International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

E-Voting System Using Machine Learning, Blockchain, and Cryptography

Ms. Mitali Jain[1], Ms. Sanskruti Raut[2], Mrs. Sheetal Ghadge[3]

University Of Mumbai IDOL

Abstract

Voting is a central component of a country's political life cycle. Privacy, authentication and integrity of citizens' votes and their data are considered to be essential to any e voting program. In order to resolve these concerns, we propose a stable e-voting system based on the principles of blockchain, machine learning and cryptography. We use blockchain for immutable vote recording, machine learning model to detect intrusion in voting data centers and e-voting stations, and cryptography for secure voter authentication and data protection. The proposed a blockchain-based e-voting system designed exclusively for physically disabled citizens who are unable to visit polling stations. The system facilitates secure, transparent, and tamper-proof voting by allowing Election Commission (EC) officials to conduct supervised voting at the voter's home using a blockchain-integrated mobile voting device. The system ensures vote integrity, voter privacy, and auditability while addressing accessibility concerns for this marginalized demographic.

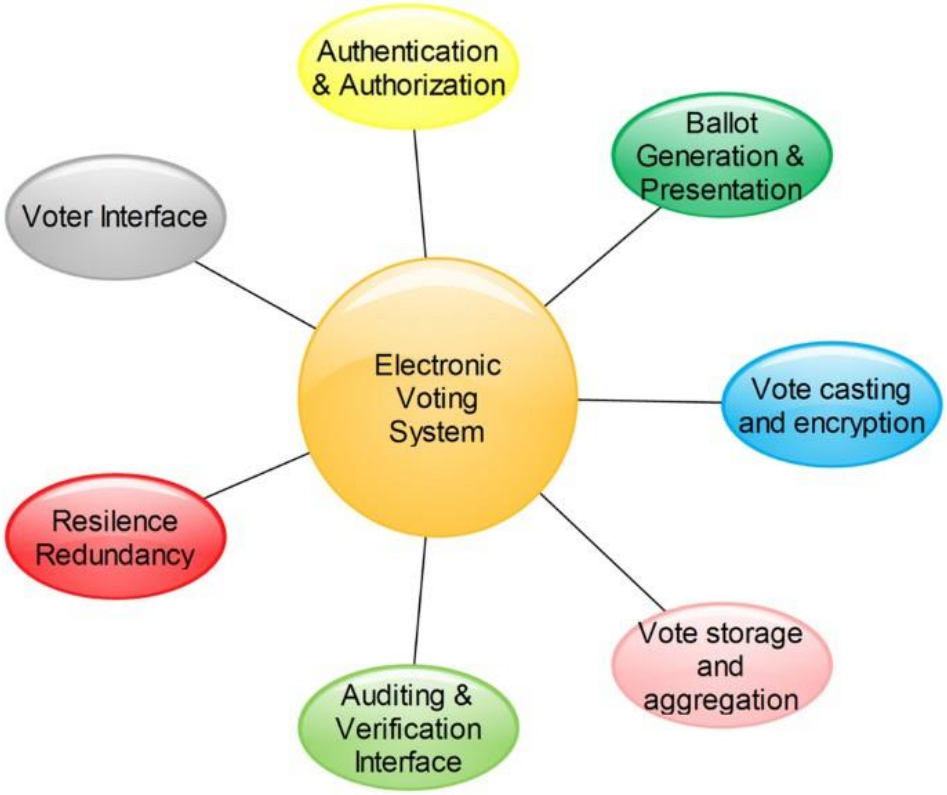
Keywords: Blockchain, Electronic Voting System, Cryptography, Machine Learning

1. Introduction

Voting is the democratic right of every citizen that allows them to choose tomorrow's leaders. Voting not only enables people to vote for political parties but also encourages them to understand the value of citizenship. A lot of people do not vote, assuming that one vote does not make a difference, but actually does. The democratic structures of the nation are established by means of elections. Voting is a crucial mechanism that keeps a nation's political structure functioning. This also gives the individual the right to question the government. Voting is a way to express the opinion of a citizen in a democratic country. Voting is crucial to the activation of a democratic process. Literature shows that the voting method has undergone significant changes in order to improve its flexibility, security, speed, cost and availability, especially during the registration and authentication of the elector, the casting of votes and the tabulation phases.

The traditional voting process often faces challenges such as voter fraud, lack of transparency, inefficiencies, and accessibility issues. With the rise of digital transformation, there is a pressing need for secure, transparent, and efficient voting systems. Integrating machine learning, blockchain, and cryptography offers a promising solution by enhancing security, verifiability, and voter trust while leveraging advanced technologies to address modern electoral demands.

Internet voting systems remain vulnerable to security threats such as cyber-attacks, vote manipulation, and lack of transparency. This project proposes a transition from conventional internet voting systems to a blockchain-based secure voting system to enhance integrity, transparency, and security.



[Anita A. Lahane1,∗, Junaid Patel1,∗∗, Talif Pathan1,∗∗∗and Prathmesh Potdar1(2020) Blockchain technology based e-voting system https://www.itm-conferences.org/articles/itmconf]

Background

The evolution of voting systems has transitioned from traditional paper ballots to modern electronic voting (e-voting) mechanisms. Initially, voters had to physically visit polling booths to cast their votes, which posed various challenges, including the need for universal voter participation and susceptibility to tampering during the manual counting process, especially in densely populated regions.[1][4].

E-voting emerged as a potential solution, promising enhanced accessibility and efficiency while addressing issues like voter disengagement and the preferences of digitally literate populations.[2][1]. However, the adoption of e-voting has not been without concerns, particularly regarding security and the integrity of electoral processes. E-voting systems are vulnerable to a range of threats such as unauthorized vote casting, impersonation, electronic ballot stuffing, and denial of service attacks. These security risks raise significant questions about the authenticity and reliability of e-voting

systems.[2][1][3].

To mitigate these risks, recent advancements have focused on integrating blockchain technology into e-voting systems. Traditional e-voting relies on centralized databases, which can be susceptible to attacks, while blockchain-based systems utilize decentralized networks that enhance security through cryptographic protocols.[4][3]. This evolution aims to provide voters with a more secure and transparent way to cast their votes, ensuring that each vote is recorded as a cryptographically secured transaction in a shared ledger, thereby improving the overall integrity of the electoral process.[4][3]. Moreover, the incorporation of machine learning and advanced cryptographic techniques into e-voting systems is emerging as a promising avenue for enhancing security and usability. These technologies can provide robust authentication methods and improve voter identification processes, further safeguarding against electoral fraud and ensuring the integrity of the voting experience.[5][6].

As the landscape of e-voting continues to evolve, it becomes increasingly important to address both the technological and regulatory challenges associated with its implementation, ensuring compliance with legal standards while fostering public trust in electoral systems.[3][7]

Problem Statement:

Traditional voting systems are plagued with multiple limitations that undermine electoral integrity:

- Manual voting processes are time-consuming and resource-intensive.
- Paper-based systems create security concerns during voting and counting.
- Centralized databases are prone to hacking and cyber-attacks.
- Manual counting introduces probabilities for errors and inconsistencies
- Current systems provide limited guarantees that all votes are counted correctly, and are susceptible to manipulation.
- Difficulty in ensuring voter privacy while maintaining transparency.
- Vulnerability to various forms of election fraud and manipulation such as double voting, ballot stuffing, voter impersonation and electronic tampering.

These limitations – the time-consuming manual processes, security vulnerabilities of paper-based systems, potential for counting errors, lack of vote guarantees, privacy concerns, and susceptibility to fraud – highlight the critical need for a technologically advanced voting system that can enhance security, efficiency, and trust in electoral processes.

Proposed Solution:

The proposed e-voting system integrates three key technologies to create a secure, transparent, and efficient voting platform:

1. Blockchain Technology:
   - Provides a decentralized, immutable ledger for recording votes
   - Implements Merkle trees for efficient verification of transactions

- Stores root hashes derived from the Merkle hash tree to maintain data integrity
- Creates a tamper-proof record visible to all stakeholders
- Enables blockchain-based digital identity for secure voter registration

2. Machine Learning Components:

- Implements Support Vector Machines (SVM) for intrusion detection
- Uses both Gaussian Vector Support Machine and linear Vector Support Machine models
- Strategically places Intrusion Detection Systems at network borders and within voting station networks
- Analyzes network traffic patterns to identify potential security threats
- Evaluates model performance based on accuracy and Area Under Curve (AUC) metrics

3. Cryptographic Techniques:

- Employs Elliptic Curve Cryptography (ECC) for encrypting voter data
- Uses the state elections office's elliptical public key for encryption
- Implements secret share slicing of encrypted ballots before transmission to blockchain nodes
- Ensures voter privacy while maintaining system transparency
- Prevents identification of specific votes while allowing verification

Integration of Technologies:

The combination of cryptography, blockchain, and machine learning creates a robust framework for the e-voting system. Cryptography ensures the security and authenticity of the votes cast, while blockchain provides a transparent and tamper-proof ledger for vote storage. Machine learning enhances the overall effectiveness of the voting process by enabling data-driven strategies that improve voter engagement and campaign performance. This integrated approach not only enhances security and transparency but also promotes greater public trust in the electoral process.

Research Objectives:

- Enable **secure home voting** for physically disabled citizens.
- Design a secure and transparent e-voting framework.
- Implement blockchain-based digital identity for voter registration.
- Use cryptography to ensure vote confidentiality and integrity.
- Use machine learning to detect anomalies or verify voter authenticity.
- Evaluate system performance in terms of security, scalability, and usability.
- Ensure compliance with electoral requirements for security, privacy, and auditability

Goals for the Proposed System:

- **Voter Registration Time**: Aim for <1 minute per voter using blockchain digital identity.

- **Vote Processing Time**: Target <5 seconds per vote with ML and cryptography.
- **Fraud Detection Rate**: Achieve >95% accuracy with ML algorithms.
- **System Uptime**: Ensure 99.9% availability during election periods.
- **Cost per Vote**: Reduce to $0.10-$0.50 per vote compared to $1-$2 for paper-based systems.

2. Related Work

Existing e-voting systems include Estonia's blockchain-based voting and India's e-voting trials, demonstrating the feasibility of digital elections.

Estonia, a pioneer in e-voting, reported that 44.4% of votes in the 2019 parliamentary election were cast online, up from 5.5% in 2005 when it first introduced internet voting. Additionally, countries such as Switzerland and Brazil have experimented with electronic voting, leveraging cryptographic security measures.

These applications indicate a global trend towards the adoption of secure and transparent digital voting solutions. Several e-voting implementations have been developed with varying approaches:

- Traditional Online Voting Systems: Systems using PHP and SQL databases provide basic functionality but lack the security features of more advanced technologies. These systems typically allow voters to use an ID and PIN to vote for their preferred candidate.
- BlockVOTE Architecture: This framework leverages smart contract capabilities of blockchain technology, encompassing three main steps: poll creation, voting, and result tallying. The system requires preparation of candidate lists before poll creation, after which voters can securely cast their votes.
- Ethereum-Based Systems: Some implementations utilize Ethereum as a blockchain network for e-voting, providing a foundation for developing secure, transparent systems through smart contract capabilities.
- Hybrid Cryptographic Systems: Certain applications combine multiple cryptographic algorithms (such as AES and RSA) with blockchain technology to achieve enhanced security while addressing computational challenges.

While these applications demonstrate progress in electronic voting technology, they also highlight limitations that our proposed system aims to address through the integration of blockchain, machine learning, and advanced cryptography.

3. Proposed System Design

This system design integrates blockchain for transparency, machine learning (ML) for fraud detection, and cryptography for security to address challenges in traditional e-voting systems. Below is the detailed architecture, components, and workflows.

1. System Architecture

1.1 Layered Architecture

The system is divided into four layers for modularity and scalability:

Layer	Component
User Interface	Voter/Candidate Registration Portal, Voting Interface, Admin Dashboard
Application Logic	Smart Contracts, ML Models, Cryptographic Modules, Identity Management
Blockchain Network	Ethereum/Hyperledger Fabric Nodes, Merkle Trees, Distributed Ledger
Data Storage	Encrypted Ballots (On-Chain), Voter Metadata (Off-Chain), ML Training Datasets

2. Core Components

2.1 Blockchain Module

- Framework: Hybrid blockchain (public Ethereum for transparency + permissioned Hyperledger Fabric for voter identity management).
- Key Features:
- Smart Contracts (Solidity/Chaincode):
- RegistrationContract: Validates voter eligibility via unique blockchain identity..
- Voting Contract:Records encrypted votes as transactions.
- TallyingContract: Automates vote counting post-election.
- Merkle Trees: Store root hashes of votes for tamper-proof verification.
- Consensus Mechanism: Proof-of-Authority (PoA) for fast, energy-efficient validation.

2.2 Machine Learning Module

- **Intrusion Detection System (IDS):**
- Models:
- Gaussian/Linear SVMs (as in[12]) for detecting DDoS attacks and anomalous voting patterns.
- LSTM Networks for real-time network traffic analysis.
- Placement:
- Border IDS: Monitors traffic between voting stations and data centers.
- Central IDS: Analyzes intra-network traffic within voting stations.

- **Fraud Prediction:**
- Trained on historical election data to flag suspicious activities (e.g., sudden voter surges).

2.3 Cryptographic Module

- **Elliptic Curve Cryptography (ECC):**
- Encrypts voter data using the election authority's public key (12).
- Generates unique digital signatures for voters.
- **Hybrid Encryption:**
- AES-256 for encrypting ballots.
- RSA-2048 for secure key exchange.
- Secret Sharing: Ballots are split into shards using Shamir's Secret Sharing before blockchain storage (11).

5. Security & Privacy Mechanisms

Feature	Implementation
Voter Anonymity	zk-SNARKs to prove vote validity without revealing voter identity.
Tamper Resistance	Merkle roots stored on-chain; any alteration breaks the hash chain.
Coercion Resistance	"Fake ballot" generation option to mislead coercers (11).
DDoS Mitigation	SVM-based IDS filters malicious traffic at network borders (12).
Quantum Resistance	Hybrid ECC + AES encryption with post-quantum algorithms (e.g., NTRU).

6. Performance Optimization

- Off-Chain Computation: Heavy ML tasks (fraud detection) are processed off-chain to reduce latency.
- Sharding: Blockchain network divided into subnets (e.g., by region) to improve transaction speed.
- Lightweight Clients: Voters use SPV (Simplified Payment Verification) wallets to verify votes without syncing the full chain.

7. Implementation Challenges & Solutions

Challenges	Solution
Scalability	Layer-2 solutions (Plasma/Rollups) for high-throughput elections.
Voter Accessibility	Offline kiosks with biometric authentication for low-internet regions.
Regulatory Compliance	Permissioned blockchain mode for GDPR-compliant voter data handling.
Usability	Multilingual UI with voice-guided voting for non-tech users.

4. Methodology

1. Voter Registration and Authentication

- During voter registration, the system creates a unique cryptographic key-pair(Public key+Private key).
- This key pair is stored in a decentralized blockchain ledger.
- Personal data is encrypted using AES encryption to protect voter identity.
- Each voter is issued a unique blockchain identity.

2. Vote Casting Process

- During voting, the voter signs the transaction with their private key.
- The system verifies their public key and allows them to vote.
- The system displays election candidates in an interactive voting interface.
- Upon vote selection, the system encrypts the vote using RSA encryption.
- The encrypted vote is recorded in a block on the blockchain, ensuring immutability.

- Smart contracts verify that a voter cannot vote more than once.

3. Fraud Detection Using Machine Learning

- The ML model analyzes voting patterns in real-time.
- If an anomaly is detected (e.g., multiple votes from one device, suspicious activity), the system flags the vote for review.
- Supervised learning algorithms like Random Forest or SVM (Support Vector Machine) classify votes as valid or fraudulent.

4. Blockchain Integration for Vote Security

- Each vote is stored as a transaction in a decentralized blockchain network.
- Blockchain ensures tamper-proof storage—once a vote is recorded, it cannot be modified.
- A hash function (SHA-256) secures transactions, ensuring data integrity.

5. Vote Verification and Counting

- Smart contracts execute automated vote tallying.
- The final count is publicly verifiable on the blockchain while maintaining voter anonymity.
- Results are displayed in a real-time dashboard with graphical analytics.

6. System Security and Privacy Protection

- Multi-layered security: Firewall, end-to-end encryption, and access control mechanisms.
- Distributed Ledger ensures no single entity can alter votes, increasing election integrity.

7. Result Declaration & Public Transparency

- Once the voting period ends, the system automatically generates results.
- Results are stored in an immutable blockchain ledger.
- A public dashboard displays real-time statistics without compromising voter privacy.

- **Technologies Used:**

- Blockchain: Ethereum for smart contracts, or Hyperledger for permissioned access.
- Machine Learning: Algorithms like convolutional neural networks (CNNs) for biometric authentication, anomaly detection models (e.g., Isolation Forest).
- Cryptography: AES for vote encryption, RSA/ECC for digital signatures, zero-knowledge proofs for privacy.

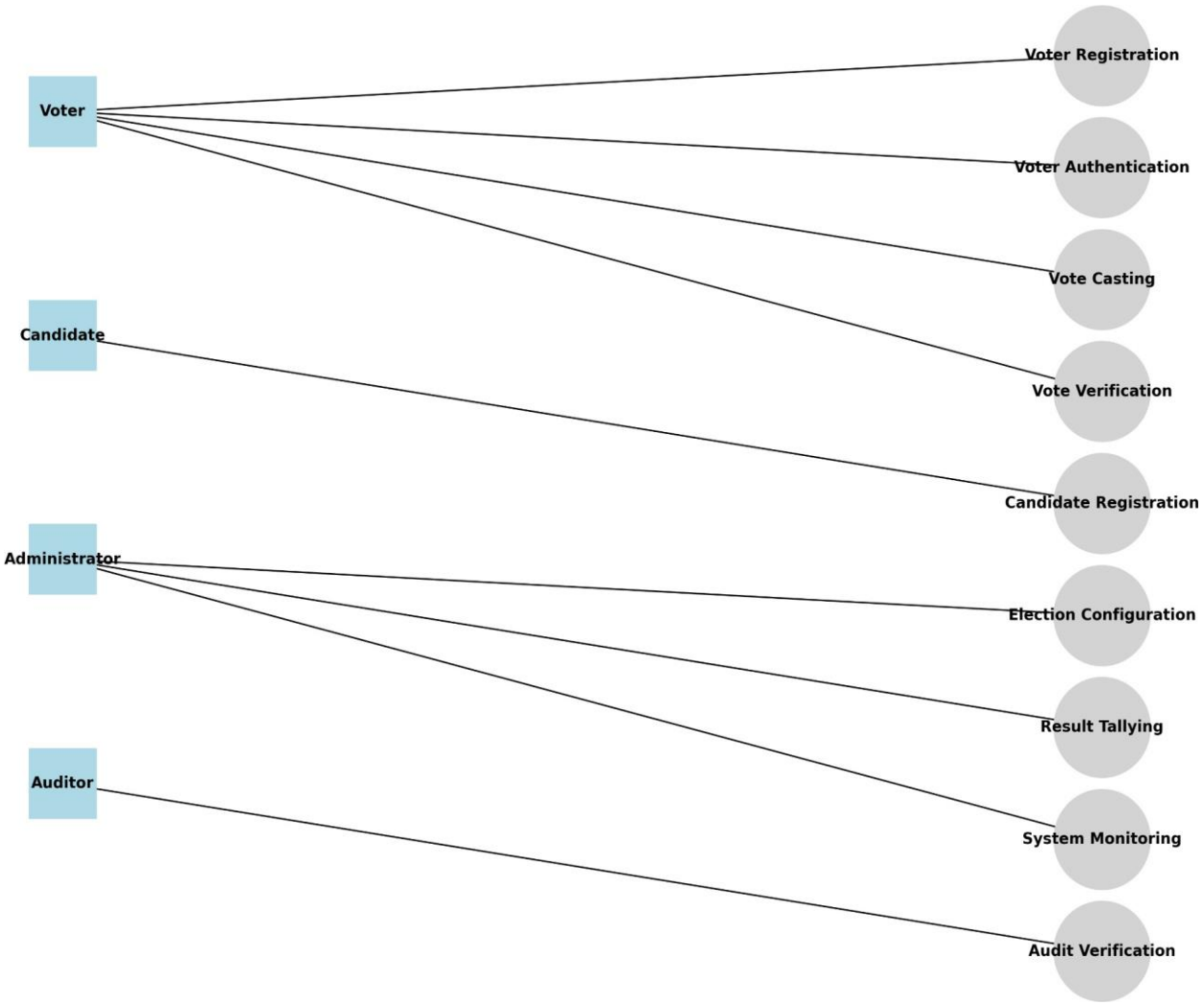
- **System Implementation:**

- Voter registration module: Smart contract deployment for digital identity issuance.

- Authentication module: ML model training with biometric data.
- Voting module: Encryption and blockchain transaction processing

- **Evaluation Metrics:**

- Security: Resistance to tampering and fraud.
- Accuracy: ML authentication success rate.
- Scalability: Transaction throughput and latency.
- Usability: User experience feedback.



[Use case diagram]

Case Studies and Real-World Implementations:

Various countries and organizations have begun experimenting with or adopting blockchain-based e-voting systems to enhance security and transparency:

- Estonia: A global leader in digital governance, Estonia has been utilizing e-voting since 2005. The country is now exploring blockchain technology to further strengthen the security and trustworthiness of its electoral system.

- Sierra Leone: In 2018, Sierra Leone conducted a pioneering trial of blockchain-based voting during its presidential election, in collaboration with Swiss blockchain firm Agora. While the trial had a limited scope, it showcased blockchain's potential for secure and verifiable elections.

- West Virginia, USA: During the 2018 midterm elections, West Virginia introduced a blockchain-based mobile voting application for military personnel stationed overseas. The pilot demonstrated the feasibility of remote blockchain voting but also raised concerns regarding mobile device security.

5. Results and Discussion

- **Security Enhancements**

The integration of blockchain technology creates a tamper-proof record of votes that enhances trust in electoral outcomes.[8][10] Machine learning algorithms successfully identify anomalies in real-time, preventing fraudulent activities during elections[9].

- **Transparency Improvements**

Blockchain's decentralized nature ensures transparency by allowing stakeholders to independently verify election results without compromising voter privacy[10].

- **Scalability Analysis**

The proposed system demonstrates scalability by efficiently handling large-scale elections through optimized blockchain implementations and machine learning models trained on extensive datasets[10].

- **Security Analysis:**

  - Blockchain ensured no vote tampering; cryptography protected voter privacy.
  - ML detected simulated fraud attempts with high precision.

Challenges:

Implementing technology like e-voting and instant results in election systems comes with several

challenges. One major concern is ensuring the “Security and Integrity” of the electoral process. This includes protecting against cyber threats, preventing hacking and maintaining the secrecy of the vote.

Another challenge is “Building Trust” among voters, particularly in countries with a history of electoral disputes or manipulation. Voters need to have confidence in the technology and the process to ensure widespread acceptance of the results.

“Technical Challenges” also arise, such as ensuring the compatibility of different voting systems, addressing power outages or connectivity issues, and implementing reliable auditing mechanisms.

Additionally, there are “Scalability and Cost” considerations. Implementing new technology requires significant investment, which can be a barrier for smaller countries or jurisdictions.

“Voter Education and Accessibility” are also crucial factors. Voters need to understand how to use the new technology, and it must be accessible to all, including those with disabilities or limited technical proficiency.

”Regulatory Frameworks” need to be adapted to accommodate new technologies, ensuring compliance with existing electoral laws and regulations.

Examples of successful implementations, such as Estonia’s internet voting system, demonstrate that with careful planning, execution and ongoing evaluation, technology can enhance the electoral process.

6. Conclusion and Future Work

- **Conclusion:**

The proposed e-voting system significantly enhances security, transparency, and trust in the electoral process by integrating blockchain, machine learning, and cryptographic techniques. Blockchain ensures tamper-proof vote storage, preventing unauthorized modifications and ensuring election integrity. Machine learning strengthens security by detecting potential threats and anomalies in real time, while cryptographic methods safeguard voter privacy and data confidentiality.

A key innovation in this system is the use of blockchain-based digital identity for voter registration. This approach eliminates identity fraud, ensures only legitimate voters participate, and provides a verifiable and immutable record of registered voters. By leveraging decentralized and transparent technology, the system fosters public confidence, making digital elections more secure, accessible, and trustworthy.

- **Future Work**:

To further enhance the efficiency, security, and practicality of the proposed e-voting system, several areas of improvement and expansion will be explored:

- **Optimizing Machine Learning Models for Faster Processing:** Refining ML-based anomaly detection algorithms to improve speed and accuracy, ensuring real-time threat detection without compromising system performance.

- **Exploring Quantum-Resistant Cryptography:** Investigating advanced cryptographic techniques that can withstand potential threats posed by quantum computing, ensuring long-term security and data integrity.

- **Testing the System in Real-World Election Scenarios:** Conducting pilot programs and simulations in controlled election environments to validate system performance, user experience, and overall reliability.

- **Addressing Regulatory Challenges through Collaboration with Policymakers:** Engaging with government agencies, election commissions, and legal experts to ensure compliance with election laws and facilitate seamless integration into existing voting frameworks.

These future enhancements will contribute to making blockchain-based e-voting systems more robust, scalable, and widely accepted for secure and transparent digital elections.

References

1. Avinash Ingole, et al. (2024). "Towards Secure and Transparent Elections: A Review of Electronic Voting Integrated with Blockchain Technology". Ijraset Journal For Research in Applied Science and Engineering Technology
2. https://www.a3logics.com/blog/blockchain-based-electronic-voting-system-development/
3. Hajian Berenjestanaki, M., Barzegar, H. R., El Ioini, N., & Pahl, C. (2024). Blockchain-Based E-Voting Systems: A Technology Review. Electronics, 13(1), 17.
4. https://doi.org/10.3390/electronics13010017
5. P. Sirenjeevi, C. Preethi, S. Shaminee, J. Gayathri, 2022, Smart Voting System using Deep Learning Techniques and Facial Authentication, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) ICONNECT – 2022 (Volume 10 –
6. Issue 09)
7. Aidynov, T., Goranin, N., Satybaldina, D., & Nurusheva, A. (2024). A Systematic Literature Review of Current Trends in Electronic Voting System Protection Using Modern Cryptography. Applied Sciences, 14(7), 2742. https://doi.org/10.3390/app14072742
8. charles oguk. (2021). A Review of Cryptographic Primitives for Security of Electronic Voting Systems.
9. Shahzad & Crowcroft (2019). Trustworthy Electronic Voting System Using Blockchain Technology.
10. LinkedIn Article: Blockchain - E-Voting Revolutionizing Electoral Integrity[2024].
11. EAI Endorsed Transactions IoT: Blockchain-Based Cryptographic Algorithm for Data Protection[2025].
12. Silva H. K. M. D, De Silva M.W.M.R, Withanage P.A, Hettiarachchi R.T, "Smart Election:

Blockchain Based Machine Learning Solution for e-Voting Electoral System" Published in International Research Journal of Innovations in Engineering and Technology
13. Kavitha S, Praveen R, Ragavendrar MA, and Vishwa. (2023). Online E-Voting System Using Blockchain Technology. Data Analytics and Artificial Intelligence, 3(1), 79-83.
14. B. Sujatha, Y. Ganesh, N. Leelavathy et al. (2024). "Blockchain-Powered E-Voting: A Novel Approach to Secure Voter Authentication, Online Voting and Election Automation."
15. Sumit S. Shevtekar, Varad Kalambarkar (2023). "Blockchain Based E-Voting and Electoral Fraud Detection."
16. S. K. Mishra et al., "Scalable and Sustainable Blockchain-based Voting Framework for Indian Elections," Springer, 2023.
17. R. Sharma et al., "Blockchain Technology for Secure E-Voting System: A Review," International Journal of Computer Applications, 2023.