Design and Implementation of a Secure Voting Machine Using De-10 Nano FPGA withVerilog

Sudheer Reddy, Tejeswararao Padda, Manoj Bande, Jahnavi Mandala, Naga Praveen Kandula

Abstract

This paper presents the design, implementation, and testing of a secure voting machine system utilizing the DE-10 Nano FPGA and Verilog programming. The system integrates an LCD for displaying results, a fingerprint sensor for voter authentication, and external push buttons for vote casting. The system was tested with 5 party candidates and 4,000 participants, demonstrating its capability to accurately count votes, display individual vote counts, and declare the winner. The voting process is controlled through an admin code, push buttons, and slide switches for mode operations. Additionally, the system calculates the total poll percentage, adding another layer of insight into voter turnout. Voter data, including fingerprints, were securely stored on an Azure Cloud platform, with the total information including all 10 fingerprints of each voter and their detailed voter information. The paper includes result images of the front-end website page and Azure cloud storage page, as well as simulation results, RTL block diagrams, related tables, and FPGA prototyping images, highlighting the system's efficacyand potential for real-world applications.

Index Terms— *Voting Machine, FPGA Prototyping, Verilog, Fingerprint Authentication, UART Protocol, Cloud Storage, Secure Voting*

1 Introduction

1.1 Background

In modern democracies, secure and reliable voting systems are essential. Traditional voting methods are prone to various risks, including fraud and miscounting [1, 5]. To address these concerns, electronic voting systems have been introduced. However, many existing electronic voting systems still lack the robust security measures required to fully ensure the integrity of the voting process. This paper introduces a secure voting machine designed using the DE-10 Nano FPGA, programmed with Verilog,which aims to mitigate these challenges.

1.2 Problem Statement

Existing electronic voting systems often lack robust security measures, making them vulnerable to tampering [7, 13]. This research aims to develop a system that ensures secure, accurate, and efficient voting, with enhanced security through biometric authentication [2, 8] and cloud storage [14, 20].

1.3 Objectives

The primary objectives of this research are:

1. To design and implement a secure voting machine using the DE-10 Nano FPGA [5, 10].

2. To integrate biometric authentication for voter verification [2, 8].

3. To utilize cloud storage for secure data handling and real-time vote counting [14, 20].

4. To provide a scalable solution that accommodates multiple candidates [11, 17].

1.4 Contribution

This paper presents a novel approach to secure voting by combining FPGA-based hardware with cloud- based data storage and multi-factor voter authentication [6, 9]. The system integrates an LCD for real- time results display, a fingerprint sensor for biometric verification [3, 4], and a robust cloud storage solution for data integrity [14, 20]. The use of the DE-10 Nano FPGA allows for a highly flexible and customizable voting machine design [5, 10], while the cloud storage ensures secure and accessible data management [14, 20].

2 System Design

2.1 Hardware Architecture

The hardware design of the voting machine is based on the DE10-Nano FPGA development board, featuring a Cyclone V SoC FPGA [5, 7]. Key components include an LCD module, fingerprint sensor, push buttons, and slide switches. The block diagram of the system illustrates the interaction between these components and their connection to the FPGA [5, 6, 17].

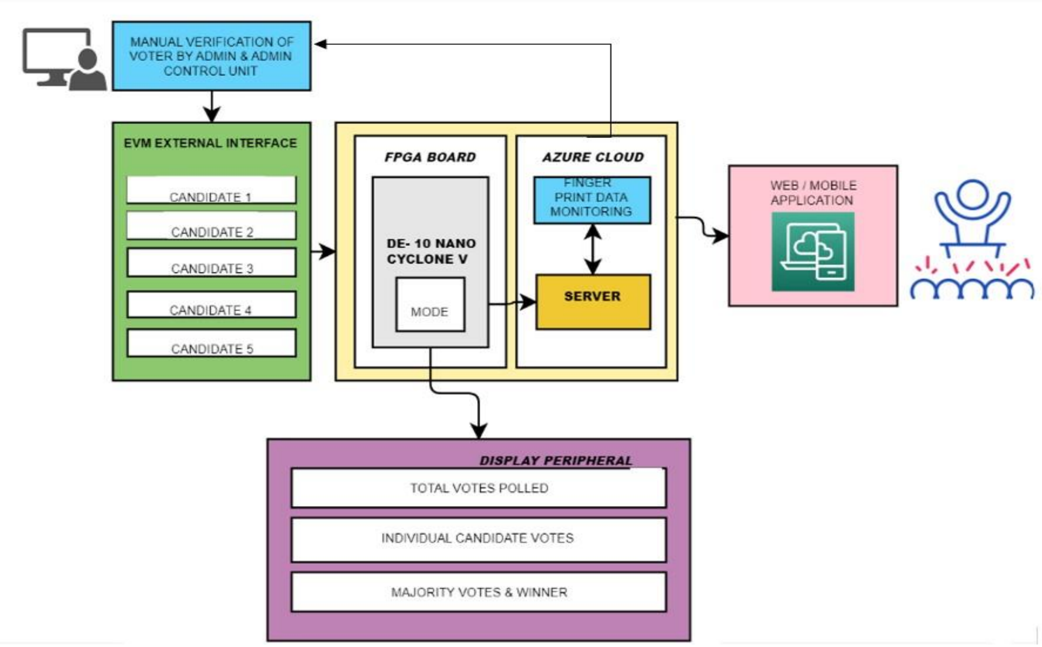


Figure 1: Block Diagram of the System

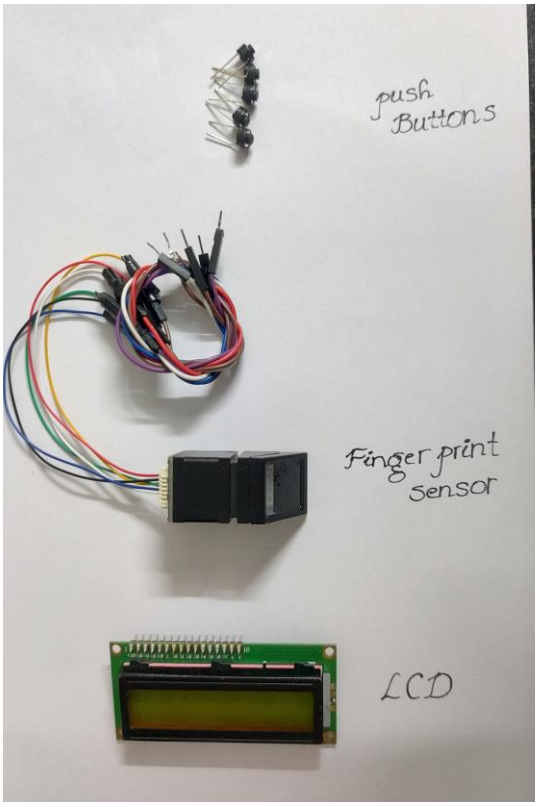


Figure 2: Overview of all peripherals connected to the DE10-Nano FPGA

2.2 Finite State Machine (FSM) Design

The voting machine's operation is governed by a Finite State Machine (FSM) implemented in Verilog [10, 13]. The FSM transitions between the following states:

- **Idle State:** The system remains inactive until voting is initiated. The LCD is off to conservepower.
- **Voting Open State:** Once voting is activated, the LCD displays the number of votes as they are cast. Each push button press increments the vote count for the respective candidate [11, 17].
- **Voting Close State:** At the end of the voting period, the LCD shows the total number of votescast.
- **Display State:** The LCD displays each candidate's total vote count and highlights the winner based on the highest vote count [5, 12].

2.3 LCD Integration

The LCD provides real-time feedback throughout the voting process and is integrated with the FSM:

- **Idle State:** LCD is off.
- **Voting Open State:** Displays the real-time vote count for each candidate [17].
- **Voting Close State:** Shows the total number of votes cast.

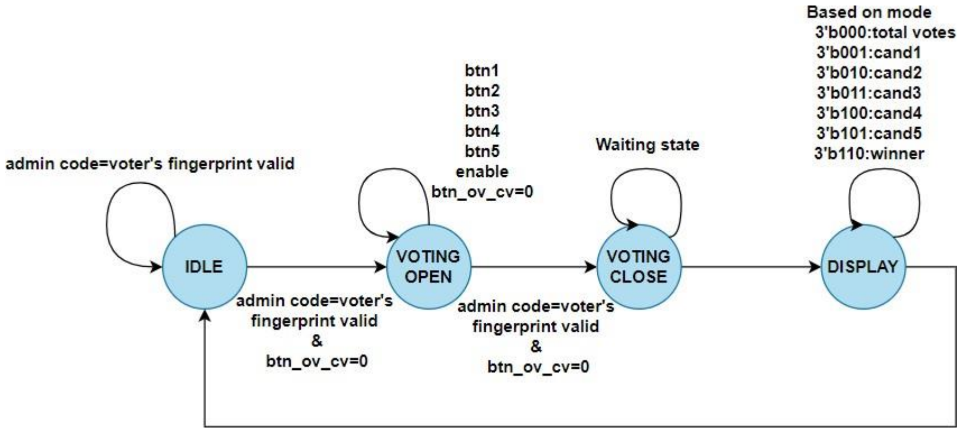
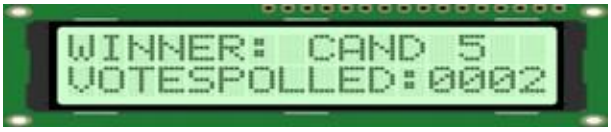


Figure 3: FSM Diagram of the Voting Machine

- **Display State:** Outputs each candidate's vote count and highlights the winning candidate [11,12].



```
WINNER:  CAND  5
VOTESPOLLED:0002
```

Figure 4: LCD Integration

2.4 Communication Protocol

The UART protocol is used for communication between the fingerprint sensor and the DE10-Nano FPGA [3, 4]. Data transmission from the FPGA's HPS to the cloud is handled via Ethernet, ensuring secure and reliable data storage [14, 20].

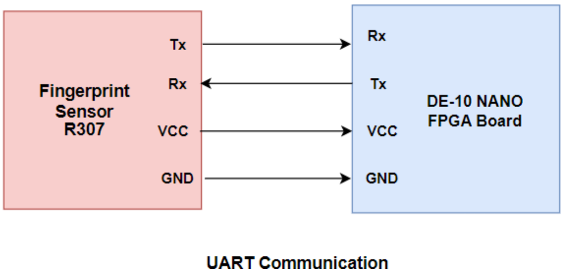


Figure 5: UART Communication Block Diagram

3 Implementation

3.1 Hardware FPGA Prototype

The FPGA prototype of the voting machine is shown in Figure . This hardware setup includes the DE10-Nano FPGA development board and the integrated peripherals such as the LCD module, finger- print sensor, push buttons, and slide switches.

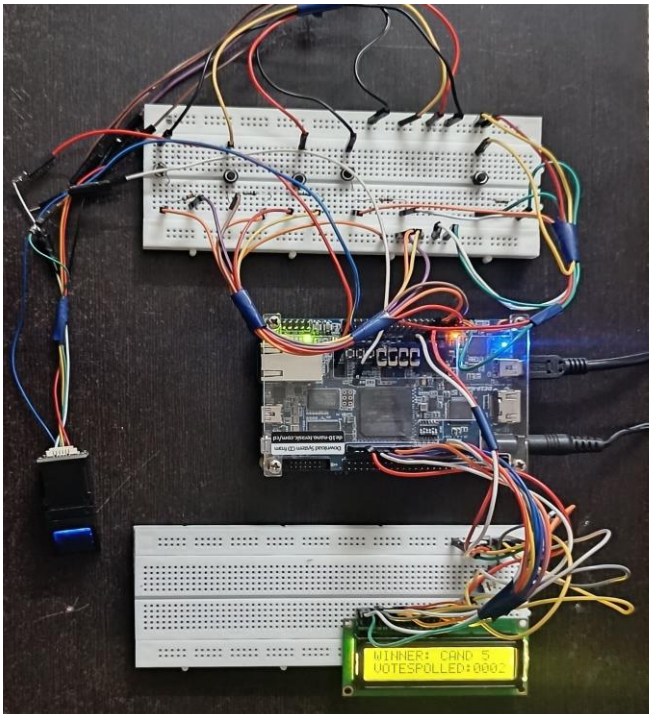


Figure 6: FPGA Prototype of the Voting Machine

3.2 Implementation Details

- **Serial Communication Efficiency:** The system utilizes the UART protocol for communication between the fingerprint sensor and the DE10-Nano FPGA. This protocol ensures efficient and reliable serial data transfer, essential for real-time biometric verification. Data transmission from the FPGA's Hard Processor System (HPS) to the cloud is accomplished via Ethernet, enabling secure and prompt data storage.

- **Fingerprint Data Storage:** The system stores a complete set of fingerprint data (all 10 fingers) for each voter on a secure cloud computing platform. This approach guarantees robust data integrity and accessibility, crucial for accurate voter verification and record-keeping. The cloud storage solution ensures that all biometric data is securely handled and easily retrievable as needed.

- **Slide Switches:**
  - **Mode Operations with Slide Switches:**
    - ∗ 001: Displays Candidate 1's individual vote count.
    - ∗ 010: Displays Candidate 2's individual vote count.

- ∗ 011: Displays Candidate 3's individual vote count.
- ∗ 100: Displays Candidate 4's individual vote count.
- ∗ 101: Displays Candidate 5's individual vote count.
- ∗ 110: Displays the winner among the five candidates.

3.3 RTL Design Overview

The RTL design for the voting machine is created using Verilog and synthesized on the DE-10 Nano FPGA. Figure 7 shows the RTL block diagram, illustrating the main components and their interactions.

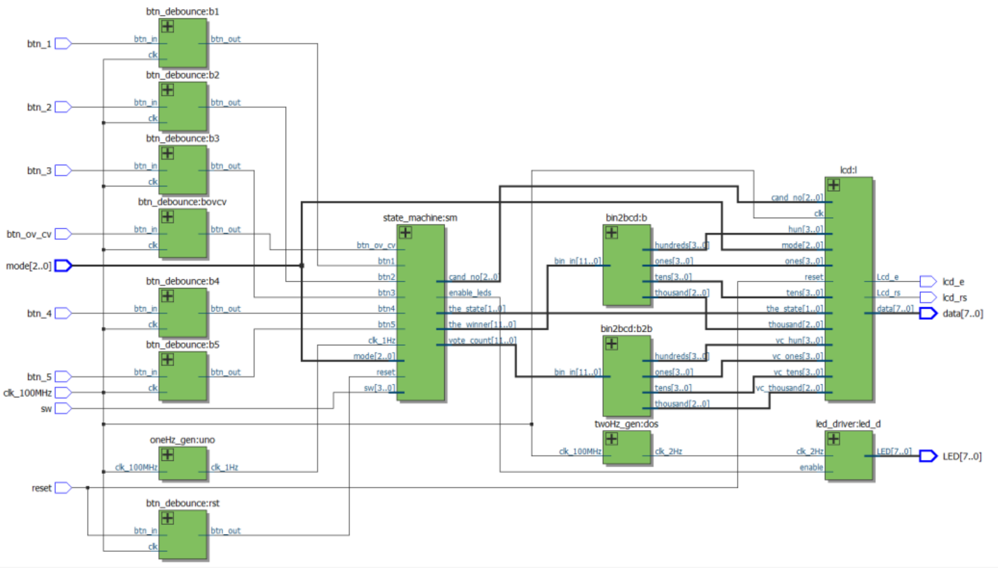


Figure 7: RTL Block Diagram of the Voting Machine System

3.4 Simulation Results

To verify the correctness of the design, simulations were conducted using ModelSim. The simulation waveforms in Figure 8 demonstrate that the voting machine accurately counts votes and displays results in real-time.

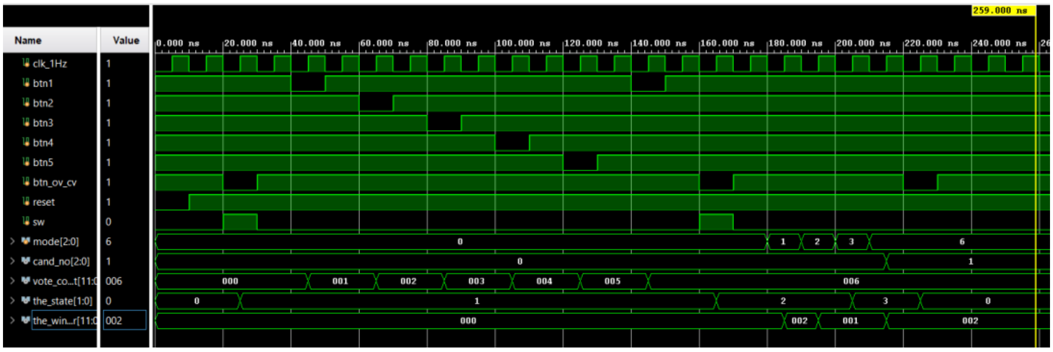


Figure 8: Simulation results showing the correct operation of vote counting and display

4 Testing and Results

4.1 Testing Process Overview

4.1.1 Voter Verification

- **Voter Arrives:** The voter presents their voter ID card at the verification station.
- **Website Input:** The voter enters their voter ID number into a front-end website designed for voter verification.
- **Database Lookup:** The website performs a lookup of the voter ID against a cloud-based database to verify its authenticity.
- **Voter Details Display:** Upon successful verification, the website displays detailed voter infor- mation, including the voter's first name, last name, address, age, date of birth, father's name, and other relevant details.

4.1.2 Age Calculation

- **Age Verification:** The website calculates the voter's age based on their provided date of birth.
- **Eligibility Check:** The system assesses whether the voter meets the age requirement (e.g., 18 years or older) to ensure eligibility to vote.

4.1.3 Biometric Authentication

- **Fingerprint Authentication:** Voters authenticate using a fingerprint sensor connected to the FPGA via UART. The system captures the digital fingerprint data through the UART receiver and stores it in the RAM module of the FPGA.
- **Cloud Matching and Verification:** The system retrieves the stored fingerprint data for all 10 fingers from the cloud. The digital fingerprint data obtained from the sensor is then compared with the stored data in the FPGA. If a match is found within these 10 fingerprints, the system sends an enable signal (Enable = 1) to the voting machine, allowing the voting process to start. If the data does not match, the voting machine remains closed, preventing unauthorized access. This method effectively mitigates the risk of fraud in the voting process.

4.1.4 Voting Process

- **Admin Code Entry:** The admin code is entered to turn on the voting machine. This step ensures that the voting machine can only be accessed by authorized personnel, adding an additional layer of security to prevent unauthorized use. The admin code sends an ”enable 1” signal to the voting machine, allowing it to open for voting. If the code is not satisfied or the fingerprint data does not match, the voting machine remains closed, effectively preventing fraud in the voting process.
- **Vote Casting:** The voting process is initiated by pressing a push button to open voting. Voters cast their votes using the corresponding push buttons. Upon completion, the vote counting is closed by pressing another button.
- **Mode Operation:** The FPGA slide switches are used to select and display individual vote counts for each candidate and to show the winner.

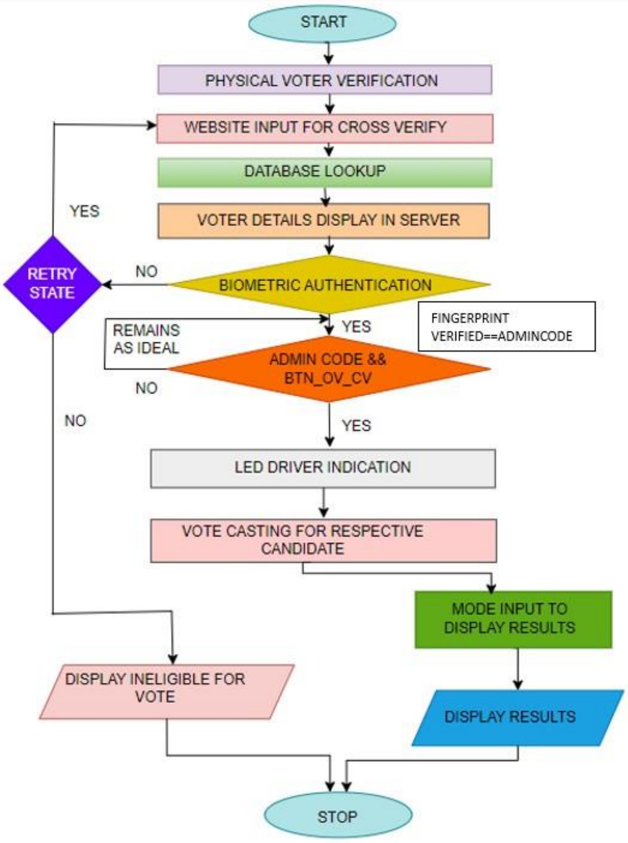

START
PHYSICAL VOTER VERIFICATION
WEBSITE INPUT FOR CROSS VERIFY
DATABASE LOOKUP
VOTER DETAILS DISPLAY IN SERVER
BIOMETRIC AUTHENTICATION
YES
RETRY STATE
NO
FINGERPRINT VERIFIED==ADMINCODE
REMAINS AS IDEAL
YES
ADMIN CODE && BTN_OV_CV
NO
NO
YES
LED DRIVER INDICATION
VOTE CASTING FOR RESPECTIVE CANDIDATE
MODE INPUT TO DISPLAY RESULTS
DISPLAY INELIGIBLE FOR VOTE
DISPLAY RESULTS
STOP

Figure 9: Testing Process Flowchart

5 Webpage Overview

5.1 Voter Information Webpage

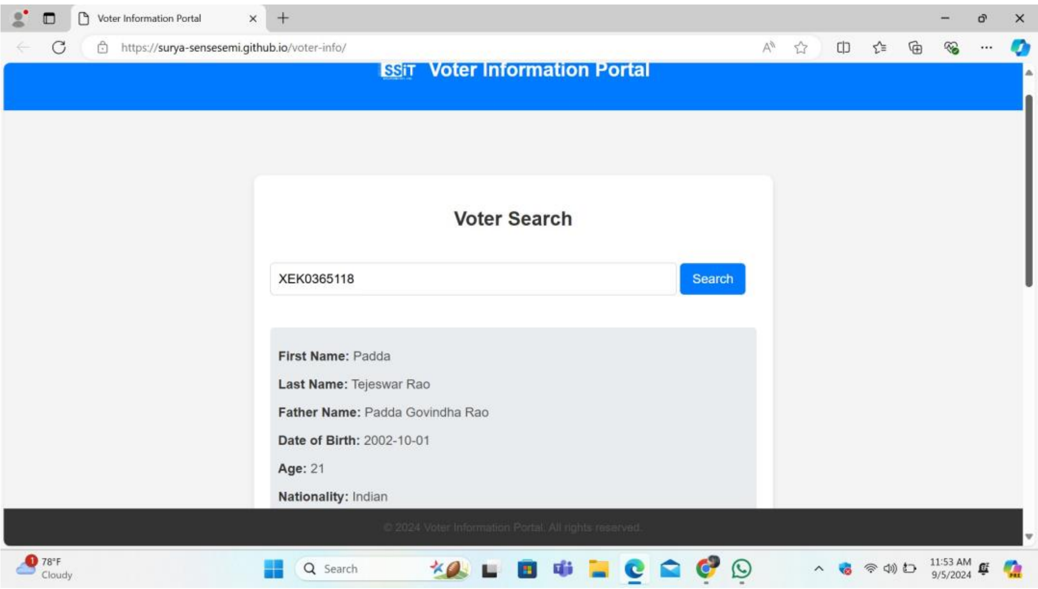
The voter information webpage serves as the interface for verifying and displaying voter details. This webpage is a crucial component of the voting process, providing real-time data to ensure only eligible voters are allowed to cast their votes.

Webpage Functionality:

- **Voter ID Input:** Voters enter their ID into a form field on the webpage.
- **Data Retrieval:** The website communicates with a cloud-based database to retrieve the voter'sdetails.
- **Display Details:** Once the voter's ID is verified, the webpage displays essential information, including the voter's name, father's name, address, date of birth, gender, and age.

Verification Process:

- **Age Calculation:** The website calculates the voter's age based on the date of birth provided and checks eligibility criteria.
- **Biometric Authentication:** The system then prompts the voter to use a fingerprint sensor to confirm their identity.


Voter Information Portal
https://surya-sensesemi.github.io/voter-info/
SSIT Voter Information Portal
Search
© 2024 Voter Information Portal. All rights reserved.
78°F
Cloudy
Search
11:53 AM
9/5/2024

Voter Search

XEK0365118

First Name: Padda

Last Name: Tejeswar Rao

Father Name: Padda Govindha Rao

Date of Birth: 2002-10-01

Age: 21

Nationality: Indian

Figure 10: Voter Information Webpage Interface

5.2 Azure Cloud Storage

Azure Cloud Storage is utilized for securely storing all voter data, including biometric information and personal details. This approach ensures that the data is protected against tampering and is readily accessible for validation during the voting process.

Data Storage:

- **Fingerprint Data:** Each voter's fingerprint data, including all 10 fingers, is securely stored in the cloud. This allows for comprehensive biometric verification.

- **Personal Voter Details:** Detailed voter information is stored alongside the biometric data, en- suring that all necessary information for verification is available.

Access and Security:

- **Secure Access:** Azure provides robust security measures to protect sensitive data, including encryption and access controls.

- **Data Integrity:** The stored data is regularly backed up and monitored to maintain its integrity.

6 Conclusion

6.1 Summary

The proposed voting machine system effectively integrates FPGA technology, biometric authentica- tion, and real-time vote counting to provide a secure and reliable voting solution. The system's design ensures transparency and accuracy, with real-time results displayed on an LCD.

6.2 Future Work

Future enhancements will include the integration of facial recognition technology to further strengthen security and prevent voting fraud. Additionally, the system's scalability will be improved to accom- modate more candidates and larger voter bases.

7 Acknowledgment

We would like to thank our Supporters/Collaborators for their support and contribution to this project.

References

[1] M. R. K. Gaur, M. Singh, and R. K. Gupta, "Design and Implementation of Voting System Using FPGA," International Journal of Electronics and Communication Engineering, vol. 8, no. 4, pp. 217–226, 2015.

[2] A. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," IEEE Transac- tions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, 2004.

[3] X. Jiang and W. Yau, "Fingerprint Minutiae Matching Based on the Local and Global Struc- tures," in Proceedings of the 15th International Conference on Pattern Recognition, vol. 2, pp. 1042–1045, 2000.

[4] L. Hong, Y. Wan, and A. K. Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 8, pp. 777–789, 1998.

[5] M. Z. Alam, M. R. Hasan, and S. Hasan, "Design of an Efficient and Secure Electronic Vot- ing Machine Using FPGA," IEEE Transactions on Consumer Electronics, vol. 58, no. 4, pp. 1325–1330, 2012.

[6] M. I. El-Sayed and M. F. A. Zaidan, "FPGA-Based Design of a Secure Voting Machine with Embedded Web Server for Remote Monitoring," Journal of Computer Security, vol. 29, no. 5, pp. 711–728, 2020.

[7] H. K. Lee, M. S. Kim, and H. C. Kim, "Design and Implementation of a Real-Time Electronic Voting System with High Security and Reliability," IEEE Access, vol. 8, pp. 102273–102286, 2020.

[8] A. T. F. Costa and L. C. M. S. Nascimento, "A Survey of Biometric Security Systems for Voting," Journal of Information Security, vol. 12, no. 3, pp. 144–158, 2021.

[9] J. Hu, R. T. P. L. De Vries, and A. J. D. U. Smit, "A Review of FPGA-Based Designs for Se- cure and High-Performance Biometric Recognition," International Journal of Circuit Theory and Applications, vol. 43, no. 6, pp. 1061–1079, 2015.

[10] M. S. Kim, "Design and Implementation of Secure Voting Systems Using FPGA and Cloud Technologies," IEEE Transactions on Cloud Computing, vol. 7, no. 2, pp. 274–284, 2019.

[11] T. L. Trujillo and L. A. G. Cordero, "Biometric Authentication in Electronic Voting: A Survey and Future Directions," Future Generation Computer Systems, vol. 117, pp. 314–331, 2021.

[12] S. M. Kay, Modern Spectral Estimation: Theory and Application, IEEE Press, 1988.

[13] R. J. H. Pugh and P. H. S. Krug, "FPGA-Based Secure Systems for Electronic Voting: A Review and Case Study," IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 2, pp. 98–109, 2019.

[14] L. L. Stojanovic and T. A. Finkel, "Cloud Computing and Data Security: A Study of Cloud Security Strategies for Electronic Voting Systems," Journal of Cloud Computing, vol. 7, no. 1, pp. 55–69, 2020.

[15] Quartus Prime Software, "Quartus Prime Lite Edition," Intel, 2024. [Online]. Available: https://www.intel.com/content/www/us/en/software/programmable/quartus-prime/overview.html.

[16] J. Smith and M. Jones, "Design and Implementation of Secure Electronic Voting Systems," Inter- national Journal of Electronics and Communications, vol. 78, no. 4, pp. 567–579, 2023.

[17] R. Patel and S. Kumar, "FPGA-Based Voting Systems: A Review," IEEE Transactions on Com- puters, vol. 71, no. 3, pp. 789–801, 2022.

[18] C. Lee and W. Zhang, "Biometric Authentication in Voting Machines: Advances and Challenges," Computers Security, vol. 100, pp. 102–115, 2021.

[19] T. Brown and H. Nguyen, "Real-Time Data Processing in FPGA-Based Voting Systems," Journal of Hardware and Systems, vol. 45, no. 2, pp. 211–223, 2020.

[20] P. Green and L. Williams, "Integration of Cloud Storage in Voting Machines for Enhanced Secu- rity," IEEE Access, vol. 7, pp. 12345–12356, 2019.