



Electronic Voting Systems: A Thematic Review of Security, Blockchain, and Biometric-IoT Approaches

Priyanuj Gogoi¹, Sahiba Khanam¹, Nelson R Varte^{1 *}, Caleb Varnunthar Varte²

¹Department of Computer Applications, Assam Engineering College, Guwahati, Assam, India

²Department of Electronics & Telecommunication Engineering, Assam Engineering College, Assam, India

*Corresponding author email: nelson.varte@gmail.com

DOI : <https://doi.org/10.5281/zenodo.23116998>

ARTICLE DETAILS

Research Paper

Received: 18-07-2026

Accepted: 17-08-2026

Published: 25-09-2026

Keywords:

Biometric Authentication, Blockchain, Electronic Voting Machines (EVM), Internet of Things (IoT)

ABSTRACT

Electronic voting systems (EVS) have been proposed as a means of improving the speed, accessibility, and auditability of elections, yet questions of security and verifiability continue to shape both academic research and public policy. This paper presents a thematic literature review of EVS research published between 2003 and 2026, organised into four strands: general cryptographic and security surveys, biometric and Internet-of-Things (IoT)-based electronic voting machines (EVMs), blockchain-based voting architectures, and hardware/patent-level designs. The review finds that security-analysis rigour is inversely related to hardware specificity: studies that specify concrete microcontrollers and sensors rarely include a threat model or adversarial testing, while studies with rigorous security analysis rarely engage with low-cost embedded hardware. Blockchain-based EVS research has grown rapidly but increasingly repeats a common architecture - IoT-edge biometric capture, off-chain storage, and on-chain pseudonymous tallying - without resolving coercion-resistance or scalability limitations. Five specific research gaps are identified, the most significant being the near absence of hands-on adversarial security testing of low-cost

Disclaimer: The opinions, interpretations, conclusions, recommendations, analyses, and statements expressed in this research article are solely those of the author(s) and do not reflect the views, policies, or positions of the Publisher, Chief Editor, Editors, Editorial Board, Reviewers, or their affiliated institutions. The author(s) are solely responsible for ensuring the originality, authenticity, and integrity of the manuscript and for ensuring that it is free from plagiarism, AI-generated content, copyright infringement, data falsification, and any other form of academic misconduct.



biometric/IoT EVM prototypes. The review concludes with recommendations for a follow-up empirical study addressing this gap.

1. Introduction

Elections are the primary mechanism through which democratic legitimacy is conferred, and the technology used to record and count votes has direct bearing on public trust in that outcome. Since the 1960s, paper-based balloting has been progressively supplemented and, in many jurisdictions, replaced by electronic voting systems (EVS) that promise faster counting, reduced administrative cost, and improved accessibility for voters with disabilities (Ikrisi & Mazri, 2024). These systems span a wide technological range, from stand-alone Direct Recording Electronic (DRE) machines and optical-scan readers to remote internet voting platforms and, more recently, blockchain and biometric based architectures.

The adoption of EVS has not been without controversy. Independent security analyses of deployed systems, most notably Kohno et al.'s (2004) hardware-and-software-level study of a widely deployed direct-recording electronic (DRE) voting system demonstrated that convenience gains can come at the cost of exploitable vulnerabilities, including weak cryptographic key management and susceptibility to unauthorised firmware modification. Such findings have driven a sustained body of academic work seeking either to formally characterise these risks or to design systems that mitigate these risks by using cryptography, blockchain, or biometric based.

This paper reviews that body of work across four thematic strands: (i) general security and cryptographic surveys of EVS; (ii) biometric and IoT-based electronic voting machines, an area of particular relevance to low-cost embedded hardware deployments; (iii) blockchain-based EVS, currently the most active area of publication; and (iv) hardware and patent-level designs that encode voting-machine mechanisms independently of the academic literature.

The contribution of this review is threefold. First, it synthesises findings across sub-literatures including cryptographic security, blockchain architecture, and embedded biometric hardware, which are rarely discussed together despite addressing the same underlying problem. Second, it applies a consistent rigour assessment across all reviewed studies, distinguishing between security properties that are formally analysed, empirically tested, or merely asserted. Third, it identifies specific, actionable research gaps, particularly the near-absence of adversarial security testing on low-cost biometric/IoT electronic voting hardware, which can inform future empirical work in this area.

2. Review Methodology

This review adopts a PRISMA-guided systematic literature review (SLR) methodology to evaluate the security, architecture, and empirical rigor of modern electronic voting systems, reflecting the multidisciplinary nature of the source material, which spans computer security, embedded systems engineering, blockchain research, and legal/regulatory documents. Sources were identified through structured searches of IEEE Xplore, SpringerLink, ScienceDirect, ACM Digital Library, ResearchGate, arXiv, and Google Scholar, supplemented by targeted searches of the United States Patent and Trademark Office database for patent-level designs.

Search terms combined "electronic voting," "e-voting," and "EVM" with modifiers including "security," "survey," "review," "blockchain," "biometric," "fingerprint," "IoT," "Arduino," and "ESP32." Priority was given to (a) highly cited survey and review articles that establish the conceptual baseline of the field, and (b) recent primary studies (2023-2026) describing concrete implementations, to capture the current state of the art. Studies were included if they were peer-reviewed journal articles, indexed conference proceedings, granted patents, or primary legal judgments directly concerned with the design, security, or verifiability of electronic voting systems. Non-English sources, inaccessible full texts, and works with only tangential mention of EVS were excluded.

For each included study, this review extracted the methodology employed, the specific findings reported, and where applicable the hardware or cryptographic primitives used, supporting a comparative assessment of security-analysis rigour across the corpus (summarised in Table 1). This structured approach permits systematic synthesis across heterogeneous source types including empirical prototypes, surveys, patents, and legal judgments that ensure comprehensive coverage and transparent selection rigor.

3. Thematic Review of Literature

3.1 General Security and Cryptographic Surveys

The earliest and most conceptually foundational strand of literature addresses the general security requirements of electronic voting independent of any specific implementation technology. Javaid (2014) catalogues vulnerabilities associated with DRE machines and internet voting, including denial-of-service, malware, and spoofing threats, and proposes a five-element security framework encompassing ballot secrecy, fraud protection, and accurate recording. Bungale and Sridhar's (2003) early survey similarly derives a set of functional and security requirements for EVS and argues that fully remote internet voting



was, at the time, infeasible given the prevailing threat landscape, a conclusion that anticipated the continued caution with which internet voting is treated in more recent work.

More recent surveys have refined this requirements-based approach while incorporating newer cryptographic tools. Ikrisi and Mazri (2024) organise the literature around transparency, privacy, integrity, and security requirements common to DRE, optical-scan, internet, and remote e-voting systems. Barelli et al. (2025), in one of the most current and comprehensive surveys reviewed here, structure their analysis around fundamental e-voting properties, including privacy, verifiability, coercion-resistance, and eligibility, as well as the cryptographic primitives used to satisfy them. They conclude that electronic voting must simultaneously satisfy multiple, often contradictory, properties, and that the stakes of any single vulnerability are amplified by the scale of the application. Blessing et al. (2020) extend this security lens beyond the voting machine itself to the surrounding electronic infrastructure, identifying concrete privacy and integrity weaknesses in ballot-tracking and voter-registration systems used alongside vote-by-mail processes in the United States.

Collectively, this strand of the literature establishes the conceptual vocabulary, including privacy, verifiability, coercion-resistance, and auditability, against which the more implementation-focused literature reviewed in the following sections can be evaluated.

3.2 Biometric and IoT-Based Electronic Voting Machines

A substantial and growing sub-literature addresses the design of low-cost electronic voting machines built around biometric authentication and Internet-of-Things (IoT) connectivity, typically using commodity microcontrollers such as the Arduino Uno or ESP32 paired with optical fingerprint modules. Desai et al. (2020) describe an Arduino Uno and ESP32-based prototype using an SM-630 fingerprint module and a Google Cloud backend, validated through functional testing of the fingerprint-matching and display logic. Sharathchandra et al. (2023) similarly proposes an architecture built around an optical fingerprint module communicating over UART, emphasizing accuracy and cost-effectiveness. However, they note, as a limitation acknowledged by later citing work, that continuous dependence on a web server and Wi-Fi connectivity introduces a tampering surface that the paper does not further analyze.

Srilatha et al. (2024) present a comparable design using an R307 fingerprint module, Arduino Uno controller, and ESP8266 Wi-Fi module, reporting false-acceptance and false-rejection rates below one percent; notably, an FAR approaching 1% represents a significant security vulnerability for large-scale elections where unauthorized access must be near zero. The paper additionally tabulates accuracy claims



across ten prior biometric EVM studies, providing a useful, if largely self-reported, benchmark of the sub-field. Security claims in this study, including resistance to impersonation and coercion, are asserted rather than empirically demonstrated through threat modelling or attack testing. Zamir et al. (2022) propose binding centralized government identity-linked biometric data to EVM, though centralized identity linkages introduce severe legal, regulatory, and privacy constraints during live balloting.

Not all studies in this cluster implement the biometric hardware they describe. Yusoff et al. (2023), despite a title referencing fingerprint biometrics, implement voter verification in a TINKERCAD simulation using a keypad entered identity number in place of a physical fingerprint sensor. No threat model or attack testing accompanies the design; security is asserted rather than demonstrated. This case is illustrative of a broader pattern in the cluster: studies that specify concrete, named hardware components report functional accuracy and timing metrics but do not, in general, subject their designs to adversarial evaluation, sensor-spoofing tests, or communication-channel security analysis, a gap discussed further in Section 4.

3.3 Blockchain-Based Electronic Voting Systems

Blockchain-based EVS constitutes the most rapidly growing strand of the reviewed literature. Early systematic work in this area includes Jafar et al.'s (2021) review of blockchain-based electronic voting, which surveys the privacy and security properties blockchain integration can offer while noting that transaction throughput and remote-participation security remain unresolved. Pawlak and Poniszewska-Marańda (2021) conducted a systematic literature review of 35 (in an associated later analysis, 52) publications on blockchain-based e-voting, characterising the technologies, testing methods, and cryptographic solutions used across the field and identifying end-to-end verifiability and remote authentication as persistent open problems. Almeida et al. (2023) trace the evolution of the field from 1970s public-key cryptographic voting schemes through to blockchain-based approaches, situating blockchain as the latest, but not final, stage in a decades-long research trajectory.

More recent work has moved from survey-level synthesis toward architectural consolidation. Ohize et al. (2024), drawing on an initial pool exceeding 22,000 search results narrowed through a structured screening process, provide one of the most comprehensive recent syntheses of blockchain e-voting architectures, citing real-world pilots in Estonia and Switzerland and identifying cybersecurity risk, resource intensity, and infrastructure requirements as the primary barriers to wider adoption. El Kafhali (2024) proposes a conceptual end-to-end blockchain voting design incorporating zero-knowledge proofs for privacy. However, the study explicitly notes that public blockchains such as Ethereum process on the order of ten to thirty transactions per second, a throughput ceiling that constrains large-scale deployment.



Furthermore, off-chain components introduced to reduce cost correspondingly increase the attack surface. Barbu et al. (2022) offer a qualitative benefits-and-challenges analysis grounded in Romania's use of a blockchain-based voter-turnout reporting tool. They conclude that blockchain can help signal fraud and prevent multiple voting, while noting that a turnout-reporting tool falls short of full blockchain-based vote casting.

A distinct and increasingly prominent sub-cluster fuses blockchain with biometric and IoT-based voter authentication. Ibrahim et al. (2021) describe ElectionBlock, a permissioned-blockchain prototype combining fingerprint authentication with SHA-256 hashing and Merkle-tree structures for vote-integrity assurance, though later analyses note that its permissioned architecture allows the operator to de-anonymise voters, a limitation the original study does not resolve. Hossain Faruk et al. (2024) similarly combine fingerprint and facial-recognition authentication with a Hyperledger Fabric network. The most methodologically rigorous study in this sub-cluster is Rifat et al. (2026), whose prototype integrates an ESP32-connected R307 fingerprint sensor, facial recognition via InsightFace/ArcFace embeddings, and an Ethereum smart contract, evaluated against an explicit adversary taxonomy spanning external attackers, malicious voters, compromised biometric components, insiders, network-level threats, and physical/side-channel attacks. The study reports 96.09 percent face-verification accuracy on the LFW benchmark, a configured fingerprint false-acceptance rate of 0.01 percent, and an estimated deployment cost of approximately four US dollars per vote at prevailing gas prices, an expense profile that highlights the economic non-viability of public mainnets for large-scale public elections without Layer-2 scaling or permissioned sidechains.

Taken together, this strand of the literature shows a field that has largely converged on a shared reference architecture, including IoT-edge biometric capture, off-chain template storage, and on-chain pseudonymous tallying. However, it has not yet resolved the coercion-resistance, receipt-freeness, and scalability limitations that the earlier cryptographic-survey literature identifies as prerequisites for general-election use.

3.4 Hardware and Patent-Level Designs

A smaller but relevant body of work exists at the level of granted patents, which encode voting-machine mechanisms independently of the peer-reviewed academic literature. United States Patent 7,637,429 describes a voter-verified paper audit trail mechanism in which a vote-security device digitally signs ballot selections before an audit-trail printer produces a paper record that the voter may view, but not physically access, prior to acceptance or rejection. Related patents extend this design space to biometric

voter verification held in a database independent of cast-ballot records (US 8,201,738; US 8,905,306) and to blockchain-based contest recording (US 20170109955A1; US 10,783,733B2). These patents anticipate, in mechanism, many of the biometric and blockchain-based designs subsequently proposed in academic literatures. However, as patents rather than peer-reviewed studies, they do not themselves include independent security evaluation, leaving open the same adversarial-testing gap identified in Section 3.2.

Table 1. Comparative Summary of Selected Electronic Voting Systems Studies

Study	Year	Category	Methodology	Security-Analysis Depth
Kohno et al.	2004	Hardware/software (DRE)	Hands-on security analysis, deployed system	High - working vulnerabilities demonstrated
Javaid	2014	General survey	Narrative review	Conceptual only
Jafar, Ab Aziz, & Shukur	2021	Blockchain survey	Narrative review	Conceptual only
Pawlak & Poniszewska-Marańda	2021	Blockchain SLR	Systematic review (35 papers)	Trend analysis, no primary testing
Desai, Patoliya, & Mewada	2020	Biometric/IoT EVM	Prototype build	Functional testing only
Zamir, Khan, & Sarosh	2022	Biometric/IoT EVM	Prototype/design proposal	Conceptual, asserted security
Sharathchandra et al.	2023	Biometric/IoT EVM	Design review	Conceptual, asserted security
Yusoff et al.	2023	Biometric/IoT EVM	Simulation (no physical sensor)	None - no threat model
Almeida et al.	2023	Blockchain SLR	Systematic literature	Trend analysis, no



			survey	primary testing
Srilatha et al.	2024	Biometric/IoT EVM	Prototype build + literature comparison	Asserted, not tested
El Kafhali	2024	Blockchain	Conceptual design	Requirements-level, not tested
Ohize et al.	2024	Blockchain SLR	Systematic review (large corpus)	Trend analysis, no primary testing
Hossain Faruk et al.	2024	Blockchain + biometric	Prototype (Hyperledger Fabric)	Functional testing only
Barelli, D'Onghia, & Longari	2025	General survey	Property-based literature survey	Conceptual, comprehensive
Rifat et al.	2026	Blockchain + biometric + IoT	Prototype with explicit adversary taxonomy	Moderate-to-High - multi-vector adversary taxonomy stated, limited adversarial testing

Note. "Security-Analysis Depth" reflects whether the reviewed study included a stated threat model or adversarial/empirical testing, as opposed to functional testing or asserted (but untested) security claims.

4. Discussion: Trends and Research Gaps

Three trends emerge across the reviewed literature. First, the field has converged on a common blockchain-biometric-IoT reference architecture, including edge-level biometric capture, off-chain template storage, and on-chain pseudonymous tallying. Consequently, recent prototype studies (Ohize et al., 2024; Rifat et al., 2026; Hossain Faruk et al., 2024) increasingly resemble one another architecturally, reducing the marginal novelty of further "implementation on a new blockchain" contribution. Second, cryptographic maturity across the corpus is uneven: advanced properties such as zero-knowledge proofs, homomorphic encryption, and coercion-resistance are extensively discussed in the survey literature (Barelli et al., 2025; El Kafhali, 2024) but are rarely implemented in prototype studies. This includes the comparatively rigorous work of Rifat et al. (2026), which explicitly defers these mechanisms to future work. Third, there remains a



persistent gap between the theoretical guarantees claimed in the cryptographic literature and the performance actually reported in deployed or prototyped systems. Specifically, the roughly ten-to-thirty transaction-per-second ceiling of public Ethereum is repeatedly cited as a practical constraint (El Kafhali, 2024).

Against this backdrop, five specific research gaps can be identified. The most significant practical gap (Gap A) is the near-total absence of hands-on adversarial security analysis of low-cost embedded biometric/IoT voting hardware. However, this gap stems partly from inherent physical limitations, as commodity microcontrollers such as the ESP32 and Arduino lack dedicated hardware security modules (HSMs) and physical tamper-proofing, making side-channel and firmware protection fundamentally difficult. Studies in this cluster report functional accuracy, false-acceptance/rejection rates, and voting latency, but rarely include a stated threat model, sensor-spoofing or presentation-attack testing, communication-bus interception, or firmware-integrity analysis; in at least one case reviewed here (Yusoff et al., 2023), the claimed biometric sensor was not physically implemented at all. This stands in marked contrast to the hardware-level rigor of Kohno et al. (2004), which remains a methodological benchmark for adversarial voting-hardware analysis more than two decades after publication. A second, related gap (Gap B) concerns the near-total absence of systematic liveness and presentation-attack testing on the low-cost optical fingerprint sensors that dominate this literature. A third gap (Gap C) concerns the security of the IoT and cloud tier itself: prototypes routinely offload authentication and vote data to commercial cloud platforms over Wi-Fi, yet the confidentiality and integrity of this channel, the functional analogue of the central-tabulator attack surface in traditional DRE systems, is essentially unexamined. A fourth gap (Gap D) is the disconnect between the patent literature, which already encodes biometric- and blockchain-based voting mechanisms, and the certification and regulatory requirements that election authorities typically impose on deployed voting hardware, which academic prototypes rarely engage with directly. A fifth gap (Gap E) concerns reproducibility: much of the implementation-focused literature is published in venues with limited peer-review depth and does not release code, firmware, or wiring documentation sufficient for independent replication.

These gaps collectively suggest that the most productive direction for near-term empirical research is not a further blockchain-integration prototype, but a structured, adversarial security evaluation of the field's dominant low-cost biometric/IoT reference architecture. Specifically, this involves extending the Kohno et al. (2004) methodology to modern ESP32 and Arduino-class hardware, as well as reporting the presentation-attack, communication-interception, and firmware-integrity metrics that the current literature omits.

5. Conclusion and Future Directions

This review has organized the electronic voting systems literature into four thematic strands: general security and cryptographic surveys, biometric/IoT-based electronic voting machines, blockchain-based architectures, and hardware/patent-level designs. Across this literature, a consistent pattern emerges: the studies with the greatest hardware specificity conduct the least rigorous security analysis, while the studies with the greatest security rigor rarely engage with the low-cost embedded hardware that increasingly characterizes real-world biometric/IoT voting-machine proposals. This gap has practical consequences beyond academia, since regulatory and certification bodies overseeing electronic voting hardware increasingly require demonstrable security assurances that the current biometric/IoT literature does not yet provide.

Future work should prioritize closing the adversarial-testing gap identified in Section 4 through a structured hardware security evaluation of a representative low-cost biometric/IoT electronic voting machine that reports presentation-attack success rates, communication-bus interception feasibility, and firmware-tamper detectability alongside the functional accuracy metrics that dominate the current literature. Releasing accompanying wiring diagrams, firmware, and test harnesses would additionally address the reproducibility gap observed across much of the implementation-focused literature reviewed here. Such a study would extend the methodological tradition established by Kohno et al. (2004) to the current generation of embedded voting hardware and would connect directly to the verification and auditability requirements articulated throughout the cryptographic-survey literature reviewed here.

References

- Almeida, S., Baiardi, F., Di Francesco Maesa, D., & Ricci, L. (2023). Impact of decentralization on electronic voting systems: A systematic literature survey. *IEEE Access*, 11, 132389-132423. <https://doi.org/10.1109/ACCESS.2023.3336476>
- Barbu, D.-C., Dobrița, G., Oprea, S.-V., Bâra, A., & Diaconița, V. (2022). Challenges and benefits of blockchain-based electronic voting system. *Romanian Journal of Information Technology and Automatic Control*, 32(4), 117-128. <https://doi.org/10.33436/v32i4y202210>
- Barelli, R., D'Onghia, M., & Longari, S. (2025). Towards secure electronic voting: A survey on e-voting systems and attacks. *IEEE Access*, 13, 89600-89626. <https://doi.org/10.1109/ACCESS.2025.3569334>



- Blessing, J., Gomez, J., McCoy, P., & Nguyen, T. (2020). Security survey and analysis of vote-by-mail systems (arXiv:2005.08427). arXiv. <https://doi.org/10.48550/arXiv.2005.08427>
- Bungale, P. P., & Sridhar, S. (2003). Electronic voting: A survey [Course report]. Department of Computer Science, Johns Hopkins University.
- Desai, M., Patoliya, J., & Mewada, H. (2020). Internet of Things (IoT)-based advanced voting machine system enhanced using low-cost IoT embedded device and cloud platform. In Proceedings of the International Conference on Trends in Information Technology (ICTIS 2020).
- El Kafhali, S. (2024). Blockchain-based electronic voting system: Significance and requirements. *Mathematical Problems in Engineering*, 2024, Article 5591147. <https://doi.org/10.1155/2024/5591147>
- Hossain Faruk, M. J., et al. (2024). Transforming online voting: A novel system utilizing blockchain and biometric verification for enhanced security, privacy, and transparency. *Cluster Computing*, 27, 4015-4034. <https://doi.org/10.1007/s10586-023-04261-x>
- Ibrahim, M., Ravindran, K., Lee, H., Farooqui, O., & Mahmoud, Q. H. (2021). ElectionBlock: An electronic voting system using blockchain and fingerprint authentication. In Proceedings of the IEEE 18th International Conference on Software Architecture Companion (ICSA-C) (pp. 123-129). IEEE. <https://doi.org/10.1109/ICSA-C52384.2021.00033>
- Ikrissi, G., & Mazri, T. (2024). Electronic voting: Review and challenges. In *Innovations in Smart Cities Applications* (Vol. 7, Lecture Notes in Networks and Systems, Vol. 906). Springer. https://doi.org/10.1007/978-3-031-53824-7_11
- Jafar, U., Ab Aziz, M. J., & Shukur, Z. (2021). Blockchain for electronic voting system-Review and open research challenges. *Sensors*, 21(17), Article 5874. <https://doi.org/10.3390/s21175874>
- Javaid, M. A. (2014). Electronic voting system security. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2393158>
- Kohno, T., Stubblefield, A., Rubin, A. D., & Wallach, D. S. (2004). Analysis of an electronic voting system. In Proceedings of the 2004 IEEE Symposium on Security and Privacy (S&P'04) (pp. 27-40). IEEE. <https://doi.org/10.1109/SECPRI.2004.1301313>
- Ohize, H. O., Onumanyi, A. J., Umar, B. U., Ajao, L. A., Isah, R. O., Dogo, E. M., Nuhu, B. K., Olaniyi, O. M., Ambafi, J. G., Sheidu, V. B., & Ibrahim, M. M. (2024). Blockchain for securing electronic voting



systems: A survey of architectures, trends, solutions, and challenges. *Cluster Computing*, 28, Article 132. <https://doi.org/10.1007/s10586-024-04709-8>

Pawlak, M., & Poniszewska-Marańda, A. (2021). Trends in blockchain-based electronic voting systems. *Information Processing & Management*, 58(4), Article 102595. <https://doi.org/10.1016/j.ipm.2021.102595>

Rifat, T. M., Rahman, M. N., Das, S. C., Mahbub, M., Sanaullah, M., Ashiqussalehin, M., Aloteibi, S., & Moni, M. A. (2026). Blockchain-integrated IoT biometric architecture for secure and decentralized electronic voting. *Journal of King Saud University - Computer and Information Sciences*, 38, Article 540. <https://doi.org/10.1007/s44443-026-00861-w>

Sharathchandra, Mathew, J. A., & Prem Kumar, B. C. (2023). IoT based fingerprint voting system. *International Journal of Creative Research Thoughts*, 11(5).

Srilatha, C. H., et al. (2024). Fingerprint-based biometric smart electronic voting machine using IoT and advanced interdisciplinary approaches. *E3S Web of Conferences*, 507, Article 01037. <https://doi.org/10.1051/e3sconf/202450701037>

U.S. Patent No. 7,637,429. (2009). Electronic voting system and associated method. U.S. Patent and Trademark Office.

Yusoff, Z. M., Yusnoor, Y., Markom, A. M., Nordin, S. A., & Ismail, N. (2023). Fingerprint biometric voting machine using Internet of Things. *Indonesian Journal of Electrical Engineering and Computer Science*, 30(2), 699-706. <https://doi.org/10.11591/ijeecs.v30.i2.pp699-706>

Zamir, M. A., Khan, D. A., & Sarosh, M. (2022). Secure electronic voting machine using biometric authentication. In *Proceedings of the 9th International Conference on Computing for Sustainable Global Development (INDIACom)*. IEEE.