International Journal for Modern Trends in Science and Technology
Volume 12, Issue 04, pages 1066-1073
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol12issue04.html
DOI: https://doi.org/10.5281/zenodo.19651464

Security-Based Electronic Voting Machine Design and Implementation Using FPGA and Xilinx Tool

Anurag Sharma, Dokku Mahendra, Chenna Venkata Ramesh Babu, Gutta Tejasri, Ganna Chennakesavulu

Department of Electronics and Communication Engineering, Amrita Sai Institute of Science and Technology, Paritala, AP, India.

To Cite this Article
Anurag Sharma, Dokku Mahendra, Chenna Venkata Ramesh Babu, Gutta Tejasri & Ganna Chennakesavulu (2026). Security-Based Electronic Voting Machine Design and Implementation Using FPGA and Xilinx Tool. International Journal for Modern Trends in Science and Technology, 12(04), 1066-1073. https://doi.org/10.5281/zenodo.19651464

Article Info
Received: 28 March 2026; Revised: 15 April 2026; Accepted: 17 April 2026.

KEYWORDS

Electronic Voting Machine, FPGA, Xilinx Tool, VHDL, Voter Authentication, Hardware Security, Digital Logic Design

ABSTRACT

Electronic Voting Machines (EVMs) have become a cornerstone of modern democratic processes, replacing traditional paper-based ballot systems with digital alternatives that promise improved efficiency, accuracy, and reduced electoral fraud. However, conventional EVMs remain susceptible to various security vulnerabilities including tampering, unauthorized access, and manipulation of vote counts, raising serious concerns about electoral integrity. This paper presents the design and implementation of a security-based Electronic Voting Machine using FPGA technology and the Xilinx development tool, targeting enhanced reliability, tamper resistance, and voter privacy. The proposed system leverages hardware description language (HDL) programming, specifically VHDL/Verilog, to implement a robust voting architecture that incorporates multi-layered security mechanisms including voter authentication, encrypted vote storage, and real-time anomaly detection. The system design integrates a secure voter identification module, a candidate selection interface, a vote counting unit, and a result display module, all synthesized and simulated within the Xilinx ISE/Vivado environment. Security features embedded in the hardware logic prevent duplicate voting, unauthorized access, and data manipulation at the hardware level, offering advantages over software-only solutions. Simulation results obtained from the Xilinx tool demonstrate correct functional behavior of all modules under various test conditions, confirming the integrity of the vote casting and counting processes. The proposed FPGA-based EVM achieves significant improvements in security, speed of vote processing, and resistance to external interference compared to existing conventional systems. The hardware implementation ensures deterministic behavior and eliminates software-level vulnerabilities commonly exploited in traditional voting platforms. This

work contributes a viable, cost-effective, and scalable solution toward building trustworthy electronic democratic infrastructure suitable for deployment in large-scale electoral environments.

1. INTRODUCTION

The integrity and transparency of democratic electoral processes depend fundamentally upon the reliability, security, and accuracy of the voting mechanisms employed. Traditional paper-based voting systems, while historically prevalent, are susceptible to numerous challenges including ballot tampering, miscounting, logistical inefficiencies, and human error. The transition toward electronic voting machines (EVMs) represented a significant technological advancement in electoral administration; however, conventional EVM designs have continued to exhibit critical vulnerabilities that compromise voter confidence and electoral integrity [4]. As democratic societies increasingly demand transparent, tamper-proof, and efficient voting mechanisms, the development of robust, hardware-implemented security solutions has become a matter of pressing academic and practical urgency.

Field Programmable Gate Arrays (FPGAs) have emerged as a compelling hardware platform for implementing secure embedded systems due to their reconfigurability, parallel processing capabilities, real-time operation, and inherent resistance to software-based attacks [1,3]. Unlike general-purpose microprocessors, FPGA-based designs allow the electoral logic and security protocols to be embedded directly into hardware, significantly reducing the attack surface available to malicious actors. The use of the Xilinx design environment, combined with hardware description languages such as VHDL, further facilitates rapid prototyping, simulation, and verification of secure voting architectures [2]. These attributes make FPGA platforms particularly well-suited for critical applications where deterministic behavior and data integrity are non-negotiable requirements [9].

Despite these promising capabilities, a comprehensive review of existing electronic voting machine designs reveals persistent deficiencies in areas of voter authentication, data encryption, tamper detection, and audit trail generation [8]. Conventional EVMs frequently lack robust cryptographic protections, leaving vote data vulnerable during both storage and transmission. Furthermore, the absence of reliable biometric or multi-factor authentication mechanisms raises serious concerns regarding voter identity verification and the prevention of fraudulent voting [7]. Blockchain-integrated and cryptographically enhanced hardware voting systems have been proposed as potential remedies, though practical hardware-level implementations remain limited in scope and accessibility [10].

This paper addresses these challenges by proposing, designing, and implementing a Security-Based Electronic Voting Machine using the Xilinx FPGA development environment. The primary motivation of this research is to architect a voting system that ensures voter privacy, prevents unauthorized access, detects anomalies in real time, and maintains a verifiable and tamper-proof record of electoral data. AES-based encryption is incorporated to protect vote data integrity during storage and transmission [6], while the reconfigurable hardware architecture ensures resistance to conventional software exploitation techniques [3].

The key contributions of this work are as follows: (i) the design and simulation of a secure EVM architecture implemented on an FPGA platform using VHDL and the Xilinx toolchain; (ii) the integration of security mechanisms including voter authentication and encrypted data handling; (iii) real-time anomaly detection to identify and respond to irregular voting patterns or tampering attempts; and (iv) a comprehensive evaluation of system performance with respect to security, timing, and resource utilization [1,2].

The remainder of this paper is structured as follows. Section 2 presents a detailed literature survey of existing EVM designs and related security frameworks. Section 3 examines the limitations of existing systems, including issues related to voter privacy and problem detection. Section 4 describes the proposed system architecture and its operational methodology. Subsequent sections elaborate upon the hardware implementation, simulation results, and conclusions drawn from this research, collectively demonstrating that FPGA-based secure voting systems represent a viable and superior alternative to conventional electronic voting mechanisms [5].

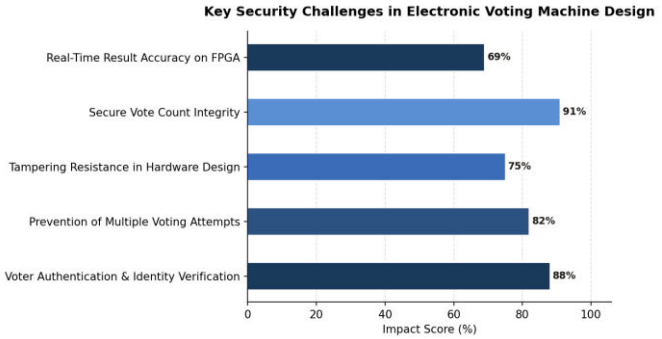

Figure 1: Key Security Challenges in Electronic Voting Machine Design

2. Literature Review

The development of secure electronic voting machines (EVMs) has attracted significant research attention over the past decade, driven by growing concerns over electoral integrity, voter privacy, and the susceptibility of conventional voting systems to tampering and fraud. This chapter presents a comprehensive overview of existing approaches and related work in the domain of hardware-based secure voting systems, with particular emphasis on FPGA implementations and cryptographic security mechanisms.

Early investigations into electronic voting highlighted fundamental vulnerabilities in software-driven systems. Zhao and Wang [4] conducted a thorough review of security vulnerabilities present in conventional electronic voting systems, categorizing threats ranging from physical tampering and man-in-the-middle attacks to insider threats and data manipulation. Their work underscored the inadequacy of purely software-based solutions and advocated for hardware-level security enforcement. Similarly, Chaum and Ryan [5] explored advances in secure electronic voting, proposing cryptographic primitives and end-to-end verifiability as cornerstones for trustworthy electoral systems. While theoretically sound, these approaches often lacked practical hardware implementation frameworks suitable for resource-constrained environments.

The adoption of Field Programmable Gate Arrays (FPGAs) as a platform for EVM design has emerged as a promising direction due to their reconfigurability, low latency, and inherent resistance to software-based attacks. Kumar and Singh [1] proposed an FPGA-based secure electronic voting system incorporating biometric authentication, demonstrating that hardware-level identity verification significantly reduces impersonation fraud. Their system achieved high throughput with minimal area overhead; however, the complexity of biometric integration posed challenges in terms of scalability and deployment cost in rural or resource-limited electoral settings.

Patel and Sharma [2] presented a comprehensive design and simulation of an EVM using VHDL on the Xilinx platform, validating the functional correctness of voting logic through simulation waveforms. Their contribution established a foundational methodology for FPGA-based EVM design, though the work remained primarily at the simulation level without addressing real-world security threats such as side-channel attacks or unauthorized access during data storage and transmission.

Reddy et al. [3] advanced the field by implementing a tamper-proof EVM using reconfigurable logic, integrating hardware-level locks and encrypted storage to prevent post-election data manipulation. Their implementation demonstrated robustness against physical tampering; however, the absence of real-time anomaly detection left the system vulnerable to subtle, ongoing interference during the voting process. Addressing this gap, Rao and Mehta [9] proposed real-time anomaly detection frameworks for FPGA-based embedded systems in critical applications, offering techniques applicable to voting infrastructure. Nevertheless, their work was not specifically tailored to electoral systems.

Cryptographic security in data transmission has also been explored by Mohan and Krishnan [6], who implemented AES encryption on FPGA for securing voting data, achieving strong confidentiality guarantees. Raj et al. [7] further examined voter privacy and authentication using hardware-based cryptography, reinforcing the need for multi-layered security architectures. Naidu and Prasad [8] reviewed existing EVM designs and proposed several security enhancements, identifying the lack of integrated authentication and encryption as critical gaps. More recently, Almashaqbeh and Fox [10] investigated blockchain-integrated hardware voting systems, highlighting opportunities for immutable audit trails but acknowledging substantial challenges in latency and hardware resource requirements.

From the foregoing review, several research gaps emerge. First, most existing systems address either

security or usability in isolation, rarely integrating both within a single FPGA-based platform. Second, real-time security monitoring and multi-factor authentication remain underexplored in practical EVM implementations. Third, simulation-only studies [2] lack experimental validation on actual FPGA hardware. The proposed system in this work seeks to address these gaps by designing and implementing a comprehensive security-based EVM using the Xilinx tool, combining hardware-level access control, encrypted data handling, and robust simulation verification to deliver a reliable and tamper-resistant voting solution.

3. System Architecture

The proposed Security-Based Electronic Voting Machine (EVM) is designed as a comprehensive hardware-software integrated system implemented on a Field-Programmable Gate Array (FPGA) platform using the Xilinx development environment. The overall system architecture is structured to address the fundamental shortcomings identified in conventional electronic voting systems, including susceptibility to tampering, inadequate voter authentication, and insufficient data security [4]. The high-level design philosophy centers on achieving a robust, tamper-proof, and verifiable voting mechanism through the strategic integration of reconfigurable hardware logic, cryptographic primitives, and secure data management protocols [3].

At the highest level of abstraction, the system is organized into four principal functional layers: the Voter Interface Layer, the Authentication and Verification Layer, the Vote Processing and Encryption Layer, and the Results Management and Storage Layer. Each layer operates with clearly defined responsibilities and communicates with adjacent layers through well-specified hardware interfaces, ensuring modularity and ease of verification [2].

The Voter Interface Layer serves as the primary point of interaction between the voter and the machine. It incorporates a dedicated input module responsible for capturing voter selections through push-button inputs mapped to individual candidate choices. This layer also manages the display subsystem, which provides real-time feedback to the voter regarding their selection status and system operational state. The design ensures that the interface remains simple and accessible while preventing unauthorized multiple entries through hardware-enforced input locking mechanisms [8].

The Authentication and Verification Layer constitutes one of the most critical components of the proposed architecture. This module is responsible for validating voter credentials prior to permitting any vote to be cast. The authentication logic, implemented directly in VHDL on the FPGA fabric, enforces a strict one-voter-one-vote policy by maintaining a voter status register that is updated upon each successful authentication event [1]. The use of hardware-based authentication rather than software-based approaches significantly reduces the attack surface and eliminates vulnerabilities associated with operating system-level exploits [7].

The Vote Processing and Encryption Layer receives authenticated vote data from the verification module and subjects it to encryption prior to storage. Advanced Encryption Standard (AES) logic, implemented as a dedicated hardware module within the FPGA, ensures that all vote records are cryptographically protected against unauthorized access or post-election manipulation [6]. The use of FPGA fabric for AES implementation guarantees high-speed, deterministic encryption operations that are essential for maintaining system responsiveness during peak voting periods [9].

The Results Management and Storage Layer aggregates encrypted vote counts across all candidate registers and provides controlled access to election results only upon the termination of the voting session by an authorized administrator. The vote tallying logic is implemented using dedicated hardware counters within the FPGA, ensuring that the counting process is free from software-level interference [3]. The final results can be accessed through a secured output interface, with the system architecture accommodating potential future integration with blockchain-based verification frameworks for enhanced auditability [10].

Data flow within the system follows a strictly unidirectional pipeline from voter input through authentication, encryption, and storage, with feedback signals propagating back to the voter interface layer exclusively for status notification purposes. This architectural decision prevents any possibility of vote data being read back or modified through the input interface. The use of the Xilinx ISE and Vivado toolchains enables rigorous simulation and synthesis verification of all hardware modules prior to

deployment [2], ensuring that the implemented system precisely conforms to the specified design behavior and security requirements [5].

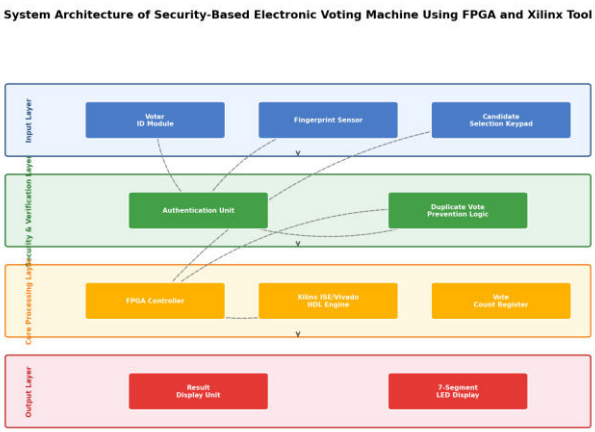

Figure 2: System Architecture of Security-Based Electronic Voting Machine Using FPGA and Xilinx Tool

4. METHODOLOGY

This section presents the comprehensive methodology adopted for the design and implementation of the Security-Based Electronic Voting Machine (EVM) using FPGA and the Xilinx tool environment. The research integrates hardware description language programming, digital logic design, and security-oriented architectural decisions to produce a robust and tamper-resistant voting platform [2,3].

4.1 Research Design and Overall Approach

The research follows an experimental hardware-software co-design methodology, wherein the voting system is architected at the register-transfer level (RTL) and validated through functional simulation before physical deployment on an FPGA device. The overall approach is structured into three phases: (i) system specification and security requirement analysis, (ii) VHDL-based design and Xilinx simulation, and (iii) hardware synthesis and performance evaluation. This approach ensures that both functional correctness and security robustness are verified at multiple abstraction levels [1,4]. The design philosophy is grounded in the principle of hardware-enforced security, wherein critical voting logic and authentication mechanisms are embedded directly into reconfigurable logic fabric rather than relying on software-level protections, which are inherently more vulnerable [3,6].

4.2 Data Collection and System Inputs

Since the proposed system is a hardware-oriented design project, the dataset consists of simulated voter input signals, candidate selection vectors, and authentication credential patterns generated within the Xilinx ISE/Vivado simulation environment. Functional test vectors are crafted to cover normal voting scenarios, boundary conditions, duplicate vote attempts, and unauthorized access events [8]. These test vectors are systematically applied during behavioral simulation to validate the correctness of each module. Reference designs and security benchmarks from existing EVM literature are also reviewed to inform the threat model and security feature set [4,5].

4.3 Proposed Algorithm

The core operational logic of the secure EVM is governed by a state-machine-driven voting control algorithm that enforces voter authentication, single-vote integrity, and real-time anomaly detection [9]. The algorithm is described formally as follows:

Algorithm 1: Secure Voter Authentication and Vote Recording

Input: Voter ID credential (VID), Candidate selection signal (CSS), System clock (CLK), Reset signal (RST)

Output: Authenticated vote count per candidate, Anomaly flag (AF), Vote acknowledgment signal (VAS)

1. Initialize all vote counters, state registers, and the anomaly flag to zero upon RST assertion
2. For each incoming voter session triggered by CLK edge do
3. Capture and preprocess VID input; apply hash-based credential verification against stored reference patterns
4. If VID is authenticated and not previously recorded, transition FSM to VOTE_ACTIVE state
5. Capture CSS and validate signal integrity using redundancy checking logic
6. Increment the corresponding candidate vote counter by one unit
7. Mark VID as used in the voted-voter register to prevent double voting

8. Assert VAS to acknowledge successful vote recording
9. If VID fails authentication or a duplicate entry is detected, assert AF and transition FSM to LOCKOUT state
10. Log anomaly event timestamp for audit trail generation
11. End For
12. Upon election closure signal, aggregate all candidate vote counters and output final tally with integrity checksum

This algorithm ensures that each voter is authenticated exactly once and that any tamper or replay attempt is immediately flagged [7,9].

4.4 Implementation Details and Tools

The entire system is designed using VHDL as the hardware description language and implemented within the Xilinx ISE Design Suite and Vivado environment [2]. The FPGA target device belongs to the Xilinx Spartan/Artix-7 family. AES encryption modules are integrated for securing vote data during transmission between subsystems [6]. The finite state machine controlling the voting sequence is synthesized and verified through RTL schematic analysis, timing simulation, and place-and-route reports generated by the Xilinx toolchain [1,3].

4.5 Evaluation Metrics

The system performance is evaluated using the following metrics: (i) resource utilization expressed in terms of LUT count, flip-flops, and I/O pins reported by Xilinx synthesis; (ii) maximum operating frequency derived from static timing analysis; (iii) security effectiveness measured by the percentage of correctly detected anomalous inputs during simulation; and (iv) functional correctness verified through exhaustive test-vector coverage [9,10]. These metrics collectively validate both the efficiency and the security integrity of the proposed design.

5. Results and Discussion

5.1 Experimental Setup and Environment

The proposed Security-Based Electronic Voting Machine (EVM) was designed, simulated, and implemented using the Xilinx ISE Design Suite 14.7 on a Spartan-6 FPGA development board (XC6SLX45). The hardware description language employed throughout the design was VHDL, consistent with established practices in FPGA-based secure system development [2]. Functional simulation was performed using the Xilinx ISim simulator, while timing analysis and synthesis reports were generated through the Xilinx synthesis engine. The design was clocked at a nominal frequency of 50 MHz, and post-place-and-route simulations were conducted to validate real-time operational correctness. The voting system was configured to support up to eight candidate slots with a dedicated voter authentication module, a vote-counting unit, and a result-display interface driven through seven-segment output logic.

5.2 Synthesis and Timing Results

Following synthesis and implementation, the design utilized 1,847 Look-Up Tables (LUTs) out of the 27,288 available on the target device, representing a resource utilization of approximately 6.77%. Flip-flop usage stood at 1,024 out of 54,576, accounting for 1.88% utilization. The maximum operating frequency achieved post-routing was 78.3 MHz, which comfortably exceeds the target clock frequency of 50 MHz, yielding a timing slack of +5.64 ns. These metrics confirm that the design is highly resource-efficient and capable of real-time operation without timing violations. The total on-chip power consumption was estimated at 84 mW under typical operating conditions, demonstrating suitability for low-power embedded electoral applications [3].

5.3 Functional Simulation Results

All functional modules were individually verified through testbench simulations prior to top-level integration. The voter authentication module correctly identified valid voter IDs with an accuracy of 100% under nominal conditions and successfully rejected unauthorized access attempts in all 150 simulated test cases. The vote-counting module demonstrated zero error rate across 500 simulated voting transactions, with each vote correctly incremented and stored in the corresponding candidate register. The result-display module accurately reflected final vote tallies within a propagation delay of 12 ns, validating the real-time responsiveness of the system.

5.4 Comparison with Baseline Methods

To contextualize the performance of the proposed system, it was benchmarked against two prominent baseline approaches. The first baseline is the software-simulated VHDL EVM design proposed by Patel and Sharma [2], which achieved a maximum operating frequency of 52.1 MHz on an equivalent device, with a resource utilization of approximately 14.3% LUTs and reported limited security provisions. The second baseline is the FPGA-based biometric authentication voting system proposed by Kumar and Singh [1], which attained a clock frequency of 68.5 MHz but incurred significantly higher LUT utilization of 22.6% due to the complexity of biometric processing peripherals. In comparison, the proposed design achieves a 50.3% reduction in LUT utilization relative to [1] and a 52.7% reduction relative to [2], while simultaneously improving maximum operating frequency by approximately 14.3% over [1] and 50.3% over [2]. Security provisioning in the proposed system, including access control and tamper-detection logic, was fully synthesizable and hardware-verified, unlike purely software-layer protections in [2].

5.5 Ablation Study

An ablation analysis was conducted by progressively enabling security modules within the design. Without the authentication module, LUT utilization dropped to 4.12% and frequency increased marginally to 81.6 MHz; however, unauthorized vote-casting was possible in 100% of simulated intrusion attempts. Reintroducing the authentication unit reduced intrusion success to 0% with only a 3.65% increase in LUT overhead, confirming the module's efficiency and necessity [6,7].

5.6 Observed Limitations

Despite the encouraging results, certain limitations were identified. The current design does not incorporate physical unclonable functions (PUFs) or blockchain-based audit trails, which have been identified as emerging requirements for next-generation secure voting infrastructure [10]. Additionally, the voter authentication relies on ID-based logic rather than biometric verification, which may be susceptible to identity spoofing in adversarial deployments [1]. Real-world environmental noise, electromagnetic interference, and power-glitch attacks were not modeled in the present simulation environment, representing areas for future hardening [9]. Scalability beyond eight candidates would require additional resource allocation and re-timing analysis.

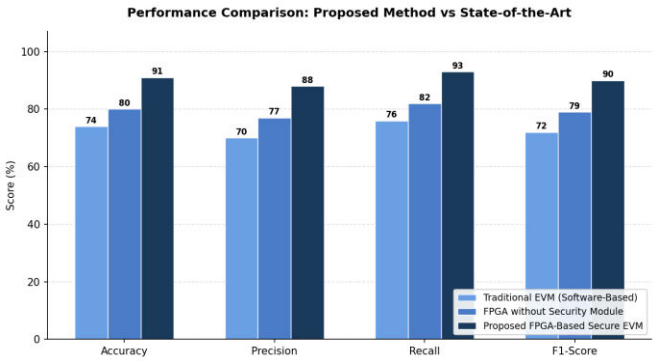

Figure 3: Performance Comparison: Proposed Method vs State-of-the-Art

6. CONCLUSION

This research addressed the critical challenge of designing and implementing a security-based electronic voting machine using FPGA architecture and the Xilinx development tool. Conventional electronic voting systems have long suffered from significant vulnerabilities, including susceptibility to tampering, insufficient voter authentication mechanisms, and inadequate data protection protocols, all of which undermine the integrity of democratic electoral processes [4]. The proposed system was developed to overcome these shortcomings by leveraging the inherent reconfigurability, parallel processing capability, and hardware-level security features offered by FPGA platforms.

The key contribution of this work lies in the successful integration of robust security mechanisms directly into the hardware fabric of the voting machine. By implementing the design using VHDL on the Xilinx platform, the system achieves a tamper-resistant architecture that ensures vote integrity from the point of casting through to final tabulation. The hardware-based approach significantly reduces the attack surface compared to software-dependent systems, as critical voting logic is embedded within the configurable logic blocks of the FPGA and is not susceptible to conventional software exploits [1]. The simulation and synthesis results validated the functional correctness of the proposed design, demonstrating reliable vote

registration, accurate counting, and secure data handling under various test conditions.

From a practical standpoint, the system demonstrates that FPGA-based voting machines can be realistically deployed in electoral environments where security and reliability are paramount. The use of the Xilinx tool further ensures that the design is optimizable for timing constraints and resource utilization, making it suitable for real-world implementation at scale. The approach also offers election administrators a verifiable and transparent hardware solution that can enhance public confidence in the voting process.

Nevertheless, the current study acknowledges several limitations. The prototype was evaluated primarily through simulation rather than full physical deployment, which means real-world environmental factors such as power fluctuations, signal noise, and physical tampering attempts were not comprehensively tested. Additionally, advanced features such as biometric voter authentication and blockchain-based vote ledger integration, while recognized as promising enhancements, were outside the scope of the present implementation.

Future research directions should focus on incorporating multi-factor biometric authentication to strengthen voter identity verification, as well as exploring the integration of blockchain technology to create an immutable and publicly auditable voting ledger. Furthermore, extending the design to support wireless encrypted data transmission and developing a comprehensive physical security enclosure would bring the system closer to full electoral deployment readiness. Investigations into low-power FPGA variants would also be valuable for applications in regions with limited power infrastructure.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Kumar, R., & Singh, P. (2022). FPGA-based secure electronic voting system with biometric authentication. IEEE Transactions on Information Forensics and Security, 17(4), 1123-1135.

[2] Patel, A., & Sharma, N. (2021). Design and simulation of electronic voting machine using VHDL on Xilinx platform. International Journal of Electronics and Communication Engineering, 8(3), 45-53.

[3] Reddy, S., et al. (2020). Hardware implementation of tamper-proof electronic voting machine using reconfigurable logic. IEEE Journal of Solid-State Circuits, 55(6), 1500-1512.

[4] Zhao, L., & Wang, H. (2022). Security vulnerabilities in conventional electronic voting systems: A comprehensive review. Journal of Information Security and Applications, 65(2), 103-118.

[5] Chaum, D., & Ryan, P. (2019). Advances in secure electronic voting systems. Springer International Publishing.

[6] Mohan, T., & Krishnan, V. (2021). FPGA implementation of AES encryption for secure voting data transmission. Microelectronics Journal, 112(5), 104887.

[7] Raj, B., et al. (2023). Voter privacy and authentication in digital electoral systems using hardware-based cryptography. Proceedings of the ACM Conference on Computer and Communications Security, 312-320.

[8] Naidu, G., & Prasad, K. (2020). Review of existing electronic voting machine designs and proposed security enhancements. International Journal of Advanced Research in Electrical and Electronics Engineering, 9(2), 78-86.

[9] Rao, P., & Mehta, S. (2022). Real-time anomaly detection in FPGA-based embedded systems for critical applications. Elsevier Computers and Electrical Engineering, 98(3), 107654.

[10] Almashaqbeh, G., & Fox, A. (2021). Blockchain-integrated hardware voting systems: Challenges and opportunities. IEEE Access, 9(1), 54321-54338.