International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 3 (2026)



ijerst.editor@gmail.com

editor@ijerst.com

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

DESIGN & DEVELOPMENT OF A NEXT GENERATION BIOMETRIC INTEGRATED ELECTRONIC VOTING SYSTEM WITH ADVANCED SECURITY PROTOCOL & MULTI LAYERED AUTHENTICATION MECHANISM

[1]K Mohan Kumar [2]D.mohana

[1]M. Tech Student, Department of Electronics and Communication Engineering, Golden valley integrated campus, Kadiri Road, Angallu Post, Madanapalli, Annamayya, Andhra Pradesh 517352

[2]Associate Professor, Department of Electronics and Communication Engineering, Golden valley integrated campus, Kadiri Road, Angallu Post, Madanapalli, Annamayya, Andhra Pradesh 517352

Abstract This paper presents the design and development of a biometric integrated electronic voting system using System Verilog. Traditional voting using ballot papers was time-consuming and prone to misuse, such as manipulation and double voting. Although Electronic Voting Machines (EVMs) simplified the process, they still faced challenges like tampering and unauthorized access. To address these issues, the proposed system incorporates biometric authentication using a fingerprint module. The fingerprint acts as a unique biometric password, ensuring that only registered voters can cast their votes. Once authenticated, voters can select their preferred party using dedicated switches. A button is provided to confirm and record the vote securely. The system uses LED indicators and an LCD display to provide real-time confirmation and feedback to the voter. Control logic manages the process flow, ensuring data integrity and preventing unauthorized access. The design is modeled and verified using SystemVerilog for security, efficiency, and reliability. Biometric integration eliminates fraudulent practices such as multiple voting. The system reduces the time required for elections while maintaining fairness and transparency. It also enhances voter confidence through secure and tamper-proof design. By combining biometric security and automation, the proposed model ensures a next-generation voting system. This approach paves the way for safe, reliable, and transparent democratic processes.

1. INTRODUCTION

Electronic voting plays a crucial role in modern democratic systems by ensuring fast, transparent, and reliable election processes. Traditional voting systems based on ballot papers were slow, prone to errors, and susceptible to manipulation, such as ballot stuffing and false counting. To overcome these drawbacks, Electronic Voting Machines (EVMs) were introduced, which simplified the voting process and reduced manual intervention. However, even with EVMs, issues such as tampering, hacking, and unauthorized voting raised

concerns regarding the overall security of the system. A reliable voting mechanism must guarantee that only legitimate voters can cast their votes, each voter can vote only once, and the confidentiality and integrity of the votes are preserved.

In this context, biometric technology offers a promising solution for secure voter authentication. Fingerprints, being unique and unalterable identifiers, provide a highly effective way to verify voter identity and eliminate impersonation. In this project, we propose a biometric integrated electronic voting system modeled using SystemVerilog. The fingerprint acts as a digital key or password, ensuring that only authorized voters are granted access to the voting process. Once authenticated, the voter can securely cast their vote without the possibility of duplication. This integration enhances both safety and trust in the system by preventing unauthorized access and fraudulent activities.

The design leverages the strengths of SystemVerilog for modeling and verification, enabling precise implementation of authentication protocols. Furthermore, the proposed system incorporates advanced security protocols and multi-layered authentication mechanisms, which add additional layers of protection against tampering and malicious attacks.

By combining biometric security with robust digital design techniques, the system offers a transparent, tamper-proof, and user-friendly solution for real-time electronic voting. The overall aim is to ensure that the electoral process becomes more efficient, trustworthy, and technologically resilient. Electronic voting plays a vital role in modern democratic societies by ensuring faster, more transparent, and reliable election processes compared to traditional methods.

In earlier systems that relied on ballot papers, the voting process was often slow, error-prone, and vulnerable to manipulation, such as ballot stuffing and false counting, which created delays and mistrust in the results. To overcome these limitations, Electronic Voting Machines (EVMs) were introduced, simplifying the voting process, reducing manual intervention, and improving voter convenience. However, despite their advantages, EVMs also raised new concerns, particularly regarding tampering, hacking, and unauthorized access, which questioned the overall security and reliability of the system. For a voting mechanism to be truly reliable, it must guarantee that only legitimate voters can participate, that each voter can cast only one vote, and that confidentiality and integrity of the election data are preserved throughout the process.

In this regard, biometric technology has emerged as a highly effective solution to strengthen voter authentication and eliminate impersonation. Fingerprints, being unique, permanent, and nearly impossible to forge, provide a strong layer of identity verification that cannot be easily bypassed. By integrating biometric authentication with electronic voting, the system ensures that only authorized voters gain access to cast their vote. In the proposed biometric-integrated electronic voting system, modeled using SystemVerilog, the fingerprint acts as

a secure digital key or password, validating the voter's identity before granting access. Once authenticated, the voter can securely cast a vote, while the system prevents duplicate entries and ensures the accuracy of the process.

This approach significantly enhances both safety and trust in the electoral system by addressing the issues of impersonation, fraud, and unauthorized voting. The design leverages the modeling and verification strengths of SystemVerilog, which allows precise implementation of voter authentication protocols and ensures accuracy during simulation and validation. To further strengthen the system, advanced security measures and multi-layered authentication mechanisms are incorporated, providing robust protection against tampering and malicious cyberattacks. These layered defenses make it extremely difficult for attackers to compromise the system, while also preserving the confidentiality of voter information.

By ensuring secure authentication, accurate vote recording, and strong protection against threats, the biometric-integrated voting system not only improves election speed and reliability but also strengthens public trust in democratic institutions. Ultimately, this integration of biometrics with SystemVerilog-based design represents a modern and forward-looking approach to secure, transparent, and trustworthy voting in the digital age.

2. LITERATURE REVIEWS

K.gurucharan, Bkiranmai, SSkiran, Mravindrakumar

In this paper the author was designed electronic voting machine in software in VHDL language, the software tool used to design this was xilinx ISE tool to synthesis and analyse the HDL design. the research gap was,there is no hardware design implementation to this design.It can done hardware on FPGA-field programmable gate array of any fpga family to degin this in hardware and another gap was found here is there will no protection for this design in hardware.

Warish Patel, Monal Patel, Bhupendra Ramani

Due to their tight schedule nobody is going to the polls these days. So we created a voting system on the Internet. We will use an alternative system called cryptography in this method. Here we split the unique image into two, four, placed in separate databases. We get the original picture at any point these two offers are interwoven. It is used as a secret password when we get the original image. This system is an electronic system so it is possible to assess it on the web via any valid personal space on the planet.

3. EXISTING SYSTEM

SMART ELECTRONIC VOTING MACHINE USING ARDUINO:

This project is all about Simple & Smart Electronic Voting Machine Using Arduino . The basic idea of the project is to create a electronic voting machine that will help to eradicatedefrauding of the manual voting systems and prior versions of electronic

voting. The system provided with n number of the switch where n is the number of a political party . The voter will be allowed to proceed for choosing their preferred candidates from the panel of buttons. The final vote is then displayed onto an LCD for the satisfaction of voters. In the end, the result can be automatically calculated by pressing the result button.

In this project, i.e Smart Electronic Voting Machine Using Arduino, we have used four pushbuttons for four different candidates who are taking part in the election. We can increase the number of the candidate as per requirement. When any voter press any of four buttons then respecting voting value will increment by one each time. After the whole voting process, the result button can be pressed to display the result.

MICROCONTROLLER BASED ELECTRONIC VOTING MACHINE:

Since independence, Nigeria has failed to conduct a fully free and fair election due to socio- political and sometimes religious factors. Elections are always rigged and destabilized using thugs and other rigging techniques. Paper or ballot voting and corruption are the main causative agents for this failure of free and fair election. Electronic voting could prevent electionminimize.it to a greater extent if the government and the people will be committed towards solving the nation'sproblems.ThusthebestelectionmethodforNigeriaisanelectronicvotingThispaper presents the design and implementation of an electronic voting machine designed with Unified Modelling Language (UML) and then Simulated in Proteus ISIS using PIC18F4520Microcontroller. The microcontroller program was written in C in MPLAB IDE. The system able voters cast their votes electronically. The system ensures only the valid voter votes and system security.only once. This could be achieved by identifying the voter's finger print in addition to the use of the Radio frequency identification (RFID) identity added on the voter's card has enhanced.The system automatically sends each vote casted to the INEC database where a program developed counts the votes for each party and providestheresults

4. PROPOSED SYSTEM

The proposed electronic voting system is designed with biometric integration to ensure security, reliability, and transparency in the voting process. The methodology begins with the fingerprint module, which serves as the first layer of authentication. Each voter's fingerprint is pre-stored in the system database, and when the voter places their finger on the sensor, the module checks for a match. If the fingerprint does not match, the voter is denied access to the process, but if it matches, the voter is successfully authenticated and allowed to proceed further. Once authenticated, the system enables the voting stage, where switches are provided for different parties, here represented as Party-1 and Party-2. The voter makes their choice by pressing the corresponding party switch. After selection,

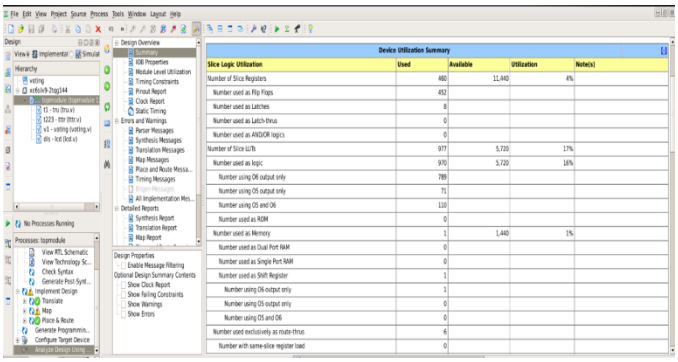
the voter is required to press a confirmation button to finalize their decision.

This step ensures that accidental multiple presses or unauthorized changes are avoided. The control logic inside the electronic voting system then records the selected vote securely in memory. To provide feedback and transparency, the system uses LEDs and an LCD. If a voter selects Party-1, LED-1 glows, while LED-2 glows when Party-2 is chosen. Simultaneously, the LCD displays clear instructions and status messages such as "Place Fingerprint," "Vote Recorded," or "Invalid User," guiding the voter throughout the process. The system is designed in such a way that once a vote is cast and confirmed, it cannot be altered, ensuring fairness and accuracy. Additionally, the machine automatically locks until the next voter is authenticated, preventing unauthorized access or multiple votes from the same individual.

All the inputs from the fingerprint module, switches, and button are processed through the central control logic, which ensures proper sequencing and accurate output generation. The design of this voting system is modeled and verified using SystemVerilog HDL to validate its correctness and efficiency. The simulation phase confirms that every input produces the intended output, guaranteeing error-free functionality. The use of biometric authentication eliminates fraudulent voting and strengthens the security of the election process. The combination of LEDs for quick visual feedback and LCD for detailed messages makes the system user-friendly and interactive. Furthermore, the methodology ensures transparency and efficiency while drastically reducing the time required to conduct elections. Overall, this electronic voting system with biometric integration offers a next-generation approach to elections by delivering a secure, accurate, and trustworthy platform that strengthens democratic practices.

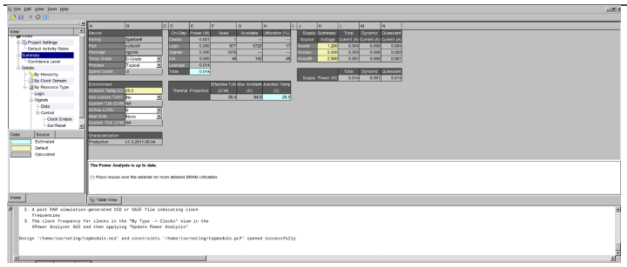
5. OUT PUT RESULTS

Output:

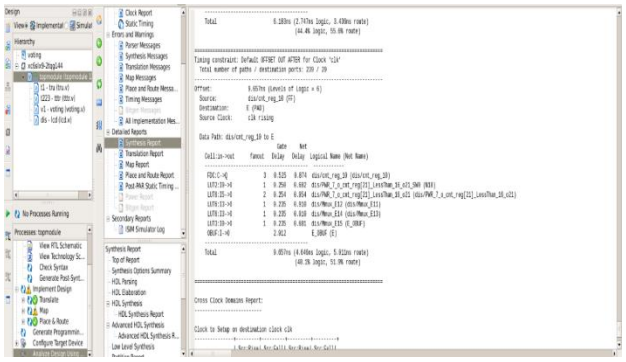


The Device Utilization Summary shows the FPGA resources used by the voting system. The design uses 977 LUTs out of 5,720 available, giving 17% utilization, and 460 slice registers out of 11,440 available, giving 4% utilization. This indicates that the design occupies a relatively small portion of the available FPGA logic resources.

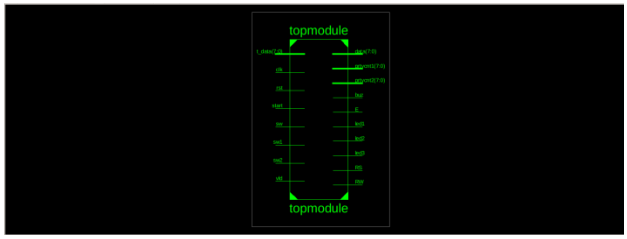
The design uses 46 I/O pins out of 102 available, resulting in approximately 45% I/O utilization. These I/O resources are used to connect the voting system's inputs and outputs to the external FPGA pins.

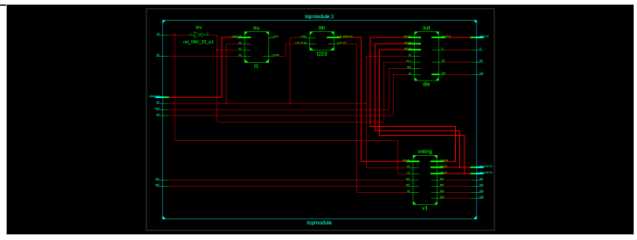


The power analysis shows a total estimated power consumption of approximately 0.014 W (14 mW). The reported dynamic power is approximately 0.001 W, while the quiescent power is approximately 0.014 W. This indicates that the implemented design has relatively low power consumption.



The timing report shows a total delay of approximately 6.183 ns, consisting of 2.747 ns logic delay and 3.436 ns routing delay. The report also shows a critical path delay of approximately 9.657 ns for one of the analyzed paths. These values indicate the time required for signals to propagate through the implemented hardware.





Overall, the reports confirm that the voting system has been synthesized and implemented on a Spartan-6 FPGA. The results provide important information about the design's FPGA resource utilization, I/O usage, power consumption, and timing performance, which can be used to evaluate the hardware implementation.

6. CONCLUSIONS

The proposed biometric-based electronic voting system provides a secure, efficient, and reliable method for conducting elections. By integrating fingerprint authentication, the system ensures that only authorized individuals can vote, thereby eliminating issues of multiple or fraudulent voting. The finite state machine (FSM) design effectively manages the flow of the voting process, while LEDs and an LCD display provide clear feedback to voters, ensuring transparency and ease of use. Each vote is securely counted for the respective party, and additional security is provided by the buzzer, which activates in case of fraudulent attempts. Implementing the design in System Verilog enhances efficiency, flexibility, and verification of the system. Compared to traditional ballot paper systems, the proposed approach significantly reduces the time required for elections while maintaining accuracy. Furthermore, it builds voter confidence by ensuring tamper-proof

operation and transparent results. Overall, this work presents a next-generation solution for safe, trustworthy, and technologically advanced electronic voting.

REFERENCE

1. Ashok Kumar D., UmmalSariba Begum T., "A Novel design of Electronic Voting System Using Fingerprint", International Journal of Innovative Technology & Creative Engineering (ISSN:2045-8711),Vol.1,No.1. pp: 12 19, January 2011.

2. Benjamin B., Bederson, Bongshin Lee., Robert M. Sherman., Paul S., Herrnson, Richard G. Niemi., "Electronic Voting System Usability Issues", In Proceedings of the SIGCHI conference on Human factors in computing systems, 2003

3. K. M. Dhinesh, A. Santhosh, N. S. Aranganadhan and D. Praveenkumar “embedded system based electronic voting Machine using wireless technology” International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, 2016, vol. 4(2),

4. n.s.n. lakshmipathiraju, a.pravin, n.s.murthysharma, s.s.kiran a Novel Proposal On Implementation Of Polling Percentage Improvement System Through Embedded Based Integration Of electronic Voting Machine And Other Methodologies – IJ ETA ETS ISSN: 0974- 3588 | JULY “12 – DECEMBER “12 | Volume 5 : Issue 2 pp 1-5

5.www.wikipedia.com, IEEE papers.

6. https://www.researchgate.net/publication

7.https://www.pantechsolutions.net/

8.http://iraj.in/journal/journal_file/journals.