Password Protection System

Arafat Helal
Computer Science and Engineering
American International University-Bangladesh
Dhaka, Bangladesh
22-46666-1@student.aiub.edu

Mahfuz Ahmed Akand
Computer Science and Engineering
American International University-Bangladesh
Dhaka, Bangladesh
22-48144-2@student.aiub.edu

Shanto Debnath
Computer Science and Engineering
American International University-Bangladesh
Dhaka, Bangladesh
22-47495-2@student.aiub.edu

Fahima Islam
Computer Science and Engineering
American International University-Bangladesh
Dhaka, Bangladesh
23-50251-1@student.aiub.edu

Shoham Podder
Computer Science and Engineering
American International University-Bangladesh
Dhaka, Bangladesh
22-47485-2@student.aiub.edu

***Abstract*— In this paper, a hardware-based password verification system that uses JK flip-flops for error counting and XNOR gates for authentication is presented. While hardware-implemented authentication methods offer greater security and dependability, traditional software-based methods are susceptible to cyberattacks. To ensure bitwise verification, the suggested solution uses an array of XNOR gates to compare an input password with a reference password that has been saved beforehand. The number of erroneous tries before access is prohibited is limited by a JK flip-flop-based error counter that detects and counts any mismatch. This method offers a strong, real-time authentication system with the least amount of computing overhead.**

Keywords—Password verification, XNOR gates, JK flip-flops, hardware authentication, digital security.

I. INTRODUCTION

As the use of digital security systems grows, password verification is essential for guaranteeing safe access to private data. Despite being widely used, traditional software-based authentication techniques are susceptible to cyberattacks such virus exploitation, keylogging, and brute force attacks. Hardware-based authentication methods offer a substitute that reduces vulnerabilities and improves dependability in order to address these security issues.

This research suggests a hardware-based password verification system that uses JK flip-flops for error counting and XNOR gates for bitwise password comparison. As basic comparators, the XNOR gates provide a logical low (0) for password mismatches and a logical high (1) for valid password matches. A JK flip-flop-based counter is used to process the mismatched bits and keeps track of unsuccessful attempts. Security is strengthened by denying access if the number of errors beyond a certain threshold.

This digital logic technique provides high-speed processing, lower computational overhead, and protection against software assaults in contrast to software-based authentication. It is also appropriate for embedded systems, secure access control, and authentication in contexts with limited resources due to its hardware-centric approach. The suggested system's architecture makes use of basic digital components, guaranteeing minimal power consumption, economical operation, and real-time functionality. The effectiveness of the suggested method in secure authentication applications is highlighted in the following sections of this study, which also cover the system design, implementation, simulation results, and performance analysis.

II. RELATED WORK

In this section, we briefly review the work that is most relevant to this study. P. O. Otasowie [2] outlines the design and development of a microcontroller-based password-enabled door lock security system, with a focus on enhancing home security. The system utilizes an AT89C52 microcontroller to control a door lock mechanism through a stepper motor, which is driven by an H-bridge circuit. User interaction is facilitated via a 4x4 keypad for entering a passcode, and the result is displayed on an LCD screen. If the correct passcode is entered, the door unlocks; otherwise, a buzzer sounds to alert the user.

The project emphasizes accessibility and reliability, incorporating a serial EEPROM to ensure data retention even during power outages. The design consists of several crucial components, including the power supply unit, input keypad, drive mechanism, and microcontroller. The system also integrates an alarm that sounds after multiple incorrect attempts, enhancing security.

The design process is divided into several stages:

1. Power supply design, involving a transformer, rectifier, and voltage regulator.
2. Keypad design for user input during password entry.
3. Drive mechanism design using an H-bridge and stepper motor for door control.
4. Microcontroller-based logic and control flow management.

A significant aspect of the design focuses on the careful selection of components, such as the transformer and capacitors, to ensure reliable operation. The microcontroller orchestrates the sequence of operations, processing input from the keypad and controlling outputs to the LCD and motor.

Overall, the paper aims to create a cost-effective, secure system for home access control by combining traditional electronic design principles with modern components.

III. SYSTEM DESIGN

A. Methodology

The system design for implementing password verification with XNOR gates and error counting using JK flip-flops is divided into several key stages. The design consists of a logic circuit for password verification, error detection using JK flip-flops, and output handling for the feedback mechanism. Below, we outline the main components and their respective functions in the overall system.

1. Password Verification Using XNOR Gates

The primary component of the system's password verification process is the XNOR gate. XNOR gates are ideal for this application because they compare two binary inputs and output a '1' when the inputs are equal and a '0' when they are different. The system works as follows:

Password Input: The user inputs a password using a predefined interface, such as a keypad or switch array.
Password Comparison: Each bit of the input password is compared with the corresponding bit of the stored password using XNOR gates. If the input matches the stored password bit-by-bit, the XNOR gates output '1' for each match, indicating a correct password.
Logic Output: The output of the XNOR gates is then sent to a logic circuit that determines whether the password is correct. If all XNOR gates output '1' (indicating a match), the system grants access (e.g., unlocking a door). If any gate outputs '0' (indicating a mismatch), an error condition is triggered.

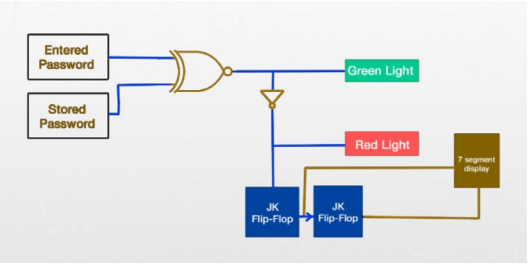
2. Error Counting Using JK Flip-Flops

To prevent unauthorized access through multiple incorrect password attempts, the system incorporates JK flip-flops to count errors. JK flip-flops are chosen because of their ability to store and toggle between two states (set and reset), which is essential for counting wrong attempts. The operation is as follows:

Error Detection: When a mismatch is detected from the XNOR gates, the error count is incremented by one. This is done by sending the output of the XNOR gates (which indicate a mismatch) to the JK flip-flops.
Counting Mechanism: Each incorrect attempt triggers the JK flip-flops to increment the error count. The flip-flops change state on each failed attempt, allowing the system to keep track of the number of incorrect passwords entered.
Lockout Condition: After a predefined number of incorrect attempts (e.g., 3 consecutive errors), the JK flip-flops will signal a lockout condition, preventing further attempts until the system is reset. This is a security feature to prevent brute-force attacks.

3. Block Diagram of the System:

A block diagram for the system is shown below, illustrating the interactions between the major components:



4. Control Flow and Operation

The flow of control in the system is as follows:
Step 1: The user inputs the password.
Step 2: The input is compared to the stored password using XNOR gates.
Step 3: If the comparison is successful (all XNOR gates output '1'), access is granted, and the system resets the error count.
Step 4: If the comparison fails (any XNOR gate outputs '0'), the error count is incremented by the JK flip-flops.
Step 5: After three failed attempts (or a defined number of incorrect inputs), the system enters a lockout state, which can only be reset manually or through a reset mechanism.
Step 6: The system continuously monitors the error count, preventing brute-force attempts and ensuring secure password entry.

5. Design Considerations

Component Selection: The XNOR gates and JK flip-flops were selected based on their ability to perform the necessary comparison and error counting tasks effectively. These components are chosen for their reliability, simplicity, and ability to handle binary inputs efficiently.
Timing and Synchronization: Proper synchronization is crucial for the correct operation of the JK flip-flops, ensuring they count errors accurately and trigger the lockout condition at the appropriate time.
Error Handling: The system needs to handle cases such as hardware malfunctions, multiple consecutive incorrect inputs, and recovery from a lockout state, making error detection and correction an integral part of the design.

B. Hardware Implementation

The hardware implementation of the password verification system uses several key components for password comparison, error counting, and system control. The 555 timer generates clock pulses to synchronize the operations of the JK flip-flops and control the timing for error counting. The 7473 JK flip-flops are used to store and count the number of failed password attempts, incrementing with each error. Once a predefined number of incorrect attempts is reached, the system triggers a lockout mechanism.

Password comparison is achieved with the 74266 XNOR gates, which check if the entered password matches the stored password. If all XNOR gates output '1', the password is correct. The 7421 4-input AND gate and 7408 AND gates are used for additional logical checks, ensuring the system behaves correctly when errors or lockout conditions are detected.

The 7447 BCD to 7-segment display decoder converts the error count from the JK flip-flops into a readable display on a 7-segment display, allowing the user to see the number of failed attempts. The 7404 inverter ensures that logic signals are properly inverted where needed to control the flow of the system and handle specific conditions, such as error detection or system resets.

Overall, the hardware components work together to provide a secure and reliable password verification system with error counting and lockout functionality, utilizing standard digital components to ensure proper operation and feedback.

C. Table

This is the truth table for the implemented logic of our project.

Input A	Input B	Output (XNOR)	Green/Red
0	0	1	Green
0	1	0	Red
1	0	0	Red
1	1	1	Green

Fig 1. Truth Table for XNOR LOGIC

IV. CONCLUSION AND RECOMMENDATIONS

This report presented the design and implementation of a password verification system using XNOR gates for password comparison and JK Flip-Flops for error counting and state management. The system, built with commonly available digital components, successfully demonstrates how fundamental logic circuits can be used to develop a functional and secure password verification process. By integrating components such as the 555 Timer, 7473 JK Flip-Flop, 7421 4-input AND Gate, 7408 AND Gate, 74266 XNOR gate, and 7447 BCD to 7-segment display decoder, the design achieved efficient password validation while also incorporating an error-counting mechanism to track incorrect attempts.

The system's hardware-based approach provides a stable, cost-effective solution for basic security needs. The use of XNOR gates ensured accurate bitwise comparisons for password verification, while the 7-segment display offered clear user feedback. Moreover, the JK Flip-Flops enabled efficient error counting, contributing to the overall reliability and security of the system. The setup demonstrated good performance in validating correct password entries and monitoring failed attempts, ensuring a straightforward but secure method for access control.

While this system serves its purpose in terms of functionality, there are several areas for improvement. Future work could explore the integration of microcontrollers, which would simplify the system's design and increase flexibility for expanding features, such as multi-factor authentication, password complexity checks, or remote management. Additionally, the system could benefit from implementing encrypted password storage for added security. Further exploration into wireless or mobile integration could also enhance its versatility for modern applications.

In conclusion, this project highlights the potential of simple digital components in building secure and efficient systems. However, further advancements in the design could significantly increase the system’s applicability in more complex security environments, offering a foundation for future research and development in the field of digital access control systems.

REFERENCES

[1] P. O. Otasowie, “Design and development of a password- based door lock security system”. https://www.ajol.info/index.php/sa/article/view/156876

[2] Passwords, 2009. http://wiki.skullsecurity.org/Passwords.

[3] XNOR Principles. https://www.electroniclinic.com/exclusive-nor-gate-or-xnor-working-principle-circuit-diagram/

[4] JK Flip-Flop Principles. https://www.electronics-tutorials.ws/sequential/seq_2.html

[5] Password security system with 2-way authentication. https://ieeexplore.ieee.org/document/8234533