A Literature Review on Anti-Scam Voting Machine with Aadhar and Biometric Verification with Blockchain Integration

Abhishek Manas V[1], Harigovind PK[2], Jishnu Jithesh[3], Sidharth APV[4], Aswathi V[5]
[1,2,3,4]*Department of Computer science and Cyber Security Vimal Jyothi Engineering College, Chemperi, Kannur*
[5]*Assistant Professor, Department of Computer science and Cyber Security, Vimal Jyothi Engineering College Chemperi, Kannur*

***Abstract*—Electronic voting systems are being adopted more frequently to modernize elections. However, most current solutions depend on centralized authorities for vote counting. This raises concerns about security, transparency, and voter privacy. This work presents a blockchain-assisted e-voting framework that combines biometric verification with Aadhaar authentication. This ensures voter legitimacy and prevents problems like double voting.**

The proposed system uses decentralized ledger technology to guarantee data immutability, anonymity, and public verifiability. It also employs secret-sharing techniques to allow ballot counting without relying on a third party. To improve efficiency, a cloud-assisted module is included to handle resource-heavy tasks, ensuring scalability for large elections.

Security analysis shows the system's resistance to common attacks. Experimental evaluation confirms that it meets key requirements for correctness, privacy, unforgeability, and verifiability. By mixing biometrics, national ID verification, and blockchain, this solution provides a secure, transparent, and efficient method for next- generation digital voting.

I. INTRODUCTION

Electronic voting systems mark a significant change in democratic processes. They aim to address the limitations of traditional voting while introducing new security and privacy issues. These systems vary from direct recording machines to internet-based platforms, each using authentication and encryption methods to maintain electoral integrity.

Biometric authentication, including fingerprint, facial, and iris recognition, plays a key role in verifying voters. Techniques like SIFT-based fingerprint matching enhance accuracy and help prevent impersonation. However, challenges persist, such as false rejections, difficulties for elderly or injured voters, and concerns about the storage of sensitive data.

Security in e-voting relies heavily on encryption and cryptographic protocols. Methods like AES-GCM, homomorphic encryption, zero-knowledge proofs, and blind signatures protect confidentiality and verifiability. Still, real-world applications face vulnerabilities due to software manipulation, insider threats, and attacks on infrastructure. Blockchain-based e-voting offers transparency and immutability but also presents issues with scalability, high transaction costs, and complexity, without resolving fundamental internet vulnerabilities.

Privacy is a fragile balance between anonymity and the ability to audit. Techniques like differential privacy, revocable anonymity, and cryptographic mixing seek to safeguard voter identities, yet achieving complete privacy alongside full verifiability is still a challenge. Internet voting provides accessibility for voters over- seas and those with disabilities, but it encounters risks from coercion, malware, and insecure devices, making widespread acceptance controversial.

Cloud integration enhances scalability and reliability. However, centralizing sensitive electoral data raises concerns about sovereignty and dependence on vendors. Authentication methods are continually evolving. Multi-factor systems, cryptographic tokens, and emerging frameworks like self-sovereign identitymopen new possibilities while trying to balance usability and security.

The main challenges for e-voting include achieving universal verifiability, resisting coercion, ensuring accessibility, and building public trust. Hybrid models that combine the transparency of paper-based voting with the efficiency of digital methods, backed by ongoing audits and secure cryptographic protocols, are likely to shape the future of electronic voting systems.

II. OVERVIEW OF PROPOSED SYSTEM

Modern electronic voting systems are changing quickly as they use new cryptography, blockchain technology, and cloud-based systems. These tools aim to fix the problems of traditional paper-based voting by improving security, privacy, and accessibility. Homomorphic encryption allows votes to be counted without showing individual choices. Techniques like zero-knowledge proofs, blind signatures, and zk-SNARKs protect voter anonymity and ensure votes can be verified without losing secrecy. Together, these cryptographic methods form the foundation of secure e- voting systems.

Blockchain technology improves e-voting by providing decentralized, unchangeable, and transparent record-keeping. Smart contracts help automate processes like checking voter eligibility and counting votes, which helps maintain consistency and reduce human mistakes. However, blockchain systems face challenges such as limits on scalability, high costs, and concerns about keeping voter privacy on public ledgers. Consensus methods like Proof-of-Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT) secure these systems, but using them in real-world scenarios requires careful coordination of efficiency and trust. Real-life examples, such as Estonia's internet voting system, show both the potential and risks of digital elections. This system uses national ID infrastructure for secure access, but issues like vulnerabilities in ballot processing and the need for better auditing tools still need attention.

Cloud computing has also become important for modern e-voting by offering scalability, automatic backups, and better system reliability. Private and hybrid cloud setups allow electoral bodies to securely handle voter records, checks, and large-scale remote voting. However, this method also brings new risks related to data ownership, reliance on vendors, and the gathering of sensitive electoral data in centralized systems. As a result, how well this system is adopted depends not only on technical protections but also on political trust, laws, and how ready societies are to accept digital governance.

Usability and accessibility for voters are also critical for successful adoption. Biometric authentication, multi-factor methods, and gesture-based verification help include diverse groups, including the elderly and disabled. Still, public trust remains a key issue.

Research shows that how willing citizens are to use e-voting largely depends on their views about transparency, fairness, and familiarity with digital systems. Blockchain-based platforms, while innovative, often find it hard to gain acceptance without strong auditing practices and clear communication with voters.

New ideas like continuous or repetitive voting push the limits of democratic participation, allowing citizens to change their preferences over time. This reflects changing political views instead of fixed-term choices. Although still in testing, these approaches could improve responsiveness and representation in government. However, key challenges remain: protecting voter anonymity while allowing verification, pre- venting coercion, reducing insider threats, and building public trust in digital systems. Finding this balance will require methods that combine paper audits with advanced digital techniques, ongoing security checks, and gradual, open deployment.

III. FUTURE RECOMMENDATIONS

Future electronic voting systems must adopt stronger security protocols to ensure confidentiality, integrity, and resilience against evolving threats. New cryptographic methods like homomorphic encryption and differential privacy can enable secure vote tallying while protecting voter identities and preventing data leaks. Adding multi-factor biometric authentication, which combines physiological traits like fingerprints, iris, or facial recognition with behavioral or gesture-based verification, will further reduce fraud and unauthorized access. These improvements together will enhance the trustworthiness of digital electoral platforms. The use of blockchain technology should be expanded to increase transparency, auditability, and trust in electronic voting. Blockchain's decentralized and unchanging structure allows for tamper-proof vote recording. Smart contracts can

automate the tallying process, verification, and checks on voter eligibility. However, scalability issues, transaction costs, and voter privacy concerns need to be ad- dressed through better consensus methods and privacy- protecting blockchain protocols. A well-designed blockchain framework can offer both transparency and efficiency while protecting user privacy.

Strong voter authentication is another important area for improvement. Future systems should use privacy-protecting identity verification frameworks that connect national identity systems like Aadhaar with bio- metric or gesture-enhanced methods. These combined approaches can reduce impersonation, prevent multiple voting attempts, and ensure that only eligible voters take part, all while protecting personal data. Balancing security and voter privacy will be crucial for gaining public acceptance.

Accessibility and usability must also be key considerations in future e-voting platforms. Systems should be built to serve a wide range of voters, including the elderly, disabled, and people with limited digital skills. Simple user interfaces, multiple authentication options, and secure methods for repetitive voting can improve inclusivity while keeping strong security measures in place. By focusing on accessibility, electronic voting can strengthen democratic participation and uphold the principle of equal representation.

The resilience of e-voting systems requires on- going assessment and management of vulnerabilities throughout their lifecycle. Experiences like Estonia's internet voting system emphasize the need for thorough security audits, penetration testing, and effective audit tools to identify and fix potential weaknesses. Incorporating continuous monitoring and real-time response systems will ensure that future systems stay strong against insider threats and external attacks.

Finally, emphasizing decentralization and system reilience is essential to avoid single points of failure and ensure availability during important election periods. Distributing system components across secure, fault- tolerant architectures will reduce the risk of downtime and targeted attacks. A decentralized, resilient design will ensure that elections can be conducted securely and reliably, even in challenging conditions.

IV. LITERATURE SURVEY

Ramesh and Muralibhaskaran [1] proposed a novel internet voting scheme leveraging cloud computing technology to address the limitations of traditional paper-based voting systems. Their approach combines internet and cryptographic techniques to enable voters to cast votes securely through cloud services. The system utilizes private or community cloud infrastructure with various services including validation, key generation, key exchange, mapping, checking, and tallying services. The authors implemented a comprehensive I-voting algorithm with 11 steps covering registration, authentication, voting, and tallying phases. The study demonstrates how cloud computing can provide reliable servers, greater memory capacity, and faster processing to handle millions of votes efficiently. The proposed model integrates biometric authentication using UID cards and employs RSA algorithms for se- cure communication between voters and data centers, ultimately reducing time consumption and expenditure while speeding up the voting process.

Mahmood et al. [2] introduced an intelligent gesture-enhanced blockchain voting system that ad- dresses security, transparency, and accessibility challenges in electronic voting, particularly for disabled, elderly, and visually impaired voters. The system operates in two phases: user identification using pre- trained datasets based on cvzone and Dlib tools for face and finger identification, and a voting process utilizing blockchain technology. The authors employed gesture recognition from face and hand movements as authentication mechanisms, enabling non-touch inter-action that reduces physical exertion for users with disabilities. Real-time simulations demonstrated user interaction times ranging from 24.3 to 29.7 seconds across different age groups, with gesture recognition accuracy between 88.7% and 92.5%. The blockchain-based voting process achieved 100% precision and 99% recall, while the system showed high accuracy in gesture recognition and robust security using Equal Error Rate quality measures, significantly enhancing inclusiveness and user-friendliness compared to traditional systems.

Alown et al. [3] conducted a comprehensive survey examining Direct Recording Electronic (DRE) voting, internet voting, and blockchain-based electronic voting systems to enhance democratic processes. The

authors systematically analyzed various e-voting schemes and technologies, evaluating their security features, verifiability mechanisms, and potential vulnerabilities through extensive literature review and comparison. Their research provides deep understanding of cryptographic primitives employed in e-voting systems, including homomorphic encryption, blind signatures, and zero-knowledge proofs, and how these address specific challenges in each voting scheme. The study examines applications proposed by previous research, assessing their strengths, limitations, and impact on democratic procedures. The authors conclude that while significant progress has been made in developing secure e-voting systems, challenges remain in ensuring voter privacy, preventing coercion, maintaining scalability, and building public trust, emphasizing the need for continued research and development in this critical area.

Jeong and Jeong [4] investigated the security implications of smaller fingerprint sensors on fingerprint authentication systems, with particular relevance to electronic voting applications. The authors conducted extensive experiments using partial fingerprint images ranging from 8% to 48% of complete fingerprint images, corresponding to sensor sizes used in various devices including smartphones, USBs, and cards. Their research demonstrates that smaller partial im- age sizes significantly increase the Impostor Matching Rate (IMR), with IMR increasing from 0.3106 to 0.9836 at 0.01% False Matching Rate when partial size decreased from 44% to 8%. The study reveals that smaller sensors create vulnerabilities to ”Master- print” attacks, where specially crafted fingerprints can successfully match multiple users in the database. The authors prove that when partial fingerprint size is 15% of a whole image, Masterprints can be effectively produced, posing significant security risks for biometric voting systems that rely on small fingerprint sensors.

Vladucu et al. [5] presented a comprehensive survey of blockchain-based electronic voting systems, analyzing over 60 proposals from academia, government implementations, and commercial solutions. The authors provide extensive up-to-date coverage of blockchain e-voting systems,

TABLE I COMPARISON TABLE

Ref	Paper Title	Advantages	Disadvantages
[1]	Internet Voting Using Cloud Computing	• Uses cloud for scalability and cost reduction • Incorporates multi-phase cryptographic verification	• Dependence on central cloud creates failure risks • Limited privacy discussion
[2]	Gesture-Enhanced Blockchain Voting	• Innovative accessibility via gesture recognition • Combines blockchain with biometric security	• Gesture recognition accuracy issues • High computational overhead
[3]	Survey of DRE, Internet	• Broad literature review of e-voting schemes • Analyzes cryptographic primitives	• Lacks practical experimentations • Limited recent blockchain coverage
[4]	Fingerprint Sensor Security	• Reveals security risks of small sensors • Demonstrates masterprint vulnerabilities	• Focuses only on fingerprint biometrics • No countermeasure proposals
[5]	Blockchain E-voting Survey	• Categorizes >60 blockchain systems comprehensively • Discusses cryptography and system properties	• Mostly survey, limited innovations • Scalability and usability issues unresolved
[6]	Cloud-based Indian Voting	• Modernizes Indian election infrastructure • Addresses low voter turnout	• No actual deployment or security tests • Security concerns are lightly addressed
[7]	BP-Vot Blockchain	• Uses differential privacy for anonymity • Reduces latency significantly	• Complex multi-tech integration • Evaluation limited to small-scale tests
[8]	Always-on Voting (AoV)	• Prevents peak-end manipulation • Supports continuous, iterative voting	• Complexity in randomness and security • Implementation complexity unclear
[9]	Aadhar-based Online Polling	• Uses biometric Aadhar for secure auth • Facilitates remote, convenient voting	• Centralized data dependency • Privacy/security practices not fully de-tailed
[10]	GIBI with Homomorphic En-cryption	• Ensures voter anonymity via group ID • Offers secure vote verification	• Cryptographic complexity • Scalability in large elections uncertain
[11]	Estonian I-Voting Vulnerabili- ties	• Identifies ballot manipulation risks • Proposes audit method for detection	• Focused on specific case study • Not a general solution
[12]	E-voting System Attacks Survey	• Exhaustive attack categorization • Analysis of cryptographic primitives	• No experimental validation • Lacks practical deployment details

[13]	Digital Voting Acceptance Model	• Validates acceptance through SEM • Uses UTAUT theory for framework	• Conceptual, no real system tested • Thailand-specific context limits generalizability
[14]	Multi-alt Election Outcome Pre- diction	• Introduces influence gap predictor • Validates on real social networks	• Focuses on prediction, not security • No direct application for voting systems
[15]	Decentralization in E-voting	• Systematic historical overview • Classifies centralized vs decentralized	• Pure review, no experimental setup • Challenges in real-world scaling remain

introducing terminology and categorizing solutions based on consensus algorithms, cryptographic frameworks, and the challenges they address. Their research examines various blockchain platforms including Bitcoin, Ethereum, Hyperledger Fabric, and Quorum, analyzing their suitability for voting applications based on throughput, scalability, and security features. The study identifies key cryptographic techniques used in blockchain voting including homomorphic encryption, zero-knowledge proofs, and digital signatures, while discussing fundamental system properties such as accuracy, anonymity, auditability, and verifiability. The authors conclude that while blockchain technology offers promising solutions for enhancing voting transparency and security, significant challenges remain regarding scalability, user experience, and legal compliance, requiring further research and development before widespread adoption.

Matharu et al. [6] proposed a Cloud-based Inte- grated Election Voting System (CIEVS) framework to modernize the Indian election voting system and address low voter turnout percentages. The authors identified that Indian election voting percentages have remained between 55% and 65%, necessitating technological intervention to boost participation. Their conceptual model leverages cloud computing, web services, and mobile phone services to integrate existing Electronic Voting Machine (EVM) systems with internet voting capabilities. The CIEVS framework comprises five main components: Database Storage Subsystem implemented as private cloud with Plat- form as a Service (PaaS), I-Voting Subsystem with verification and authentication modules, polling booths with both EVM and I-voting nodes, ECI personnel for system management, and interface devices including personal computers and mobile phones. The proposed model offers advantages including efficient data management, scalability, cost reduction, enhanced security through private cloud deployment, database backup capabilities, higher voting percentages, mobility for voters, time savings, localization support, and reinforcement of democratic processes.

Baniata and Caluna [7] developed BP-Vot, a blockchain-based privacy-preserving e-voting framework that integrates smart contracts, differential privacy, and self-sovereign identities to address security, privacy, and performance challenges in electronic voting systems. The authors implemented a novel (k)-differential privacy mechanism where votes are randomly transferred from a pivoted candidate to other candidates, with final election results statistically approximated while maintaining voter anonymity. The system utilizes Self-Sovereign Identity (SSI) mechanisms following web3.0 standards for reliable vote casting using digital identities, eliminating dependence on central authorities. Experimental evaluation on cloud-based permissioned blockchain networks using Hyperledger Besu with nodes in Google's EU and USA data centers demonstrated 24% improvement in latency over state-of-the-art solutions (1 s/TX com- pared to 1.24 s/TX). The system achieved no less than 98% accuracy in vote approximation across all experiments with linearly increasing accuracy as a function of total cast votes, while formal evaluation proved the differential privacy method's robustness against reconstruction attacks.

Venugopalan et al. [8] introduced Always-on- Voting (AoV), a framework for repetitive voting on blockchain that addresses limitations in traditional governance systems where participants cannot change votes between consecutive elections and are susceptible to peak-end effect manipulation. The authors identified two critical shortcomings: inability to change votes during long intervals between elections and manipulation through peak-end effects where judgment is based on feelings shortly before elections. AoV operates in repetitive epochs with randomized and unpredictable endpoints to thwart peak-end effects, utilizing synergy between Bitcoin

puzzle oracles, verifiable delay functions, and smart contracts. The framework supports 1-out-of-k candidate voting where only supermajority votes can change previous winning choices at epoch end. The authors analyzed Bitcoin Proof-of-Work puzzle solution randomness and AoV entropy requirements, demonstrating how public randomness determines voting interval endings through commitments to future events. The system provides continuous voting capability while maintaining security against manipulation through randomized tally timing that prevents interested parties from conducting timely peak-end effect manipulations.

Sai Pratap Varma et al. [9] developed an Aadhar card verification-based online polling system to ad- dress security challenges and fraudulent voting issues in traditional election systems. The authors identified that traditional voting procedures often become inconvenient due to voter reluctance to visit polling stations and the involvement of enormous social and human resources. Their system leverages distributed computing and Aadhar card authentication to provide enhanced security and accessibility for the voting process. The proposed model utilizes web technology to make the voting system reasonable and cost-effective, implementing server services connected to databases for persistent data storage. The authentication process relies on Aadhar database as the backbone to verify voter eligibility through unique fingerprint identification, enabling voters to make choices online while updating server databases. The system incorporates a two-step verification process during registration and authentication phases, utilizing One-Time Password (OTP) codes sent to registered mobile phones. Field officials manage voter data and voting records, with administrators maintaining comprehensive information about voters and their voting preferences through Aadhar card verification.

Vangujar et al. [10] presented a novel e-voting scheme combining Group Identity-based Identification (GIBI) with Homomorphic Encryption based on discrete logarithmic assumptions to address security and privacy challenges in electronic voting systems. The authors developed a modified Schnorr-like GIBI scheme that enables voter identification and authorization through zero-knowledge proofs while ensuring anonymity and eligibility verification. The system grants voters authorization to cast valid votes for single candidates using distributed ElGamal encryption for fairness, with partial shares for decryption enabling individual and universal verifiability without central authority dependence. The GIBI scheme prevents rev- elation of specific voter identities by any authority, maintaining vote verification through group public keys while keeping individual voter identities secret. Experimental evaluation demonstrates the scheme's security under various scenarios in the random oracle model, with performance advantages over existing digital signature-based e-voting schemes. The proposed approach generates tokens for voters who cast valid ballots, supporting vote uniqueness and unreusability while allowing voters to verify ballot submissions and final tallies with encrypted ballots and vote counts remaining secure throughout the process.

Treier and Du¨u¨na [11] conducted a systematic ex-amination of the Estonian internet voting system to identify and solve vulnerabilities in ballot integrity during the vote processing stage. The authors reviewed i-voting source code, analyzed operational systems in laboratory environments, studied documentation, and examined audit reports from previous elections to assess security against insider attacks and i-ballot-box integrity. Their systematic investigation revealed vulnerabilities that could allow dishonest insiders to re-place all ballots undetected during the processing stage between voting period conclusion and vote counting. The research proposed an audit application to verify ballot integrity during processing, with formulas rigorously tested across multiple scenarios including ballot replacement, addition, and removal. The methodology proved capable of detecting comprehensive manipulation ranges while maintaining end-to-end verifiability and addressing over-the-shoulder coercion-resistance limitations. Following responsible disclosure to Estonian State Electoral Service representatives, the authors submitted a Python script for additional i-voting process auditing, which was subsequently incorporated into the European Parliament election source code published on May 30, 2024, enhancing the auditing application based on their contributions.

Barelli et al. [12] conducted a comprehensive survey examining e-voting systems and attacks to understand the current landscape and readiness for real-world

implementations. The authors analyzed fundamental and secondary properties of e-voting systems, categorizing them based on security requirements including integrity, anonymity, eligibility, accuracy, verifiability, receipt-freeness, coercion resistance, and software independence. Their research distinguished between on-site, remote, and blockchain-based systems, focusing on property coverage and system strengths and weaknesses. The survey presents the first literature review of known attacks against e-voting systems, discussing attack methodologies, effectiveness, and limitations across different system categories. The authors examined cryptographic primitives relevant to e-voting including mix networks, homomorphic encryption, group signatures, and blind signatures, while analyzing their applications in various voting contexts. Through comprehensive analysis of current proposals and documented attacks, the authors concluded that electronic voting paradigms require additional research before being considered secure for general election settings, highlighting ongoing challenges in balancing security, privacy, accessibility, and practical deployment considerations.

Dabpimjub and Kiattisin [13] investigated success factors for conceptual digital voting models using blockchain technology through Structural Equation Modeling (SEM) analysis of 400 voter responses in Thailand. The authors developed a comprehensive framework based on Unified Theory of Acceptance and Use of Technology (UTAUT), trust theory, and factors transfer context to analyze voter acceptance of blockchain-based electoral systems. Their research identified nine critical factors affecting digital voting platform implementation: performance expectancy, effort expectancy, social influence, facilitating conditions, trust in internet infrastructure, trust in government institutions, e-governance management, political factors, and cultural influences. The study utilized SEM methodology with Mplus Version 7 to examine relationships between technology acceptance and credibility factors from voter perspectives. The authors developed a functional digital voting platform using blockchain technology and demonstrated how success factors can be applied to improve electoral systems. Their conceptual model provides framework for enhancing acceptance and trust in blockchain-based elections, offering practical insights for implementing digital voting technologies while addressing technological, social, and institutional challenges in democratic processes.

Liu et al. [14] proposed a minimal influence gap (MIG) metric for predicting voting outcomes in multi-alternative elections within social networks where opinion dynamics complicate traditional prediction methods. The authors extended the binary influence gap concept to multi-alternative scenarios, evaluating MIG as predictor across three voting behavior models: Maximizing Expected Utility model for rational voter optimization, Local Dominance model for subjective voter beliefs, and K-Pragmatist model for heuristic voter actions. Their research tested MIG effectiveness on synthetic networks with scale-free features and community structures, along with real-world Face-book social network data. Experimental results demonstrated strong correlation between MIG and voting outcomes across all three models, with particularly strong performance in Local Dominance model when voters persist in supporting favorite alternatives. In Facebook network analysis, alternatives with highest MIG values became winners in over 90% of elections, with predictive power strengthened in social net- works exhibiting homophily characteristics. The study provides neat and effective solution for predicting multi-alternative election outcomes while sidestepping complex opinion dynamics analysis, offering valuable insights for understanding collective decision-making processes in networked environments.

Almeida et al. [15] conducted a systematic literature survey examining the evolution of electronic voting systems from early cryptography-based proposals to modern blockchain-based solutions, analyzing the impact of decentralization on e-voting research. The authors reviewed 75 publications spanning from the introduction of commercial cryptography in the 1970s to contemporary smart-contract-enabled blockchain protocols, providing comprehensive chronological analysis of technological development. Their research systematized classification criteria used by various authors to characterize e-voting solutions, establishing standardized framework for evaluating both centralized and decentralized approaches. The survey identified critical cryptographic tools including threshold systems, mix-nets, blind signatures, and zero-knowledge proofs, analyzing their applications across different system architectures. The authors demonstrated how blockchain technology's

introduction in 2009 funda- mentally shifted e-voting research paradigms, enabling new levels of transparency, data immutability, and pseudo-anonymity that enhanced system security and verifiability. The systematic literature review revealed that while significant progress has been achieved in both centralized and decentralized e-voting systems, challenges remain in achieving secure, transparent, and scalable solutions suitable for widespread real-world deployment, particularly regarding voter mobility and universal accessibility requirements.

REFERENCE

[1] Ramesh and Muralibhaskaran, "Internet Voting Using Cloud Computing," in *Chennai and Dr.MGR University Second International Conference on Sustainable Energy and Intelligent System (SEISCON 2011)*, 2011.
[2] Mahmood et al., "Intelligent Gesture Enhanced Blockchain Voting: A New Era of Secure and Accessible E-Voting," *IEEE Access*, 2024.
[3] Alown et al., "Enhancing Democratic Processes: A Survey of DRE, Internet and Blockchain in Electronic Voting Systems," *IEEE Access*, 2025.
[4] Jeong and Jeong, "Effect of Smaller Fingerprint Sensors on the Security of Fingerprint Authentication," 2023.
[5] Vladucu et al., "E-Voting Meets Blockchain: A Survey," *IEEE Access*, 2023.
[6] Matharu et al., "CIEVS: A Cloud-based Framework to Modernize the Indian Election Process."
[7] Baniata and Caluna, "BP-Vot: Blockchain-Based e-Voting Using Smart Contracts, Differential Privacy and Self-Sovereign Identity," 2025.
[8] Venugopalan et al., "Always-On Voting: A Framework for Repetitive Voting on Blockchain."
[9] Sai Pratap Varma et al., "Aadhar Card Verification Based Online Polling."
[10] Vangujar et al., "A Novel Approach to E-Voting with Group Identity-Based Identification and Homomorphic Encryption," *IEEE Access*, 2024.
[11] Treier and Du¨u¨na, "Identifying and Solving a Vulnerability in the Estonian Internet Voting Process: Subverting Ballot Secrecy," 2024.
[12] Barelli et al., "Toward Secure Electronic Voting: A Survey on E-Voting Systems and Attacks," 2025.
[13] Dabpimjub and Kiattisin, "Success Factors for Conceptual Digital Voting Model," *Journal of Mobile Multimedia*, vol. 20, no. 4, 2024, DOI: 10.13052/jmm1550-4646.2042.
[14] Liu et al., "Predicting Voting Outcomes for Multi-Alternative Elections in Social Networks," *IEEE Access*, 2024.
[15] Almeida et al., "Impact of Decentralization on Electronic Voting Systems: A Systematic Literature Survey," *IEEE Access*, 2023.