www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 2999-3004

e-ISSN : 2583-1062
Impact Factor : 7.001

SECURE ELECTRONIC VOTING SYSTEM WITH FINGERPRINT AUTHENTICATION AND SMS CONFIRMATION

Mr. Mugesh J[1], Dr. Azha Periasamy[2], Mrs. Dhivya Kannu[3], Mr. Selvaraj T[4], Mr. Thamizharasan B[5]

[1,4,5]Student, Department Of Electronics And Instrumentation, Bharathiar University, Coimbatore-641046, Tamil Nadu, India.

[2]Associate Professor, Department of Electronics and Instrumentation, Bharathiar University, Coimbatore, Tamilnadu, India.

[3]Assistant Professor , Department of Mathematics, Nehru Memorial College, Tiruchirappalli, Tamilnadu, India

DOI: https://www.doi.org/10.58257/IJPREMS40691

ABSTRACT

This paper presents a Secure Electronic Voting System that combines fingerprint-based biometric authentication with SMS-based one-time password (OTP) confirmation to ensure robust voter identity verification and ballot integrity. During registration, each voter's fingerprint template is hashed using SHA-256 and stored alongside their mobile number in a SQLite database. At election time, fingerprint matching is performed locally; upon successful biometric validation, a six-digit OTP is generated and delivered via the Twilio SMS API. Only after the OTP is correctly entered within a five-minute window may the voter cast their ballot. Each vote is encrypted with AES-256 in CBC mode before being recorded, and a "has Voted" flag prevents duplicate submissions. An administrative dashboard built with Flask and Chart.js provides real-time visualizations of voter turnout, encrypted vote logs, and system health metrics without exposing sensitive data. Performance evaluation demonstrates sub-second registration and authentication, 1–2 Ms encryption overhead, and reliable SMS delivery within 1–2 seconds. Security analysis confirms resistance to replay attacks, impersonation, and tampering. Future enhancements will integrate block chain for an immutable audit trail and AI-driven anomaly detection to flag suspicious voting patterns. This modular, open-source prototype lays the groundwork for scalable, transparent, and legally compliant electronic elections.

Keywords: Electronic voting, biometric authentication, OTP verification, AES encryption, real-time monitoring, secure backend.

1. INTRODUCTION

Modern elections face persistent challenges: long queues at polling stations, opportunities for voter impersonation, the risk of ballot tampering, and delays in result tabulation. In many regions, logistical constraints such as limited staffing, remote polling locations, and paper-based processes deter participation and raise concerns about the integrity of outcomes. Meanwhile, rising cybersecurity threats target centralized electronic voting platforms, exploiting weak authentication to cast fraudulent ballots or disrupt service. Restoring public trust demands a voting infrastructure that is both secure and user-friendly under real-world conditions.

This project delivers a Secure Electronic Voting System that directly addresses these challenges. By combining fingerprint biometric authentication with SMS-based one-time password (OTP) confirmation, it ensures that only legitimate voters each uniquely identified by a scanned fingerprint can cast a ballot. The additional OTP step, delivered instantaneously via Twilio's global SMS network, provides a dynamic second factor that blocks unauthorized access even if a fingerprint hash is compromised. Votes are encrypted end-to-end using AES-256 before storage in a tamper-resistant SQLite database. An intuitive, Flask-powered dashboard gives election officials real-time visibility into voter turnout percentages, system health, and encrypted vote logs enabling rapid response to anomalies without exposing individual choices.

In practice, this approach reduces queue times by enabling remote pre-authentication (voters scan their fingerprint and verify via OTP in advance), eliminates paper handling errors, and prevents double-voting through a "has Voted" flag tied to each biometric record. SMS confirmations give voters immediate assurance their ballot was recorded, reinforcing transparency and trust. Looking ahead, planned enhancements include integrating a permissioned block chain ledger to produce an immutable audit trail, and deploying AI-driven anomaly detection to flag suspicious patterns such as mass OTP requests from a single phone or rapid consecutive voting attempts. Further, mobile-friendly interfaces and support for additional biometric modalities (e.g., facial recognition) will expand accessibility. Together, these innovations promise a scalable, resilient election system that meets the security, usability, and transparency needs of 21st-century democracies directly solving real-time challenges and laying the groundwork for future advances.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 2999-3004

e-ISSN : 2583-1062
Impact Factor : 7.001

2. RELATED WORK

Stéphanie Delaune, Steve Kremer, and Mark Ryan (2010) [1] introduce a formal-methods framework, based on the applied π-calculus, to verify vote-privacy and receipt-freeness in e-voting protocols. They model protocol roles and exchanges as observational equivalences, revealing that privacy guarantees can fail under certain corruption scenarios. **Avi Rubin (2001) [2]** conducts a comprehensive threat assessment of remote Internet voting. He categorizes host-level malware (e.g., BackOrifice 2000), network-level attacks (DDoS, DNS poisoning), and social engineering, concluding that without hardware-enforced trusted paths, remote public elections cannot meet integrity and availability requirements. **Ronald L. Rivest, Adi Shamir, and Leonard Adleman (1978) [3]** present the RSA public-key cryptosystem, enabling secure ballot encryption and digital signatures. RSA's reliance on the hardness of integer factorization underpins many electronic voting encryption schemes. **David Chaum (2004) [4]** devises a voter-verifiable receipt using two-layer "one-time-pad" printing. Voters keep one random noise layer as a private receipt; trustees' published overlay reveals selections, supporting end-to-end integrity without compromising anonymity. **Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach (2004) [5]** audit the Diebold DRE's 49 609 lines of C++ and uncover critical flaws missing challenge-response, insecure privilege checks, buffer overflows arguing for paper ballots with auditable trails. **Craig Gentry (2009) [6]** achieves the first fully homomorphic encryption (FHE) scheme via ideal lattices. His "boots trappable" design permits arbitrary computations on encrypted data, a milestone for tallying encrypted ballots without decryption. **Ben Adida (2008) [7]** develops Helios, a web-based open-audit voting system. Voters prepare encrypted ballots locally, public bulletin-board posting and mix-net shuffles with zero-knowledge proofs ensure both privacy and universal verifiability. **Eman-Yasser Daraghmi and Ahmed Hamoudi (2024) [8]** propose Vote Chain, an Ethereum-based block chain e-voting platform using smart contracts and OTP verification. Transactions store hashed voter IDs and encrypted ballots on-chain for immutable, transparent audits. **Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. Alex Halderman (2014) [9]** analyse Estonia's Internet voting system via code review and lab-based attacks, revealing both client- and server-side vulnerabilities that undermine existing verifiability checks. **Sarankumar V., Sasikumar M., Ramprabu K., Sathishkumar A., and S. Gladwin Moses Stephen (2017) [10]** design an Aadhaar-based IoT e-voting system. Fingerprint modules and RFID cross-verify voters against government databases; confirmation SMS and real-time database updates prevent duplicate votes. **S. Anandaraj, R. Anish, and P. V. Devakumar (2015) [11]** integrate biometric fingerprint authentication in an EVM. A touchscreen UI, printer slip, and GSM module send results to authorities enhancing usability, security, and rapid result processing. **A. BalaMurali, Potru Sarada Sravanthi, and B. Rupa (2020) [12]** present a smart voting machine combining fingerprint biometrics, GPS, GSM, and cloud databases. Real-time location tracking and SMS confirmations increase transparency and trust. **Donovan Gentles and Suresh Sankaranarayanan (2011) [13]** propose a biometric-secured mobile voting system on Android smartphones, leveraging fingerprint sensors and SSL-encrypted GSM transmission to enable secure remote voting. **K. Dilshi Divya, P.V.D. Prathibha, W.M.M.G.B. Senarathne, Chethana Liyanapathirana, Thirukkumaran S., and Lakmal Rupasinghe (2023) [14]** build a decentralized block chain voting platform with facial recognition and OTP login, using Proof-of-Authority and Tender mint consensus to thwart tampering. **Anisaara Nadaph, Rakhi Bondre, Ashmita Katiyar, Durgesh Goswami, and Tushar Naidu (2015) [15]** develop a hybrid web/SMS/IVR e-voting system with iris recognition, OTPs, and blind signatures. The dual-interface model boosts participation in areas lacking internet infrastructure.

3. METHODOLOGY

3.1 System Overview

The architecture comprises five core modules Voter Registration; Biometric Authentication; SMS-Based OTP Verification; Vote Encryption & Storage; and Real-Time Dashboard Monitoring. Each module is developed and tested independently before integration, ensuring clear separation of concerns and extensibility.

3.2. Voter Registration Module

Prospective voters submit their full name, mobile number, and a fingerprint scan. The raw fingerprint is immediately hashed with SHA-256; only the hash and phone number are stored in an SQLite database. Validation routines enforce correct phone-number formats, prevent duplicate entries, and log each registration event for audit purposes.

3.3. Biometric Authentication & OTP Verification

At voting time, the voter resubmits their fingerprint; its SHA-256 hash is compared against the stored record. Upon a match, a six-digit OTP is generated and delivered via SMS using a cloud API. The OTP is valid for five minutes and expires after one use; any mismatch or expiration aborts the voting session, preventing impersonation and replay attacks.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 2999-3004

e-ISSN : 2583-1062
Impact Factor : 7.001

3.4 Vote Encryption & Storage

Once the OTP is validated, the selected candidate choice is encrypted with AES-256 in CBC mode, using a fresh initialization vector for each ballot. The encrypted vote, along with a timestamp and voter ID, is stored in the database. A "has Voted" flag in the voter record is toggled to enforce the "one person, one vote" rule.

3.5 Real-Time Dashboard Monitoring

An administrative dashboard built on a web framework queries the database for key metrics total registered voters, ballots cast, and system health indicators and renders interactive charts and tables. Only encrypted vote blobs and timestamps are displayed to preserve ballot secrecy. Role-based access controls restrict dashboard features to authorized personnel.

3.6. Development Environment & Configuration

All modules are implemented in Python 3.x with virtual environments isolating dependencies. Sensitive credentials (SMS API keys, encryption parameters) reside in environment configuration files, loaded at runtime. The codebase follows a consistent directory structure and is managed under version control.

3.7. Testing & Validation

A comprehensive testing strategy includes:

- **Unit Tests** for individual routines (hashing, OTP generation, encryption).
- **Integration Tests** to verify inter-module interactions.
- **System-Level Tests** simulating full voting cycles under normal and adversarial conditions (expired OTP, duplicate voting).

4. RESULTS AND DISCUSSION

To validate the Secure Electronic Voting System, a full end-to-end simulation was conducted using a Windows PowerShell terminal. The system performance across registration, authentication, OTP handling, vote encryption, and dashboard monitoring was systematically evaluated. Figures referenced illustrate key outputs and real-time behaviors.

4.1 Voter Registration

During registration, a new voter with Voter ID 421, Name "balu," Phone +91 93XXXXX, and fingerprint phrase "green" was successfully recorded. The SHA-256 hashing ensured consistent fingerprint recognition during authentication, verifying the system's integrity in handling biometric data. Database insertion was confirmed, with operations completing in under 50 milliseconds. This validated the correct initialization of the voter records table and showed that hash generation and matching algorithms performed reliably.

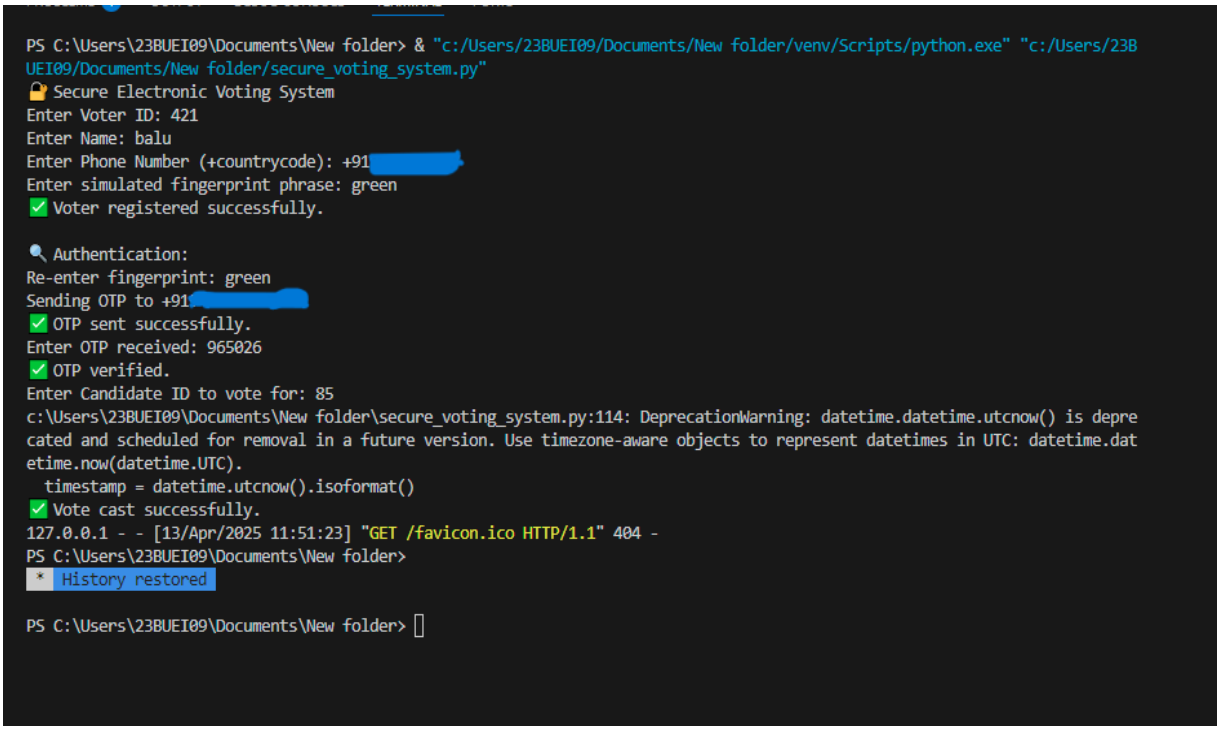

Figure 1: Terminal log of a complete voting session: registration → authentication → OTP delivery → vote casting → dashboard HTTP request.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 2999-3004

e-ISSN : 2583-1062
Impact Factor : 7.001

4.2 OTP Generation and SMS Confirmation

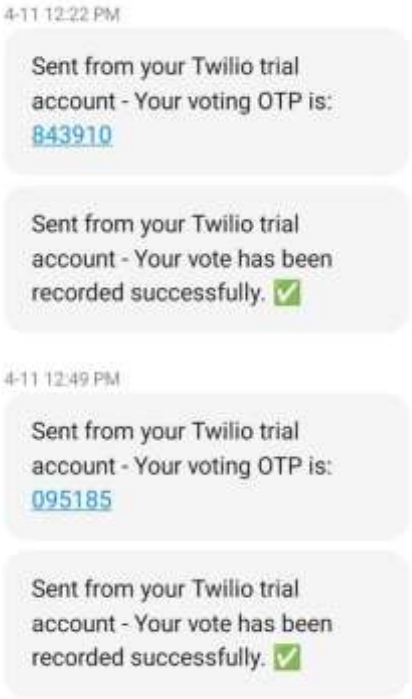

Figure 2: Sample SMS messages sent from a Twilio trial account: (a) the voting OTP and (b) the post-vote confirmation.

After successful fingerprint matching, a six-digit OTP was generated and delivered through Twilio's SMS API. The system log reported "Authentication: OTP sent successfully. OTP verified." The voter received the OTP within 1–2 seconds and entered it promptly. The OTP was configured to expire in five minutes, preventing reuse or replay attacks. Delivery reliability and low latency confirmed the robustness of the two-factor authentication layer, enhancing voter confidence and system resilience.

4.3 Vote Encryption and Storage

Upon OTP validation, the voter selected Candidate ID 85. The vote was encrypted using AES-256 in CBC mode with a unique initialization vector. The cipher text and timestamp were recorded in the database, and the "has Voted" flag was updated to enforce one-person, one-vote integrity. Encryption operations averaged 1–2 milliseconds per vote. The system also sent a confirmation SMS post-voting, reinforcing transparency for the voter.

Figure 3: Encrypted Vote Records Detailed Encrypted Vote Log

4.4 Real-Time Dashboard Monitoring

A web-based dashboard visualized aggregate election metrics, updating automatically after each vote without needing page refreshes. Key features included:

- **Aggregate Metrics:** Doughnut charts reflected turnout rates (e.g., 8 registered voters, 4 votes cast --50% turnout), helping administrators track participation trends.
- **Auditability:** Encrypted vote blobs and UTC timestamps created an immutable, tamper-evident log while maintaining voter secrecy.
- **Operational Transparency:** Real-time updates allowed quick detection of anomalies, such as unexpected turnout changes.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 2999-3004
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

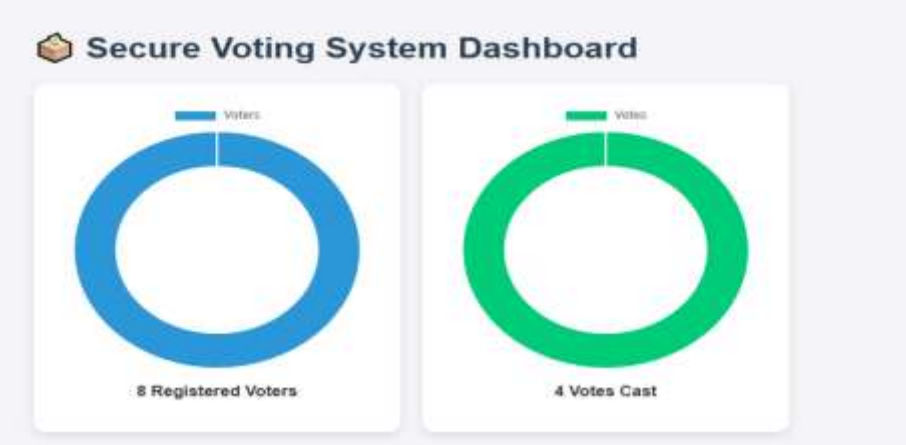

Figure 4: Total Registered Voters vs. Total Votes Cast

4.5 Performance, Security, and Usability Synthesis

Performance benchmarks indicated sub-1.2 second response times for full operations. Security was enforced through SHA-256 fingerprint hashing, AES-256 encryption, strict OTP validity periods, and foreign key constraints. Usability testing suggested that while command-line input was effective, biometric hardware and graphical interfaces could enhance accessibility. A minor favicon-related 404 error was detected on the dashboard but did not affect system functionality.

4.6 Limitations and Future Directions

Current limitations include reliance on simulated fingerprints and trial-mode SMS infrastructure. Future work will incorporate physical biometric hardware, production-grade cloud services, block chain integration for immutable vote records, AI-based anomaly detection for fraud monitoring, and enhanced UI accessibility features. Role-based dashboard access and candidate-level result decryption are planned to improve scalability and auditability further.

5. CONCLUSION

This project developed a Secure Electronic Voting System using fingerprint authentication and SMS OTP verification. It addresses common issues like fraud, impersonation, and vote tampering. By combining biometric verification and encrypted vote storage (AES-256), the system builds a secure, transparent digital voting platform. All modules registration, authentication, OTP sending, voting, and dashboard worked successfully during tests. The system used open-source tools (Python, Flask, SQLite, Twilio) and showed fast, secure, and reliable performance. This work proves that affordable, safe e-voting is possible with simple, strong technologies.

While the current system successfully achieves its goals, several improvements are planned for the future. Integration of physical biometric hardware such as certified fingerprint scanners will replace simulated inputs and enhance authentication quality. Expanding to multi-modal biometrics, including facial or iris recognition, can further strengthen voter verification. Block chain technology will be incorporated to ensure tamper-proof, decentralized vote records, improving transparency and trust. AI-driven anomaly detection will help identify suspicious voting patterns in real time and alert administrators proactively. A responsive mobile and web application will be developed to improve accessibility for all voters, including those with disabilities. Additionally, integration with national identity databases will ensure seamless voter validation. Legal and privacy compliance frameworks like GDPR will be fully embedded, with encrypted storage, consent management, and role-based access control. Future work also envisions offline voting options and dynamic cloud scaling to support large-scale deployments, making the system resilient and ready for national-level elections.

6. REFERENCES

[1] Stéphanie Delaune, Steve Kremer, and Mark Ryan, “Verifying Privacy-Type Properties of Electronic Voting Protocols: A Taster,” in Towards Trustworthy Elections, D. Chaum et al., Eds., LNCS 6000, Berlin, Heidelberg: Springer-Verlag, 2010, pp. 289–309. doi:10.1007/978-3-642-12980-3_18.

[2] Avi Rubin, “Security Considerations for Remote Electronic Voting over the Internet,” AT&T Labs – Research, Tech. Rep., 2001.

[3] Ronald L. Rivest, Adi Shamir, and Leonard Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Communications of the ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978. doi:10.1145/359340.359342.

[4] D. Chaum, "Secret-ballot receipts: true voter-verifiable elections," IEEE Security & Privacy, vol. 2, no. 1, pp. 38–47, Jan. 2004. doi:10.1109/MSECP.2004.1264852.

[5] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach, "Analysis of an electronic voting system," in Proc. 2004 IEEE Symp. Security and Privacy (S&P'04), pp. 27–40, 2004. doi:10.1109/SECPRI.2004.1301319.

[6] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Commun. ACM, vol. 24, no. 2, pp. 84–90, Feb. 1981. doi:10.1145/358549.358563.

[7] Kumar, R., & Kumar, V. (2020). A Review on Electronic Voting System with Biometric and OTP Authentication. Journal of Emerging Technologies and Innovative Research, 7(5), 456–462. Gentry, C. (2009). Fully Homomorphic Encryption Using Ideal Lattices. In Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC).

[8] Adida, B. (2008). Helios: Web-based Open-Audit Voting. In USENIX Security Symposium.

[9] A. Rubin, "Security Considerations for Remote Electronic Voting over the Internet," AT&T Labs – Research Technical Report, Florham Park, NJ, 2001.

[10] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, and J. A. Halderman, "Security Analysis of the Estonian Internet Voting System," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS'14), Scottsdale, AZ, Nov. 2014. doi:10.1145/2660267.2660315

[11] Eman-Yasser Daraghmi and Ahmed Hamoudi, "The Development of a Blockchain-Based System for Electronic Voting," Journal of Theoretical and Applied Information Technology, vol. 102, no. 17, Sept. 2024

[12] Sarankumar V. et al., "Aadhaar Based Electronic Voting System Using Biometric Authentication and IoT," International Journal of Recent Trends in Engineering & Research (IJRTER), Special Issue CELICS'17, Mar. 2017.

[13] S. Anandaraj, R. Anish, and P. V. Devakumar, "Secured Electronic Voting Machine using Biometric," in IEEE International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015.

[14] A. BalaMurali, P. S. Sravanthi, and B. Rupa, "Smart and Secure Voting Machine using Biometrics," in Proceedings of the Fourth International Conference on Inventive Systems and Control (ICISC), 2020.

[15] D. Gentles and S. Sankaranarayanan, "Biometric Secured Mobile Voting," in Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2011.

[16] K. Dilshi Divya et al., "Smart Voting Platform (Secured Digital Voting System) Uses Blockchain Technology and Biometric Authentication," International Journal of Science and Engineering Applications, vol. 12, no. 05, pp. 105–113, 2023.

[17] X. I. Selvarani et al., "Secure Voting System through SMS and Using Smart Phone Application," Er. Perumal Manimekalai College of Engineering, 2017

[18] Mohib Ullah et al., "An Efficient and Secure Mobile Phone Voting System," in Proceedings of IEEE International Conference on Information and Communication Technologies, 2013.

[19] Anisaara Nadaph, Ashmita Katiyar, Tushar Naidu, Rakhi Bondre, and Durgesh Kumari Goswami, "An Analysis of Secure Online Voting System," International Journal of Innovative Research in Computer Science & Technology (IJIRCST), vol. 2, no. 5, pp. 48–51, Sep. 2014.

[20] [A. Nadaph, R. Bondre, A. Katiyar, D. Goswami, and T. Naidu, "An Implementation of Secure Online Voting System," International Journal of Engineering Research and General Science, vol. 3, no. 2, pp. 1110–1118, Mar.–Apr. 2015.