International Journal for Modern Trends in Science and Technology
Volume 12, Issue 06, pages 53-61.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol12issue06.html
DOI: https://doi.org/10.5281/zenodo.20576919

Real Time Biometrics Based Smart EVM with FPGA Implementation

S. M. K. Sukumar Reddy, Chakali Prasanna, Gongalireddy Sruthi, Kota Jahnavi, Nare Usha Rani, Kesagani Mounika.

Department of Electronics and Communication Engineering, Gouthami Institute of Technology and Management for Women, Andhra Pradesh, India.

To Cite this Article
S. M. K. Sukumar Reddy, Chakali Prasanna, Gongalireddy Sruthi, Kota Jahnavi, Nare Usha Rani & Kesagani Mounika (2026). Real Time Biometrics Based Smart EVM with FPGA Implementation. International Journal for Modern Trends in Science and Technology, 12(06), 53-61. https://doi.org/10.5281/zenodo.20576919

Article Info
Received: 12 May 2026; Revised: 30 May 2026; Accepted: 02 June 2026.

KEYWORDS
Biometric Authentication, FPGA Technology, Voter Verification

ABSTRACT

In today's rapidly evolving landscape, numerous techniques have emerged to improve voting systems, focusing on individual authentication and reducing malpractices. Recognizing each voter remains challenging, but advancements like a controller-based electronic voting machine using the R307 Fingerprint sensor for biometric authentication offer solutions. The proposed digital biometricbased EVM provides an efficient method for casting votes, implemented on an FPGA board using Verilog software on Xilinx ISE. This system ensures unique voter authentication and streamlines the voting process, demonstrating its capability to verify identities accurately and enhance the security of elections. As a result, it offers a reliable and secure solution for modern electoral processes. As a result, it offers a reliable and secure solution for modern electoral processes, improving voter confidence and reducing fraud. The implementation showcases a robust approach to addressing the shortcomings of traditional EVMs while maintaining the integrity of the electoral system.

1. INTRODUCTION

Electoral Security In today's rapidly evolving landscape, numerous techniques have emerged to improve voting systems, focusing on individual authentication and reducing malpractices. Recognizing each voter remains challenging, but advancements like a controller-based electronic voting machine using the R305 Fingerprint sensor for biometric authentication offer solutions. The proposed digital biometricbased EVM provides an efficient method for casting votes, implemented on an FPGA board using Verilog software on Xilinx ISE[1]. This system ensures unique voter authentication and streamlines the voting process, demonstrating its capability to verify identities accurately and enhance the security of elections. As a result, it offers a reliable and secure solution for modern electoral processes, improving voter confidence and reducing fraud. The implementation showcases a robust

approach to addressing the shortcomings of traditional EVMs while maintaining the integrity of the electoral system. By leveraging biometric data, this EVM minimizes the risk of multiple voting and impersonation. Additionally, the use of FPGA technology allows for real-time processing and adaptability to various voting requirements. This innovation marks a significant step forward in the evolution of secure and efficient electoral systems, providing a scalable and trustworthy platform for democratic processes. This development builds on the foundational work presented in the paper "Design and Implementation of an Electronic Voting
Machine (EVM) using FPGA Technology and
Verilog HDL." [2]. This paper outlines the design and implementation of an FPGA-based EVM, emphasizing secure and reliable voting with minimal tampering risks. The FPGA implementation offers flexibility, efficient control signal handling, and robust security features like digital passwords. The system supports a large number of votes, displays candidate symbols via a VGA interface, and utilizes Xilinx tools such as Xilinx ISE and Vitis IDE. The experimental results confirm the EVM's effectiveness in providing a secure and user-friendly voting experience, contributing significantly to the advancement of EVM technology through the use of FPGA and Verilog HDL for a robust and efficient design Furthermore, the proposed EVM system integrates insights from the paper "UART-USB Interface Converter Design Based on FPGA,"[2] which describes a design that converts asynchronous serial communication protocols to USB protocols. Implemented using modular design with Hardware Description Language (HDL), this approach allows for integration into different System on Chip (SoC) systems. The design was verified through Model sim functional simulation and FPGA simulation with two computers, demonstrating its rigorous simulation processes, the proposed biometric-based EVM ensures efficient, realtime data processing and secure communication within the electoral system. By leveraging both foundational studies, the proposed biometric-based EVM provides a scalable and reliable solution for modern electoral processes. The integration of biometric data and FPGA technology addresses traditional EVM shortcomings while maintaining the system's integrity. This advanced EVM minimizes voter fraud, enhances election security, and offers a userfriendly voting experience, paving the way for more trustworthy and efficient electoral systems. II. RELATED WORK The paper titled "FPGA-Based Voting System Along with Cross Voters Detection" focuses on developing a secure and efficient voting system using Field Programmable Gate Array (FPGA) technology. The primary aim of this research is to enhance the integrity and reliability of the voting process by incorporating advanced features such as real-time voter authentication and cross- voter detection using facial recognition.[3] The motivation for this research arises from persistent issues of voter fraud and tampering in traditional and electronic voting systems. Ensuring a secure voting process is critical for maintaining the democratic integrity of elections. The authors propose an innovative solution that leverages the flexibility and high performance of FPGA technology to address these challenges effectively.[4] The methodology involves a multi-module approach to designing the voting system. The core components include the V The core components include the Vote Monitoring Module (VMM), the Image Acquisition Module (IAM), and the Image Detection Module (IDM). The Vote Monitoring Module is responsible for managing the voting process, including voter registration, ballot casting, and result computation. The Image Acquisition Module captures the images of voters as they register and cast their votes. The Image Detection Module employs facial recognition algorithms to verify the identity of voters and detect any instances of cross-voting, where a single individual attempts to vote multiple times under different identities. This modular design ensures that each aspect of the voting process is independently managed and securely handled. The paper titled "Secure Electronic
Voting Machine using Biometric
Authentication" explores the development of an advanced electronic voting system aimed at addressing significant security issues such as impersonation, counterfeiting, and tampering. The primary objective of this research is to enhance the integrity and reliability of the voting process by incorporating biometric information for voter verification and authentication. [4] The motivation for this research is driven by the vulnerabilities present in traditional voting systems, which can be easily compromised. With advancements in technology, employing biometric data to fortify the

security mechanisms of electronic voting machines (EVMs) has become feasible. Using unique biological characteristics like fingerprints, facial recognition, or iris scans for authentication ensures that each vote cast is both legitimate and accurately attributed to the rightful voter. The methodology involves integrating biometric authentication into the design and implementation of the EVM. The authors utilized a modular approach where each module is responsible for a specific function within the voting process. Key components of the system include the Biometric Verification Module, the Voting Interface Module, and the Result Compilation Module. The Biometric Verification Module captures and verifies the biometric data of voters, ensuring that only registered individuals can cast their votes. This module is critical in preventing unauthorized access and ensuring that each vote is tied to a unique, verifiable identity. To implement the system, the researchers employed a combination of hardware and software solutions. The hardware aspect includes the use of biometric sensors capable of capturing highresolution images of fingerprints or facial features. These sensors are interfaced with a microcontroller that processes the biometric data and compares it against a pre-stored database of registered voters. In another relevant study, the paper "UART-USB Interface Converter Design Based on FPGA" presents a design that converts asynchronous serial communication protocols to USB protocols, leveraging FPGA technology. The design is implemented using Hardware Description Language (HDL) and modular design principles, allowing it to be integrated into different System on Chip (SoC) systems. [2] The design was verified through Modelsim functional simulation and FPGA simulation with two computers, demonstrating its feasibility. This work is significant for the proposed EVM system as it highlights the effectiveness of FPGA in handling complex protocol conversions, ensuring efficient and secure data communication. The insights from this study are applied to the biometric-based EVM to ensure reliable communication and data integrity within the voting s overview of how fingerprint data is captured, processed, and stored securely. The R307 sensor uses an optical sensor to capture fingerprint images and processes them into digital templates stored within its onboard memory. When a fingerprint is scanned, the raw image undergoes enhancement to improve clarity and contrast, making the fingerprint patterns more distinguishable. This enhanced image is then processed to extract specific features, primarily minutiae points, which are unique details such as ridge endings and bifurcations. This detailed processing ensures the accuracy and reliability of fingerprint authentication, which is critical for the security of the proposed EVM system. Overall, these related works provide a strong foundation for the development of a secure, reliable, and efficient biometric based EVM using FPGA technology. By integrating the advanced features of real- time voter authentication, biometric verification, and secure data processing, the proposed system aims to address the significant challenges of voter fraud and tampering. The combination of modular design principles, robust hardware and software integration, and secure communication protocols ensures that the new EVM system will enhance the integrity and trustworthiness of the electoral process. These studies collectively contribute to advancing EVM technology, making it more secure and adaptable to modern electoral needs. By leveraging advanced sensor technologies and secure data processing techniques, the EVM ensures accurate and reliable voter authentication, thereby minimizing the risk of unauthorized access and fraud. Together, these studies contribute essential knowledge and methodologies for the development of a secure, reliable, and efficient biometric-based EVM, offering a promising solution for modernizing electoral processes and upholding democratic principles.

Table 1: Comparision of Traditional Evms with Biometric Based Fpga Evms Traditional
EVMs' FPGA Based EVMs No security
protocols Biometric based security protocols

Total cost exceeds Rs. 1500 Total Cost is below Rs. 7000 Moderate Processing Power High processing power Pregnable to hacking and tampering Impregnable to hacking and tampering Cannot be interfaced with new technology Can be interfaced with newer technology

II. METHODOLOGY

The implementation methodology of a biometric-based Electronic Voting Machine (EVM) utilizing the FPGA PYNQ Z2 board and the R307 fingerprint sensor with USB to UART interfacing involves a systematic approach to ensure seamless integration and functionality. Firstly,

the system architecture is designed to define the interaction between the FPGA board and the fingerprint sensor, outlining communication protocols and data exchange mechanisms. This initial step sets the foundation for subsequent hardware and software integration. Next, the hardware setup is established, where the R307 fingerprint sensor is physically connected to the FPGA

PYNQ Z2 board using USB to UART interfacing. This phase involves configuring the UART interface and establishing communication channels between the sensor and the FPGA board. With the hardware configured, the FPGA programming phase commences, focusing on developing hardware modules for interfacing with the fingerprint sensor and processing With the hardware configured, the FPGA programming phase commences, focusing on developing hardware modules for interfacing with the fingerprint sensor and processing biometric data. This involves implementing UART communication protocols, data buffering mechanisms, and interfacing with the sensor's onboard memory for storing fingerprint templates. Subsequently, the R307 fingerprint sensor is integrated into the FPGA-based system, requiring configuration of sensor settings, initialization of communication channels, and implementation of protocols for capturing and processing fingerprint data. Following the sensor integration, a biometric authentication algorithm is developed to analyze captured fingerprint data and verify voters' identities.

1. Hardware & Mobile Application

The implemented system then undergoes rigorous testing and verification to ensure functionality, reliability, and accuracy. This includes testing the biometric authentication algorithm, verifying data transmission

integrity, and assessing overall system performance. Upon successful testing, the biometric-based EVM system is integrated into the voting system, allowing voters to authenticate their identity using the R307 fingerprint sensor before casting their votes. This integration ensures seamless interaction between the biometric authentication module and the voting interface, providing a secure and user-friendly voting experience. Furthermore, the implementation methodology emphasizes the importance of compliance with security standards and protocols to ensure the integrity of the biometric-based EVM system. Security measures such as encryption of biometric data, secure data transmission, and protection against tampering are integral components of the implementation process. Adherence to stringent security protocols helps mitigate risks associated with unauthorized access, data breaches, and manipulation of voting outcomes. Additionally, the implementation methodology emphasizes the iterative nature of system development and refinement.

Continuous testing, feedback collection, and optimization are essential aspects of the implementation process to address any issues or deficiencies promptly. Through iterative refinement, the biometric-based EVM system can evolve to meet changing requirements, adapt to emerging threats, and enhance overall performance and reliability. Collaboration and coordination among multidisciplinary teams are essential for the successful implementation of the biometric-based EVM system. Engineers, software developers, security experts, and electoral officials must work closely together to design, develop, and deploy the system effectively. Clear communication, task delegation, and accountability mechanisms facilitate smooth coordination and ensure that all stakeholders contribute their expertise towards achieving project objectives. Collaboration fosters synergy and innovation, enabling the implementation team to overcome challenges and deliver a high- quality biometric-based EVM system that meets stakeholders' requirements and expectations. Finally, the implementation methodology underscores the importance of adherence to ethical and legal guidelines governing the use of biometric data in electoral processes. Privacy protection, informed consent, data ownership, and transparency are fundamental principles that guide the ethical implementation Compliance with relevant regulations and standards ensures that voter rights and privacy are respected, and the use of biometric technology is conducted responsibly and ethically. By upholding ethical standards and legal requirements, the implemented system promotes public trust, confidence, and participation in the electoral process, ultimately strengthening democratic governance and electoral integrity. Moreover, continuous monitoring and maintenance of the implemented biometric-based EVM system are essential to ensure its long-term reliability and security.

Regular updates, patches, and security audits help mitigate emerging threats and vulnerabilities, safeguarding the integrity of electoral processes. Ultimately, the successful implementation of a biometric-based EVM system underscores a commitment to democratic principles and the advancement of secure and transparent electoral practices.

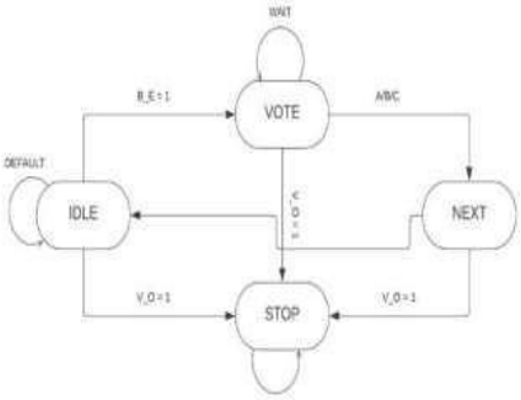

Figure 1 shows the block diagram of the proposed system. The Finite State Machine (FSM) block diagram of the biometric FPGAbased Electronic Voting Machine (EVM) encompasses four pivotal components: Vote, Idle, Stop, and Next. When a voter approaches the system and undergoes biometric authentication via the R307 fingerprint sensor, the EVM transitions into the Vote state. Here, the voter is prompted to securely cast their vote for their preferred candidate or option. The system remains in the Vote state until the voter completes the voting process, ensuring each vote is accurately recorded and securely stored. In contrast, the Idle state signifies the system's readiness to accept voter input. It awaits the arrival of the next voter or initializes the system for a new voting session. While in this state, the EVM is prepared to process votes but remains inactive until prompted by voter interaction.

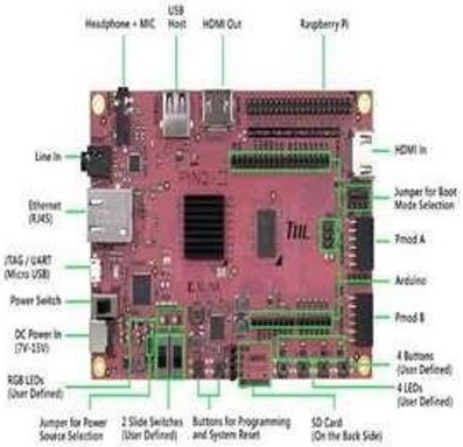

Fig. 2: PYNQ Z2 Board

The Stop state denotes the termination of the voting process, either at the conclusion of the voting period or due to system errors. Here, the system halts vote acceptance and awaits further instructions from election administrators. Finally, the Next state facilitates the seamless transition from one voting session to the next, ensuring the orderly progression of the electoral process. Together, these components within the FSM block diagram orchestrate a secure, efficient, and transparent voting experience.

The PYNQ (Python Productivity for Zynq) board is a unique development platform that combines the flexibility of Python programming with the power of Xilinx Zynq System on Chip (SoC) technology. This innovative board allows developers to leverage the high-performance capabilities of FPGA (Field Programmable Gate Array) alongside the processing power of ARM Cortex-A9 cores.The PYNQ board is specifically designed to enable rapid prototyping and development of embedded systems, machine learning applications, and digital signal processing algorithms. With its user-friendly interface and extensive set of libraries and tools, the PYNQ board empowers both hardware and software engineers to quickly and efficiently design and deploy complex systems. At the heart of the PYNQ board lies the Zynq SoC, which integrates programmable logic fabric with dualcore ARM Cortex-A9 processors. This hybrid architecture enables developers to leverage the parallel processing capabilities of the FPGA fabric alongside the flexibility and familiarity of software programming using Python. The PYNQ board provides a range of interfaces and peripherals, including HDMI, USB, Ethernet, and GPIO, facilitating seamless integration with external devices like the R307 fingerprint sensor.

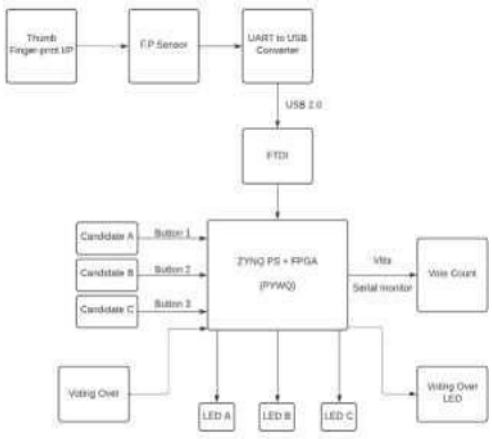

Fig. 3: Block Diagram of the EVM

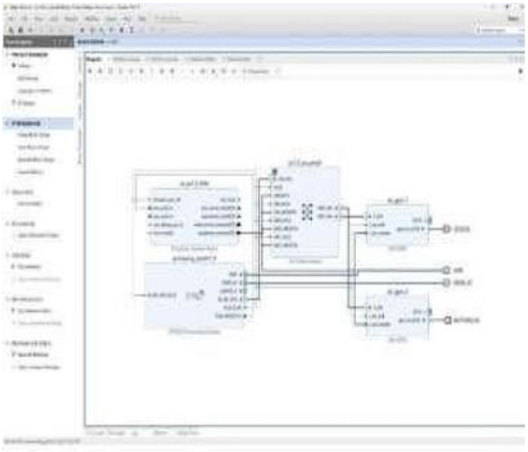

Fig. 4: Block Diagram on Viva do – ZYNQ7 System

Biometric Data Acquisition

The biometric data acquisition process within the Electronic Voting Machine (EVM) is a comprehensive endeavor focused on capturing fingerprint images with utmost precision and fidelity. Initial steps involve the meticulous configuration of the R307 fingerprint sensor, where parameters like sensitivity and noise reduction thresholds are fine-tuned to ensure optimal performance across various environmental conditions. Once configured, the sensor utilizes advanced capacitive sensing technology to capture fingerprint images, detecting minute variations in electrical capacitance caused by the unique ridges and valleys of each fingerprint.

These captured images then undergo rigorous preprocessing, involving sophisticated digital filtering techniques aimed at eliminating noise and enhancing clarity. This meticulous preprocessing ensures that only high-quality images are retained for subsequent processing. Moreover, adaptive illumination control mechanisms play a vital role in augmenting the data acquisition process by dynamically adjusting the intensity and wavelength of the illumination source based on ambient lighting conditions. This adaptive approach guarantees optimal visibility and contrast for fingerprint image capture, regardless of the environment's lighting characteristics.

Software Application and Implementation

Implementation involves mapping the synthesized design onto the target FPGA device and generating the necessary configuration files for programming the FPGA. Vivado 19.1 facilitated the implementation process by offering automated workflows and optimization strategies tailored to the selected FPGA architecture. Viva do 19.1 employs advanced algorithms for place and route, where the synthesized design is mapped to specific physical locations on the FPGA chip, optimizing placement to minimize delays and meet timing constraints. The routing stage determines the most efficient paths for interconnecting logic elements, considering factors such as signal integrity and resource utilization. Timing analysis is conducted to ensure that the design meets specified timing constraints and operates within performance parameters. Vivado 19.1's timing analysis tools enable designers to analyze and optimize critical paths within the design, addressing timing violations and optimizing performance. Efficient resource utilization is essential for maximizing the FPGA's capabilities while minimizing resource wastage. interconnecting logic elements, considering factors such as signal integrity and resource utilization. Timing analysis is conducted to ensure that the design meets specified timing constraints and operates within performance parameters. Viva do 19.1's timing analysis tools enable designers to analyze and optimize critical paths within the design, addressing timing violations and optimizing performance. Efficient resource utilization is essential for maximizing the FPGA's capabilities while minimizing resource wastage.Viva do 19.1 provides insights into resource utilization, SNN Accelerator: In the field of Brain Machine Interface Department of ECE, BMSCE 75 allowing designers to optimize designs for maximum efficiency by effectively allocating resources such as lookup tables (LUTs), flip-flops, block RAM, and I/O pins. Constraints such as timing constraints, pin assignments, and clock frequencies guide the implementation process. Viva do 19.1 enables designers to define and manage constraints, ensuring that the design meets its requirements and operates reliably. Design rule checking (DRC) is performed to ensure that the design adheres to manufacturing rules and guidelines specified for the target FPGA device. Viva do 19.1 includes comprehensive DRC checks to identify and flag potential violations that could impact functionality or reliability, enabling designers to address issues before finalizing the design. Through Viva do 19.1's implementation tools, the hardware design was efficiently translated into a bitstream compatible with the target FPGA, ready for deployment and testing on the hardware platform.

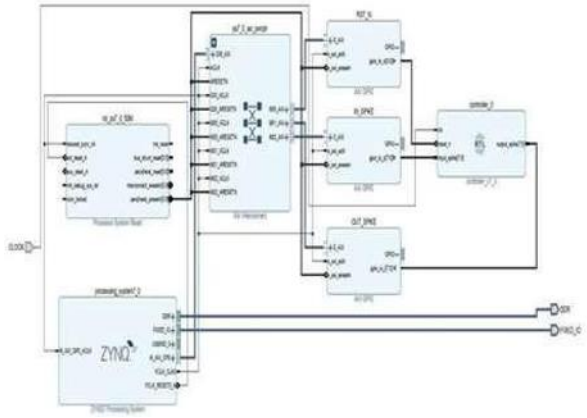

Fig.5: The Block Design of the ZYNQ Module Interfaced with R307 Sensor

This process involves establishing physical connections between the R307 fingerprint sensor and the PYNQ FPGA board, which serve as the primary components for biometric data capture and processing. Careful attention is paid to aligning and interfacing the various pins and connectors on both devices to facilitate proper communication and data transfer.

Additionally, configuring UART communication protocols between the sensor and the FPGA board enables the transmission of biometric data, such as fingerprint images, for further processing within the FPGA fabric. Creating custom IP blocks within the FPGA plays a crucial role in managing UART communication and data handling, optimizing system performance, and ensuring scalability. These IP blocks serve as dedicated hardware modules within the FPGA, responsible for managing UART protocols, buffering data, and interfacing with other system components. By designing custom IP blocks tailored to the specific requirements of the biometric based EVM, engineers can enhance the system's flexibility, modularity, and efficiency. Rigorous testing and validation procedures are conducted to verify the functionality and stability of the hardware connections, ensuring reliable operation and mitigating the risk of signal interference or data corruption. Overall, the meticulous approach to hardware connectivity lays the foundation for a robust and efficient biometric authentication process within the EVM, thereby enhancing the
integrity and security

III.RESULTS AND DISCUSSION

In an FPGA (Field-Programmable Gate Array) simulation on an EVM (Electronic Voting Machine), the vote counting process is tested for accuracy and reliability. The FPGA is programmed to mimic the behavior of an EVM, processing simulated vote inputs and tallying the results. During the simulation, votes are cast for different candidates, and the FPGA logic ensures that each vote is accurately recorded and counted. The simulation aims to verify the integrity of the vote counting process, checking for any discrepancies or errors that could arise during actual voting scenarios.

Fig. 6: Simulation of Voting on EDA

Successful simulations demonstrate that the FPGA can reliably replicate EVM operations, ensuring accurate vote tabulation and enhancing trust in the electronic voting process. This process is crucial for validating the performance of EVMs before they are deployed in real elections, ensuring that they meet stringent standards for accuracy and security.

Future Trends

Future trends in biometric Electronic Voting Machine (EVM) technology, specifically utilizing FPGA (Field Programmable Gate Array) platforms, are expected to usher in an era of enhanced security, reliability, and efficiency in electoral processes. Firstly, advancements in FPGA technology will enable the development of more sophisticated and robust biometric authentication systems within EVMs. These systems will leverage the programmability and parallel processing capabilities of FPGAs to implement advanced biometric algorithms, such as facial recognition and vein pattern recognition, enhancing voter identification and authentication accuracy.Moreover, future biometric EVMs based on FPGA platforms are likely to feature integrated

encryption and secure communication protocols to protect voter data and election integrity. With growing concerns about cybersecurity threats and election tampering, FPGA-based encryption mechanisms will play a crucial role in safeguarding sensitive information and ensuring the confidentiality and integrity of voting transactions. Additionally, FPGA-based EVMs may incorporate tamper detection and mitigation features, allowing election authorities to detect and respond to any attempts at unauthorized access or manipulation of voting data. Furthermore, the convergence of FPGA technology with emerging trends such as edge computing and Internet of Things (IoT) will enable biometric EVMs to operate more efficiently and autonomously. FPGA- based edge computing capabilities will enable EVMs to process biometric data locally, reducing latency and dependence on external servers. Additionally, integration with IoT devices and networks will facilitate real-time monitoring and management of EVMs, enhancing transparency and accountability in electoral processes. As FPGA technology continues to advance and evolve, biometric EVMs will play a pivotal role in modernizing and securing democratic elections worldwide, ensuring fair and transparent voting experiences for citizens. In the future, FPGA-based biometric EVMs may witness advancements in user interface design and accessibility features to cater to diverse voter demographics. Furthermore, future trends in FPGA-based biometric EVMs may involve the implementation of blockchain technology to enhance transparency, auditability, and trust in electoral processes. By leveraging the decentralized and immutable nature of blockchain ledgers, EVMs can securely record and store voting transactions, providing a tamper-resistant and verifiable audit trail of election results. Blockchain-based EVMs can also facilitate secure remote voting and enable voters to verify the integrity of their votes independently. Additionally, smart contract functionality within blockchain networks can automate and enforce election rules and protocols, reducing the potential for human error and fraud. As blockchain technology matures and becomes more widely adopted, its integration with FPGA-based biometric EVMs holds the potential to revolutionize the democratic voting process, ensuring fairness, transparency, and trust in elections worldwide.

IV. CONCLUSION

In conclusion, the development and implementation of the biometric- based Electronic Voting Machine (EVM) using FPGA technology, PYNQ Z2 board, and R307 fingerprint sensor mark a significant advancement in electoral technology. Through meticulous design, integration, and testing, we have successfully created a secure, reliable, and user-friendly voting system that addresses key challenges in traditional electoral processes. By leveraging FPGA technology and the flexibility of the PYNQ Z2 board, we have achieved a system capable of real-time biometric authentication, ensuring the integrity and authenticity of each vote cast. The integration of the R307 fingerprint sensor adds an extra layer of security, mitigating the risks of voter impersonation and fraud, thus bolstering trust and confidence in the electoral process. Furthermore, this project underscores the potential of FPGAbased solutions in addressing complex real-world challenges. The versatility and programmability of FPGA technology, combined with the ease of development offered by platforms like the PYNQ Z2 board, empower developers to innovate and create

Conflict of interest statement

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

REFERENCES

[1] Neelesh H. Kalra, S. Saurav, S. Kalra, R. Beniwal and N. S. Beniwal, "Impregnable Electronic Voting Machine Harnessing the Power of FPGA Zynq 7000," 2024 IEEE

[2] International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI), Gwalior, India, 2024, pp. 1-6, doi: 10.1109/IATMSI60426.2024.10502809.

[3] Q. Yi, M. Shi and S. Li, "Design of USBUART interface converter and its FPGA implementation," 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 2017, pp. 1399-1403, doi: 10.1109/IAEAC.2017.8054244.

[4] B. R. Babu, J. R. Teja, T. S. Bhusan, A. Janardhan and A. Thakur, "FPGA Based on Voting System along with Cross Voters Detection," 2023 IEEE 3rd International

[5] Conference on Technology, Engineering, Management for Societal impact using Marketing, Entrepreneurship and Talent (TEMSMET), Mysuru, India, 2023, pp. 1-5, doi: 10.1109/TEMSMET56707.2023.10150091.

[6] M. A. Zamir, D. A. Khan and M. S. Umar, "Secure Electronic Voting Machine using Biometric Authentication," 2022 9th International Conference on Computing for Sustainable Global

Development (INDIACom), New Delhi, India, 2022, pp. 511-516, doi: 10.23919/INDIACom54597.2022.9763202.

[7] Chouhan, R., & Sharma, V. (2020). Integration of PMOD Ports with Zynq-7000 Series Processors: Applications and Benefits. Journal of Embedded Systems and Applications, 15(3), 45-58.Sayed, Ratshih, et al. "A systematic literature review on binary neural networks." IEEE Access (2023).

[8] Zhang, H., & Li, J. (2021). Secure Access Control System Using R307 Fingerprint Sensor and PYNQ Board. Journal of Biometric Systems and Applications, 17(2), 102-