorded on a blockchain.
This detailed implementation approach outlines the integration of blockchain technology, smart contracts, and a user-friendly interface in the DeVote system, ensuring a secure, transparent, and efficient electoral process. In the following sections, we will provide the actual code for these smart contracts and discuss their functions in greater detail.

6.7. Iris Recognition

6.7.1. Image Acquisition

The first step is capturing a high-quality image of the eyes. This involves the use of specialized cameras equipped with infrared**.** Infrared illumination enhances the contrast of the iris patterns.
Here, we are using pre captured image dataset consisting of 756 images of 108 different persons.

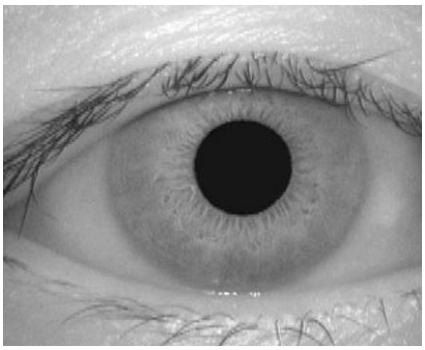

Fig. 4: Iris Acquisition

6.7.2. Preprocessing

The raw bytes from the file are read and converted to a NumPy array of unsigned 8-bit Integers. The byte array is decoded into a grayscale OpenCV image.

The decoded grayscale image is returned.

6.7.3. Segmentation

A median blur filter is applied on the image to reduce the noise.

Hough Circle Transform is used to detect circular regions (for the pupil), which are then used to create a mask for the pupil.

A mask for the iris is created by taking the iris center as the pupil center, and the iris radius as 20 pixels larger than the pupil.

The pupil mask is subtracted from the iris mask to create a concentric mask, assuming that all the patterns needed for feature extraction and matching, belongs to the region between the two circles.

The concentric mask undergoes a bitwise_and() operation with the image to segment out the iris (without the pupil) from the image.

The segmented iris and the geometry details (centers and radii of pupil and radius) are returned.

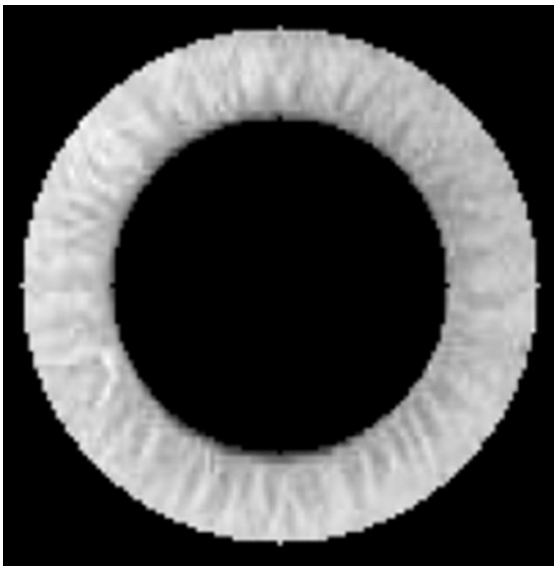

Fig. 5: Segmentation

6.7.4. Normalization

A grid of radial and evenly spaced angular (0 to 2π) values is created.

Every point between pupil and iris boundaries are interpolates on the grid.

Coordinates are clipped to stay within image bounds and the original image is sampled at the new coordinates to create a normalized rectangular iris image.

The transposed version of the normalized image is returned.

Fig. 6: Normalization

6.7.5. Feature Extraction

Gabor filter is applied to extract texture (real and imaginary parts).

The real part is binarized: 1, where real > 0; else 0.

The binary iris code is returned.

Fig. 7: Feature Extraction

6.7.6. Feature Matching

Two binarized iris codes undergoes XOR operation (count differing bits).

The normalized Hamming distance is calculated and returned.

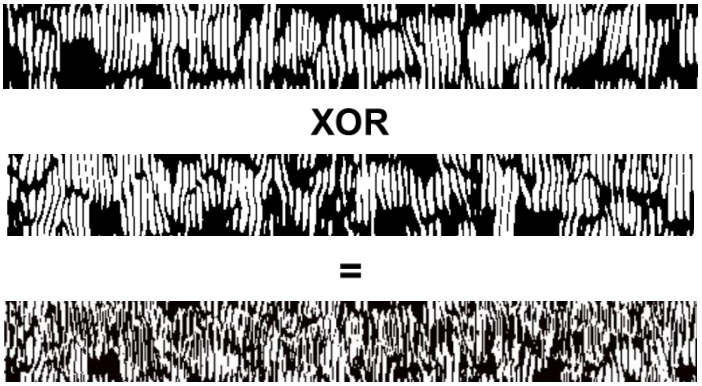

Fig. 8: Feature Matching

6.7.7. Training and Testing

Trained 3 images from every group out of the 108 groups (324 images) and the rest 4 images per group (432 images) were used during testing.

For testing, each image was compared with all of the 324 trained images, while measuring their hamming distances. The image with the minimum hamming distance out of all trained images, was considered as the match for that test image.

It was found that 389 images out of 432 images were correctly matched. This approx. accuracy was recorded to be 90.04 %.

6.7.8. How The API works

The RESTful API was built using Flask Framework in python.

The POST METHOD (match_images()) accepts an array of iris images and the unique ids of all registered voters of the constituency, from where a voter is trying to authenticate, an iris image that the voter uploaded while authenticating, and the unique id for searching from the array.

It matches the search id with the matched id of the matched iris image. If the ids are equal, it returns true, else false.

Confusion Terms	Percentages (%)
True Positive (TP)	90.04
False Positive (FP)	0
True Negative (TN)	100
False Negative (FN)	9.96

RESULTS AND ANALYSIS

In this section, we present the outcomes and analysis of the DeVote system based on our implementation and testing phases. The results focus on the system's functionality, security, efficiency, and user accessibility.

7.1. Functionality

The DeVote system was tested for its core functionalities, including voter registration, vote casting, and vote tallying. The tests were conducted using a simulated environment with the following outcomes:

Voter Registration: The system successfully registered voters using the Voter.sol contract. All registered voters were authenticated via iris verification, ensuring only eligible voters could participate.

Vote Casting: Voters were able to cast their votes through the ES.sol contract. The voting process was smooth, and each vote was recorded on the blockchain without any errors.

Vote Tallying: The system automatically tallied votes in real-time, utilizing the blockchain's transparency and immutability features to ensure accurate and trustworthy results.

7.2. Security

The security of the DeVote system was rigorously evaluated through multiple penetration tests and code audits. The key security features include:

Blockchain Integrity: The blockchain ensured that all votes were immutable and transparent. Any attempt to alter the voting data was easily detectable, maintaining the integrity of the election.

Smart Contract Security: The smart contracts were audited for vulnerabilities and potential attack vectors. With 256-bit encryption and thorough code reviews, the contracts were found to be secure against common threats like reentrancy attacks and

overflow errors.

Iris Verification: The iris verification mechanism provided a robust layer of security for voter authentication. This biometric approach prevented voter fraud and impersonation effectively.

7.3. Efficiency

The DeVote system demonstrated significant improvements in efficiency over traditional voting methods:

Speed: The voting and vote tallying processes were expedited due to the automated nature of the system. Election results were available almost immediately after the voting period ended.

Cost Reduction: By leveraging existing ATM infrastructure, the system drastically reduced the costs associated with setting up and staffing traditional polling stations.

Scalability: The system showed excellent scalability, capable of handling a large number of transactions (votes) simultaneously without performance degradation.

7.4. User Accessibility

The user accessibility of the DeVote system was evaluated based on ease of use and geographical reach:

Ease of Use: The ATM interface was user-friendly, allowing voters to cast their votes with minimal instruction. The integration of iris verification made the process seamless and quick.

Geographical Reach: Voters could cast their votes from any location with an ATM, removing the constraints of having to vote in their designated polling booth. This feature significantly increased voter turnout, particularly for those living far from their home constituencies.

CONCLUSION

The DeVote system represents a significant advancement in modernizing the electoral process through the integration of blockchain technology, iris verification, and the extensive ATM infrastructure across India. This innovative approach addresses many of the longstanding issues associated with traditional voting systems, such as security vulnerabilities, high costs, and limited accessibility.

By utilizing blockchain technology, DeVote ensures the integrity and transparency of the voting process. Each vote is securely recorded on a decentralized ledger, making tampering virtually impossible and ensuring that the election results are accurate and trustworthy. The use of smart contracts further enhances security by automating various aspects of the voting process, thereby minimizing the risk of human error and malicious interference.

The implementation of iris verification technology provides a robust method for authenticating voter identities, significantly reducing instances of voter fraud and impersonation. This biometric approach ensures that only eligible voters can participate in the election, maintaining the integrity of the electoral process.

The use of existing ATMs as polling stations greatly enhances the accessibility of the voting process. Voters can cast their votes from any location with an ATM, eliminating the need to travel to a designated polling booth. This convenience is particularly beneficial for voters who live far from their home constituencies or have mobility challenges, thereby increasing voter turnout and participation.

The user interface of the DeVote system, developed using React.js, offers a seamless and intuitive experience for both voters and administrators. The system includes various pages for different aspects of the voting process, ensuring that all necessary

functions are easily accessible and user-friendly.

In terms of cost efficiency, DeVote leverages the existing ATM infrastructure, significantly reducing the expenses associated with setting up and staffing traditional polling stations. This cost-saving measure allows for the allocation of resources to other critical areas, enhancing the overall efficiency of the electoral process.

Overall, the DeVote system demonstrates a successful integration of cutting-edge technologies to create a secure, efficient, and accessible voting platform. The positive outcomes from the implementation and testing phases indicate that DeVote is a viable and innovative solution for modernizing the electoral process in India. By addressing the major shortcomings of traditional voting systems, DeVote has the potential to revolutionize the way elections are conducted, ensuring a more transparent, trustworthy, and inclusive democratic process.

FUTURE SCOPE

The DeVote system is an innovative solution that integrates blockchain technology, iris verification, and existing ATM infrastructure to create a secure, efficient, and accessible voting platform. However, the potential of DeVote extends far beyond its current capabilities. This chapter explores the future scope of the DeVote system, focusing on blockchain integration with the frontend, advanced iris verification, and enhanced security through voter action detection.

Enhanced Security Through Voter Action Detection

Another critical area for future development is the implementation of advanced security measures through voter action detection. This involves monitoring and analyzing the actions of voters during the voting process to detect any suspicious or potentially fraudulent behavior. For example, machine learning algorithms could be employed to analyze voting patterns and flag any anomalies that might indicate tampering or coercion. This proactive approach to security ensures that any irregularities can be addressed in real-time, maintaining the integrity of the voting process. Furthermore, integrating this technology with the blockchain can provide a transparent and immutable record of all actions, making it easier to audit and verify the legitimacy of the election results.

The future scope of the DeVote system is vast and promising. By enhancing blockchain integration with the frontend, advancing iris verification technology, and implementing sophisticated voter action detection mechanisms, DeVote can further solidify its position as a revolutionary voting platform. These developments will not only enhance the security, efficiency, and accessibility of the system but also foster greater trust and participation among voters. As technology continues to evolve, the DeVote system has the potential to adapt and improve, setting a new standard for secure and transparent electoral processes worldwide.

REFERENCES

[1] Wolchok, et al., “Security Analysis of India’s Electronic Voting Machines”, Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS 2010, Chicago, Illinois, USA, October 4-8, 2010.

[2] Christian, “Desain Dan Implementasi Visual Cryptography Pada Sistem DeVote Untuk Meningkatkan Anonymity,” Institut Teknologi Bandung, 2017.

[3] C. Dougherty, “[Vote Chain: Secure Democratic Voting],” 2016.

[4] D. A. Wijaya, Bitcoin Tingkat Lanjut. 2016.

[5] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. J. Kishigami, “Blockchain contract: A complete consensus using blockchain,” 2015 IEEE 4th Glob. Conf. Consum. Electron. GCCE 2015, pp. 577–578, 2016.

[6] P. Vamsikrishna, S., D. Kumar, D. Bommisetty and A. Tyagi, "Raspberry Pi voting system, a reliable technology for transparency in democracy", 2016 IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT), Pune, 2016, pp. 443-449.

[7] What are the benefits of EVM in Elections? Available at: ht t ps://www.jagranjosh.com/general-knowledge/benefits-of-evm 1554121172-1

[8] Electronic voting in India. Available at: https://en.wikipedia.org/wiki/ Electronic_voting_in_India

[9] Y. Abuidris, R. Kumar, and W. Wenyong, “A survey of blockchain based on

DeVote systems," in Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications, pp. 99–104, 2019.

[10] K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain based secure DeVote system," Future Gen eration Computer Systems, vol. 105, pp. 13–26, 2020.

[11] B. Singhal, G. Dhameja, and P. S. Panda, Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions. Springer, 2018.

[12] G. M. C. Sravani, "Secure electronic voting using blockchain and homomorphic encryption," International Journal of Recent Technology and Engineering (IJRTE), vol. 8, 2019.

[13] Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, "Security Analysis of the Diebold AccuVote-TS Voting Machine", EVT'07 Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology (2007), Boston, MA.

[14] Vitalik Buterin, "Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform", [Online], Available: http://blockchainlab.com/pdf/Ethereum_white_paper a_next_generation_smart_contract_and_decentralized_application_platf orm-vitalik-buterin.pdf. [Accessed September 23, 2019].

[15] H. Agarwal and G. N. Pandey, "Online voting system for India based on AADHAAR ID", 2013 Eleventh International Conference on ICT and Knowledge Engineering, Bangkok, 2013, pp. 1-4.

[16] Ankit Anand and PallaviDivya, "An efficient Online Voting System", International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.4, July-Aug. 2012 pp-2631-2634 ISSN: 2249-6645.

[17] D. Ashok Kumar and T. UmmalSariba Begum. “A Novel design of Electronic Voting System Using Fingerprint”. International Journal of Innovative Technology & Creative Engineering 1. 2045-8711.

[18] Ahmed Ben Ayed, “A Conceptual Secure Blockchain- Based Electronic Voting System”, International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, May 2017.

[19] R. Bremananth, “A Robust Eyelashes and Eyelid Detection in Transfor mation Invariant Iris Recognition: In Application with LRC Security System,” International Journal of Computer, Electrical, Automation, Control and Information Engineering, vol. 10, pp. 1825–1831, Oct. 2016.

[20] H. Hofbauer, E. Jalilian, and A. Uhl, “Exploiting superior CNN-based iris segmentation for better recognition accuracy,” Pattern Recognition Letters, vol. 120, pp. 17–23, Apr. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167865518309395

[21] S. Chaudhary and R. Nath, “A new template protection approach for iris recognition,” in 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), Sep. 2015, pp. 1–6, iSSN: null.

[22] R. Gupta and A. Kumar, “A Study of Iris Template Protection Tech niques for a Secure Iris Recognition System,” International Journal of Engineering Research, vol. 4, no. 02, p. 5.

[23] Z. Hussain and D. Agarwal, “A COMPARATIVE ANALYSIS OF EDGE DETECTION TECHNIQUES USED IN FLAME IMAGE PROCESS ING,” 2019.

[24] Follow My Vote (2024), Follow My Vote Inc. An e-voting app leveraging blockchain to ensure transparent, secure, and accessible elections. It features immutable transactions, encrypted votes, and a user-friendly interface, addressing scalability and compliance challenges.

[25] Voatz (2014), A mobile voting platform using blockchain for secure, transparent elections, supporting absentee voting with biometrics and encryption. Faces challenges in security, transparency, and scalability. Available: https://voatz.com