Project Title: Password-Protected Door Lock with Anti-Theft Protection System

Abst**ract**

The “Password Security Door Lock with an anti-theft protection system demonstrates a secure, user-friendly, and cost-effective solution for security measures using an ATMega32 microcontroller. By integrating a 4x4 keypad, a 16x2 LCD, and a buzzer for alerts, the system enables users to unlock doors with a preset password, manage passwords via an admin mode, and provides an anti-theft mechanism that activates after three incorrect attempts. Designed with modularity and energy efficiency, the system supports alphanumeric passwords, which ensure diverse applications ranging from residential and commercial security to healthcare and education systems. Its scalability supports future possibilities, such as IoT integration, RFID integration, multilingual support, and enhanced encryption for user data safety. The project offers a robust solution that addresses modern security challenges, ensuring safety, usability, and adaptability across various sectors of security concerns.

I. Introduction

Security is one of the fundamental needs in both residential and commercial spaces. Traditional mechanical locks, while widely used, have certain limitations such as vulnerability to picking, tampering, and the need for physical keys, which can be lost or duplicated. To address these issues, the advancement in microcontroller-based systems has enabled the development of more secure, efficient, and user-friendly solutions. This project focuses on designing and implementing a password-protected door lock system using the ATMega32 microcontroller and a 4x4 keypad. Additionally, there will be an LCD for the user to know the current state of the system. The system provides secure access control by allowing users to unlock a door using a predefined password while incorporating an anti-theft mechanism that triggers a buzzer after multiple incorrect attempts. Additionally, it offers password management functionality, enabling users to reset or update their passwords as needed.

Furthermore, research on keypad passcode design for smart lock door systems emphasizes the importance of user-friendly interfaces and robust security measures in developing effective locking mechanisms. Sari and Wibowo (2023) discuss the implementation of automatic door security systems using solenoid lock doors controlled by microcontrollers, highlighting the relevance of integrating microcontroller technology to enhance security systems.

By combining simplicity with advanced functionality, this project offers an affordable and scalable alternative to complex smart locks. The system's compact and energy-efficient design makes it suitable for deployment in various small-scale applications, including homes, offices, lockers, and storage rooms. This report provides a comprehensive overview of the system's design, implementation, and evaluation, with a focus on its technical features, practical applications, and potential avenues for future enhancement.

II. Scopes & objective

The password-protected door lock system is designed to provide a secure, reliable, and user-friendly solution for access control in small-scale applications. This project is aimed at addressing the limitations of traditional locks by utilizing a microcontroller-based mechanism for enhanced security. In terms of applications, the system is highly versatile. It can be deployed in residential homes to secure doors, in office environments to restrict access to specific rooms or storage areas, and in lockers or vaults where simple yet robust security is essential. The compact design and affordability make it an attractive alternative to complex smart locks, especially for small-scale use cases.

Hardware Scope:

The hardware used in the system includes the ATMega32 microcontroller, which acts as the central processing unit for managing inputs, outputs, and logical operations. The 4x4 keypad facilitates user interaction, while a servo motor handles the locking and unlocking mechanism. A buzzer provides audio feedback for successful operations and serves as an alarm in case of unauthorized attempts. These components work together seamlessly to deliver a compact and efficient locking solution.

Functional Scope:

The functional scope of the system includes password-based access control, where users can lock or unlock the door by entering a predefined password through a 4x4 keypad. To ensure security, the system incorporates an anti-theft mechanism that triggers an alarm after multiple incorrect

password attempts, effectively deterring unauthorized access. Additionally, the system allows users to manage their passwords with ease, offering options to set, reset, or update it whenever needed. Energy efficiency has also been prioritized in the design, ensuring that the system consumes minimal power and remains operational over extended periods.

Looking to the future, the scope of the project extends beyond its current capabilities. The system can be enhanced with advanced features such as integration with IoT for remote access or monitoring, as well as biometric authentication methods like fingerprint or facial recognition. These upgrades would make the system even more secure and adaptable for broader applications. Furthermore, there is potential for incorporating solar power to reduce dependency on non-renewable energy, making it an eco-friendly solution. The project is not only a step toward providing better security but also a foundation for future innovations in access control systems.

Objective

The primary objective of this project is to develop a password-protected door lock system that ensures secure access control while being cost-effective, reliable, and easy to operate. The system is designed to provide an enhanced level of security by allowing only authorized users to unlock the door through password verification.

In addition to securing access, the system incorporates an anti-theft mechanism that activates an alarm after multiple incorrect password attempts, adding a layer of protection against unauthorized access. The design also emphasizes ease of use, enabling users to conveniently manage their passwords, including setting, resetting, and updating them as needed.

By addressing the limitations of traditional locks and offering an affordable alternative to complex smart locking systems, this project should be cost-effective and sustainable.

III. Apparatus & software

1. AVR Kit - ATMega32 MCU
2. Keypad 4X4 matrix
3. JumperWires
4. Buzzer
5. LED
6. CodeVisionAVR
7. ExtremeBurner
8. Proteus

IV. Project specification

To improve security and offer user-friendly functionality, this project entails creating a password-based security system with an ATmega32 microcontroller. The system has a 4x4 matrix keypad through which users can input a password. To ensure confidentiality, each keystroke is shown as '*' on a 16x2 LCD screen. After comparing the entered password to a user password that has been stored, the system allows access if the two match. After three unsuccessful tries in a row, the system locks itself, sounds a buzzer to notify staff in the vicinity, and shows "System Locked" on the LCD. A backspace function improves usability by enabling users to fix input errors. A pre-stored admin password must be entered to prevent unwanted changes, and the password reset procedure is protected by an admin mode and accessible through a dedicated button.

By preventing password resets until the admin password has been successfully verified, admin mode adds an extra degree of security. The system allows the administrator to enter a new user password after it has been validated, and it is saved for later use. Through LCD messages, the system gives users and administrators real-time feedback while they enter, validate, and reset their passwords. The system's robust error-handling design guarantees dependable operation in both typical and urgent situations. Applications needing secure access control, like electronic door locks, equipment access, or restricted areas in commercial, industrial, and residential settings, are best suited for this project. The project shows a useful and adaptable approach to microcontroller-based security systems by combining visual feedback, dependable security measures, and ease of use.

V. Non-technical constraints

The project's non-technical constraints mostly center on aspects like cost, usability, environmental concerns, and social effects that are not directly related to the system's technical design and implementation. Budgetary restrictions are one major barrier because the ATmega32 microcontroller, keypad, LCD, and related peripherals must all be reasonably priced to maintain a reasonable project cost. This is especially crucial for ensuring that the system can be widely adopted in cost-sensitive settings, like homes or small businesses.

The ease of use and accessibility for users is another limitation. For non-technical users, the system must be easy to use so that they can enter passwords, reset them, and reply to alerts without the need for specialized knowledge. The system should also use energy-efficient components to reduce power consumption and its environmental impact, making it environmentally sustainable. Social constraints include making sure the system complies with privacy and security standards set by society, such as shielding user data from unwanted access and steering clear of intrusive alerts that might needlessly disturb public areas.

VI. Methodology

We have taken a comprehensive and intuitive approach to establishing the password security system using the ATMega32. This methodology section will discuss the password-protected security system using a keypad, which is a secure and user-friendly access control mechanism using a microcontroller, ATMega32. The system integrates a 4×4 keypad for input, an LCD for displaying the messages for user interactivity, and a buzzer indicating unauthorized access. The system implements a two-step password validation, which enables users to unlock the system with a preset password while allowing administrators to reset passwords securely. This design priors the functionality of masking the digits, backspace for correction, and system lock after three failed attempts. This methodology ensures reliability and user-friendliness, making it suitable for secure applications in various sectors.

To understand the whole process systematically, we have constructed a comprehensive, detailed flowchart. Here is the flowchart given below,

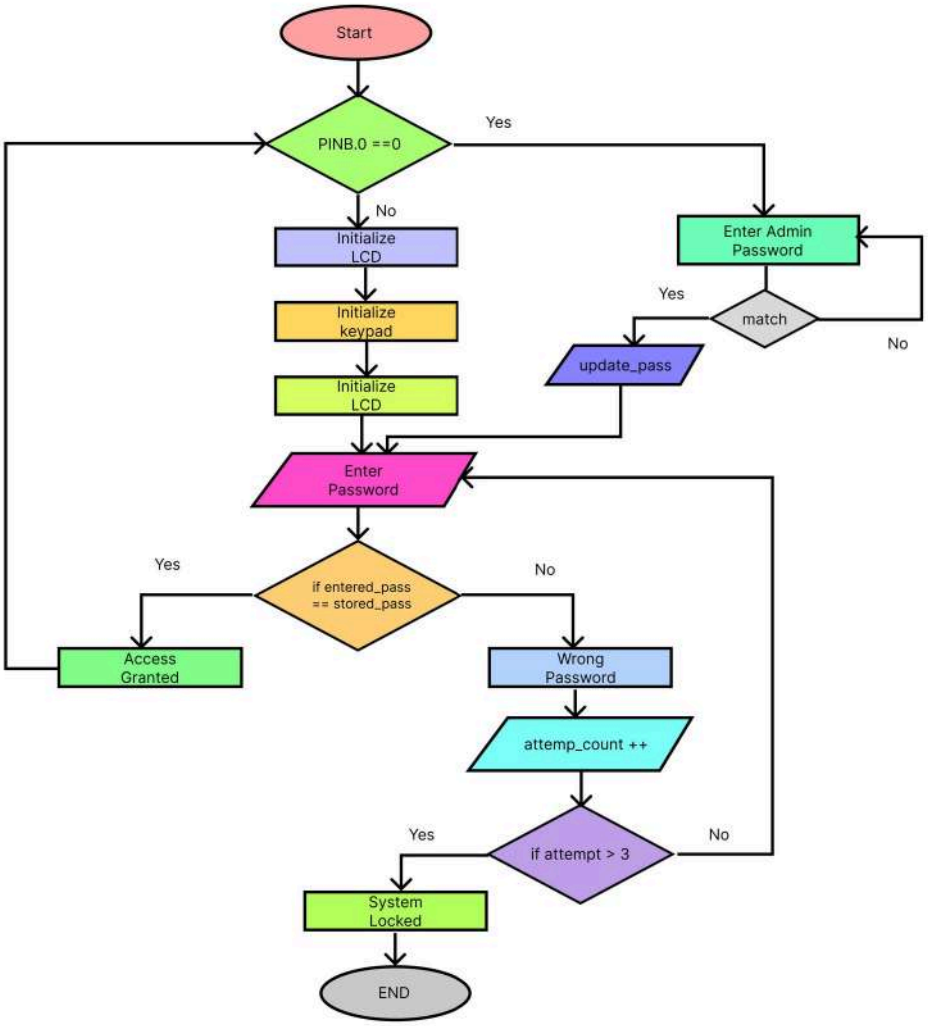

Figure: System working flowchart

First, we started the system and immediately checked whether the PINB.0 was pressed or not. If not, then we are proceeding to the main function of the system. LCD is initialized, and the Keypad is initialized. The LCD will show "Enter Password". Then the system will check whether the password is correct or not. If yes, then the LCD will show "Access granted" and again go to check if the admin button is pressed. If yes, then it will ask for an admin password. After entering the correct password, the system will update the password of the stored_password variable. And then the same process can proceed.

Now, if the entered password does not match the stored password, then the LCD will display the Wrong Password and increase the count in the attempt_count variable. If the attempt count is below 3, the system will return to "Enter Password" again, and the whole process can be started again. But if the attempt_count == 3 then the system will be locked and the process will end and stay locked until the system is reset overall. Below, we are including an algorithm to understand it more deeply:

1. Start
2. Initialize System
3. Display "Enter Password"
4. Wait for keypad input
5. If '*' is pressed: delete the last character

6. If '#' is pressed:
    a. Admin Mode:
        i. Validate admin password
        ii. On success, enable reset mode
    b. Reset Mode:
        i. Save user password
        ii. Disable Reset Mode
    c. User mode:
        i. Validate user password
        ii. On success, grant access
        iii. On failure, increment attempt_count
            - if attempt_count>=3 , Lock System
7. Display system state(access granted/denied, system locked
8. Return to step 3

This is our overall methodology which has been our base approach for implementing the overall embedded C code [Appendix A].

VII. Design choices & alternatives

A. Design approach 1:

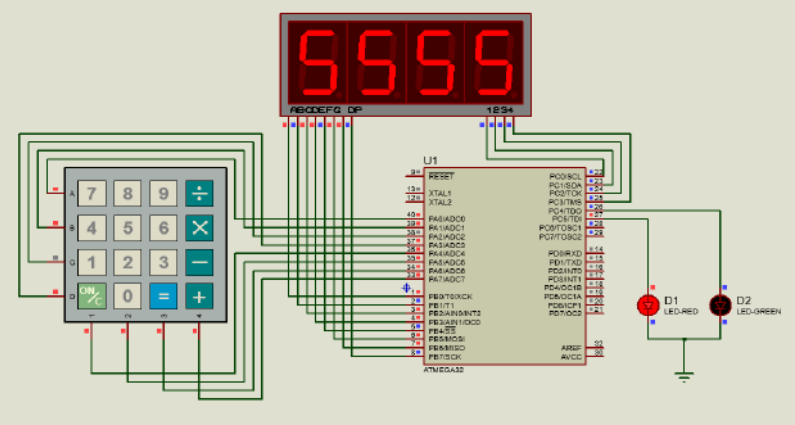

Fig: Design approach 1

In the first design approach, a 4x4 keypad is used to input numeric values into an ATmega32 microcontroller as a password. The output is displayed on a 4-digit seven-segment display, which shows relevant password entries. Two LEDs (red and green) are included to indicate different system states, such as incorrect password entry or successful access. The red LED signals a locked state or error, while the green LED signals a successful operation or access granted.

B. Design approach 2:

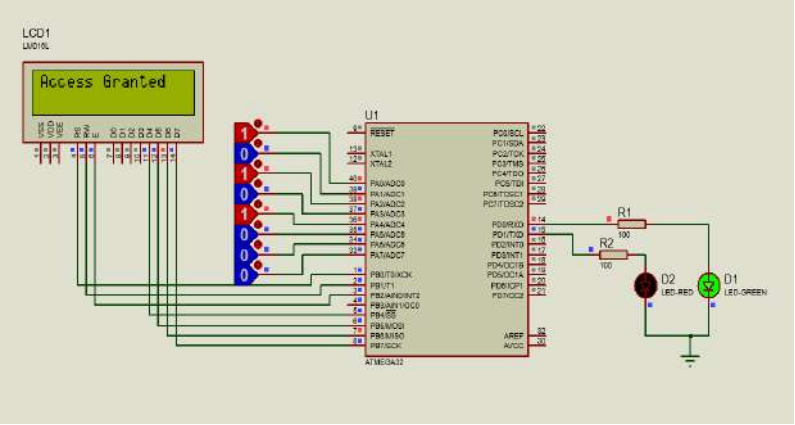

Fig: Design approach 2

The second design approach uses a 4x4 keypad for password input and an LCD screen to display detailed feedback. The system takes the entered password as the logical input for toggling the system state. If the input matches the predefined password stored in the microcontroller's code, the system unlocks and displays the message "Access Granted" on the LCD. Two LEDs are used to indicate the status: the red LED signals a locked or error state, while the green LED indicates successful access.

C. Design approach 3:

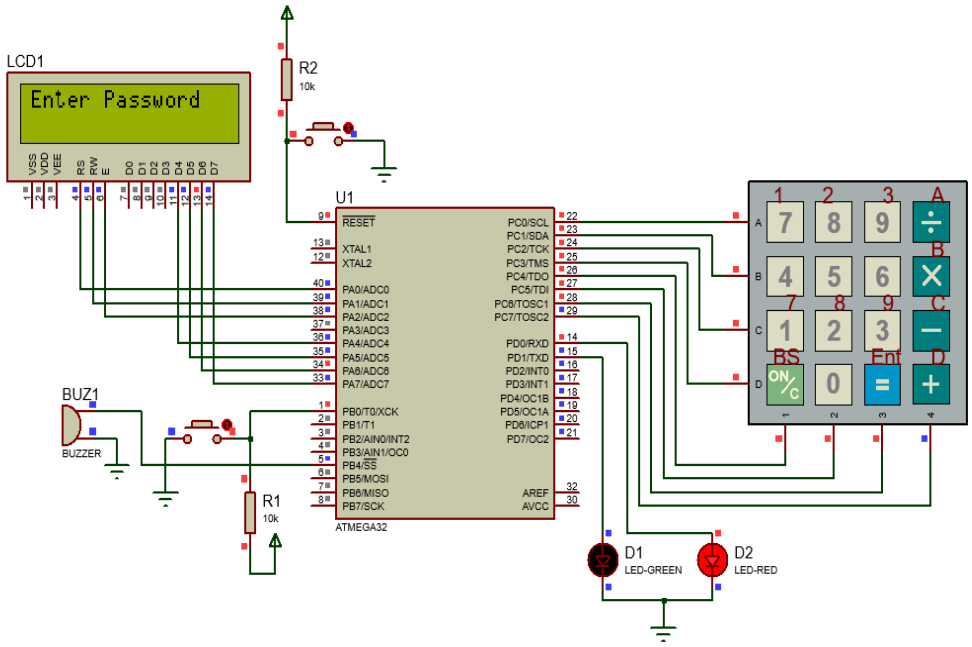

Fig: Design approach 3 (Final Design)

In this third design approach, a 4x4 keypad is used to input a password to unlock the system. The system features an LCD that shows the current state, such as prompting the user to "Enter Password" or displaying "Access Granted" upon successful entry. The LCD also displays messages during the admin verification and password reset processes, providing clear feedback to the user.

Once the correct password is entered, the system unlocks, indicated by the green LED turning on. A switch connected to port PB0 triggers the admin verification process. The admin password is predefined and must be entered correctly to access the password reset functionality. After successful admin verification, the user is prompted to enter and set a new password.

Additionally, if the password is entered incorrectly three times, the system locks, turning on the red LED and activating a buzzer to signal anti-theft mode. This design offers enhanced security through multiple layers of access control and user feedback via the LCD, LEDs, and buzzer, ensuring a user-friendly and secure experience.

D. Justification of the best approach:

The third design approach was selected as the final and best approach due to its comprehensive combination of enhanced user interaction, robust security, and added functionality. Unlike the first design, which relies on a seven-segment display for feedback, the third design utilizes an LCD screen. This allows for more detailed and intuitive feedback, showing the current system state and guiding the user through the process with clear messages such as "Enter Password" or "Access Granted." This greatly improves the user experience by providing real-time updates and reducing potential confusion. Another key advantage of the third design is its ability to handle alphanumeric passwords, including characters like A, B, C, and D. This feature significantly strengthens the security by allowing more complex password combinations compared to purely numeric inputs. The capability to use alphanumeric passwords ensures a broader range of secure and customizable password options, enhancing the system's overall resilience against unauthorized access.

Additionally, the second design introduced the LCD for better feedback but lacked advanced features such as secure password resetting. The third design addresses this by incorporating an admin verification process. A predefined admin password ensures that only authorized users can reset the system password, adding a critical layer of security. This feature is crucial for maintaining control over access and preventing unauthorized changes. Security is further enhanced in the third design with the implementation of an anti-theft mechanism. After three consecutive incorrect password attempts, the system locks, the red LED turns on, and a buzzer is activated to alert you about potential unauthorized access. This is a significant improvement over the previous designs, which either lack such features or provide limited feedback on security breaches.

Moreover, the third design allows for greater flexibility, as it combines secure password management with user-friendly interactions. The ability to reset passwords securely and receive clear, detailed feedback through the LCD makes this design not only secure but also highly functional and user-centric.

In summary, the third design was chosen as the final approach because it offers the most complete solution. It combines detailed feedback, advanced security measures, the ability to use alphanumeric passwords, and flexible functionality, making it the best choice for providing a secure, user-friendly, and interactive system.

VIII. Circuit diagram

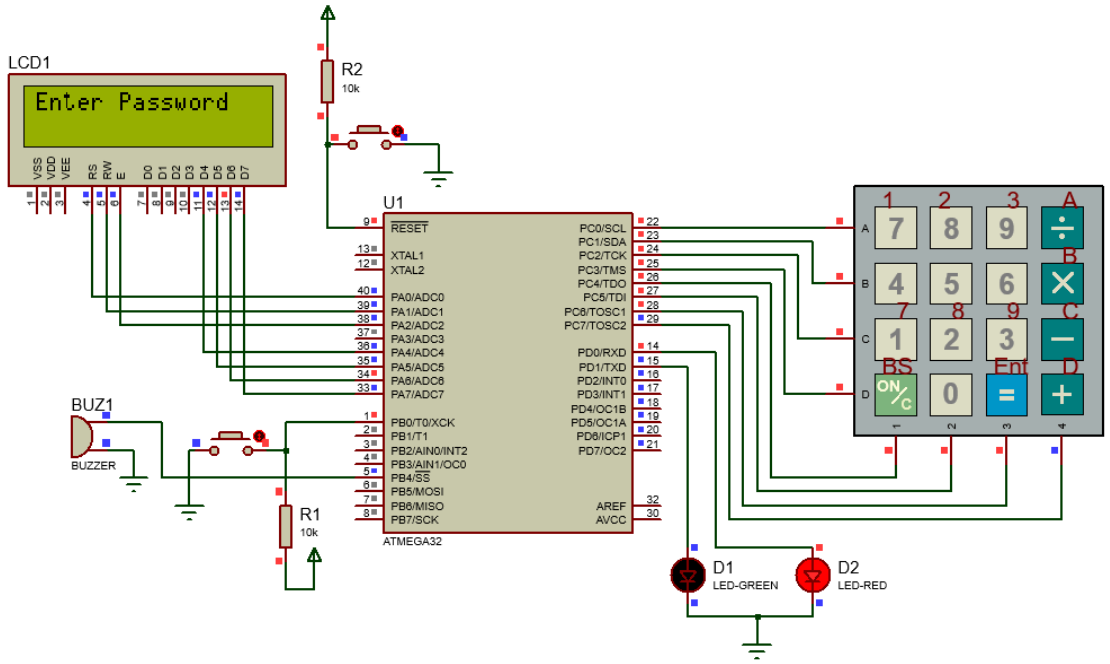

Fig: Main Circuit

IX. Results & discussion

Case 1: Normal Password Entry

In the 1st case when a user enters the correct password on the keypad, the system begins by validating the input. If the entered password matches the stored value in the system, the door will unlock, granting access. At the same time, the LCD screen will display a success message, such as "Access Granted," to confirm that the password was correct and the user is authorized to proceed.

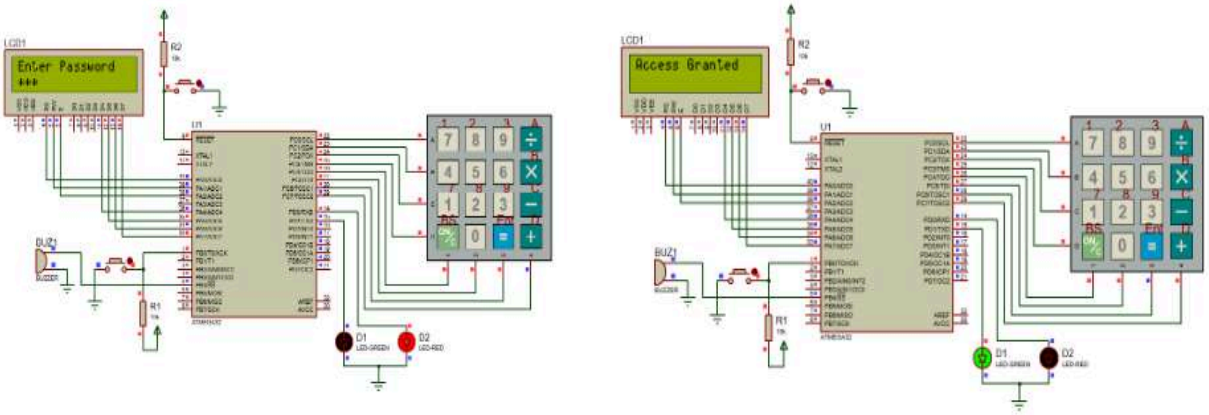

Fig: Normal Password Entry (simulation)

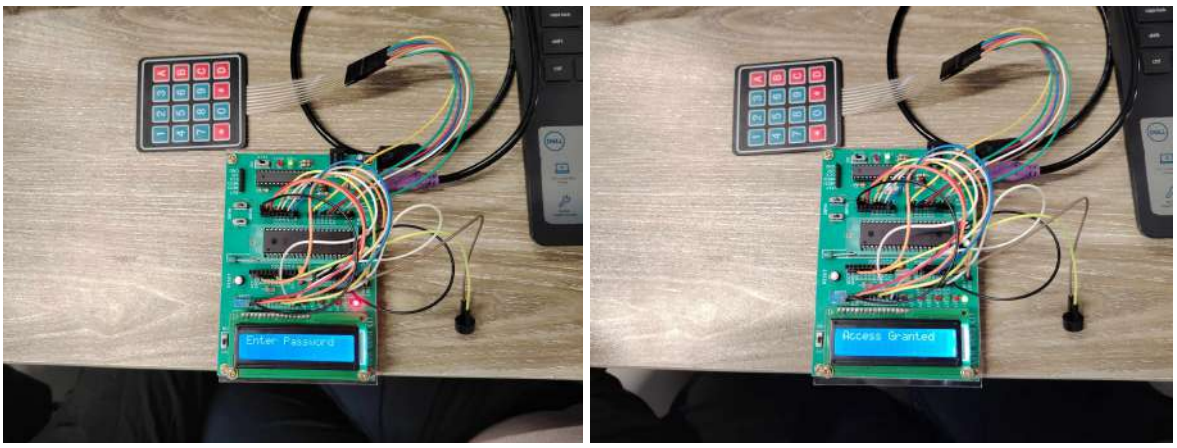

Fig: Normal Password Entry (Hardware Representation)

Case 2: Admin Mode for Password Reset

Upon pressing a designated button, the system enters admin mode and prompts for the admin password. If the password is correct, the user is allowed to set a new password, which is saved to the system's memory. Once the new password is stored, the system exits admin mode and resumes normal operation, using the updated password for future access.

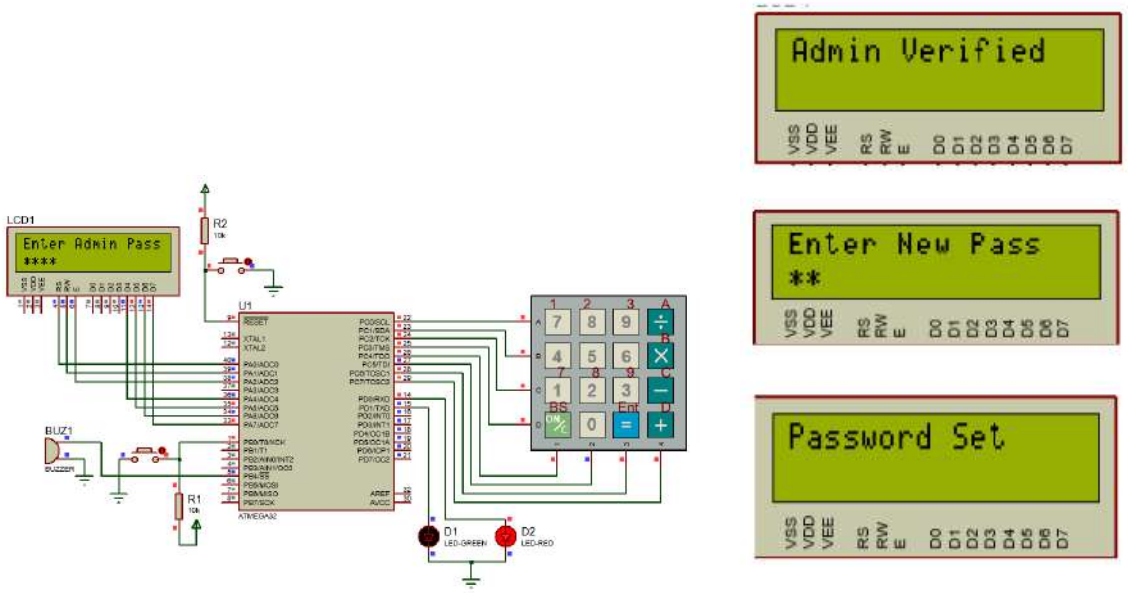

Fig: Admin password setup (simulation)

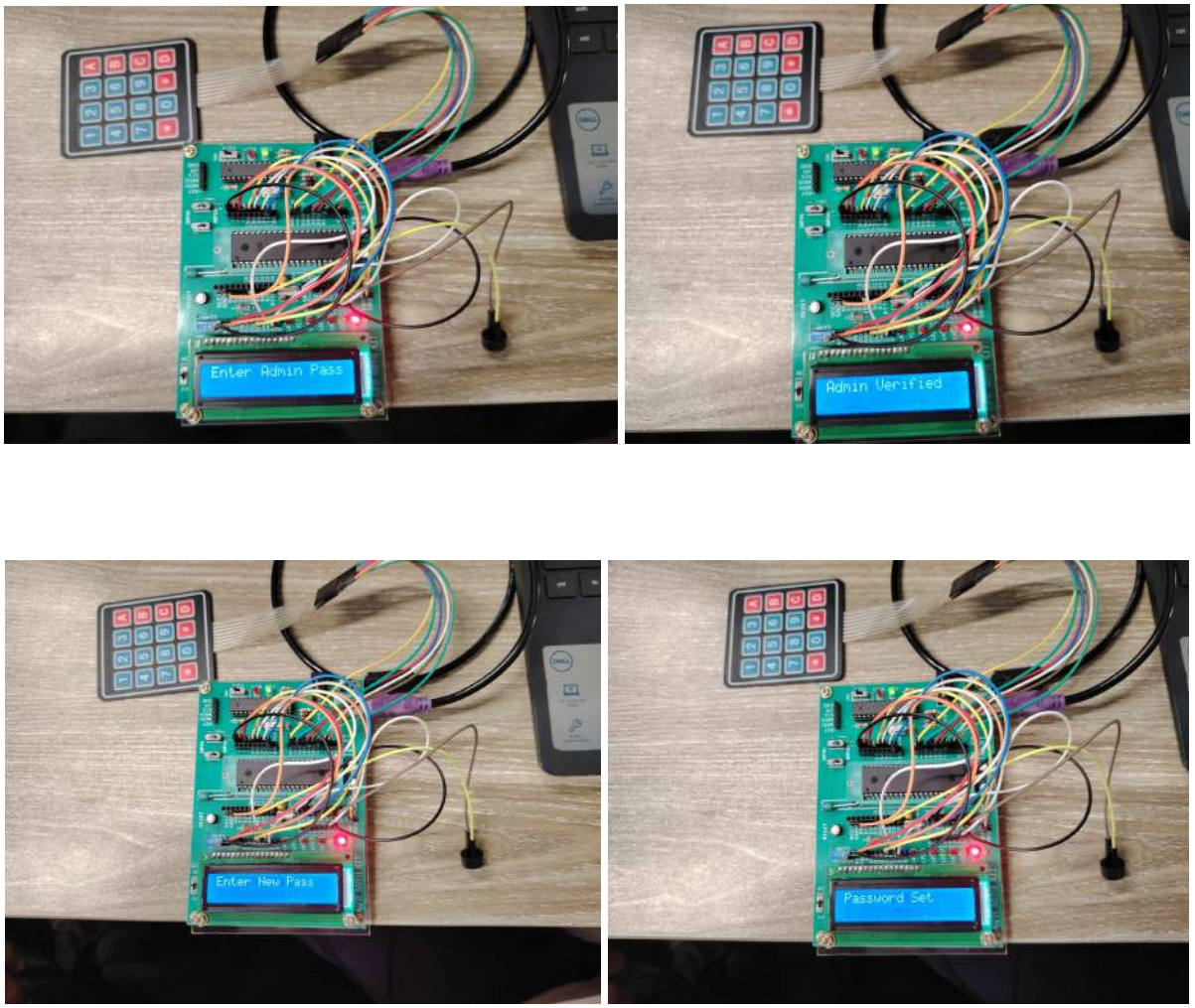

Fig: Admin password setup (Hardware Representation)

Case 3: Incorrect Password Attempts

In this case, when a user enters an incorrect password three times consecutively, the system detects the multiple failed attempts and activates the anti-theft mechanism. This triggers the buzzer, alerting nearby individuals to the potential security breach. To enhance security, the system locks itself, preventing any further attempts. For the user to try again, the system requires a reset via the reset button, ensuring that the process is controlled and no unauthorized access can occur until the system is manually reset.

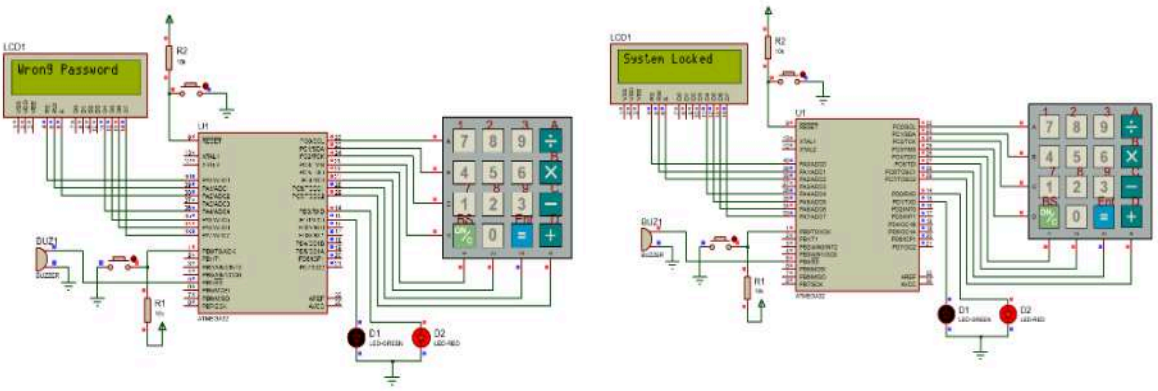

Fig: Admin password setup (simulation)

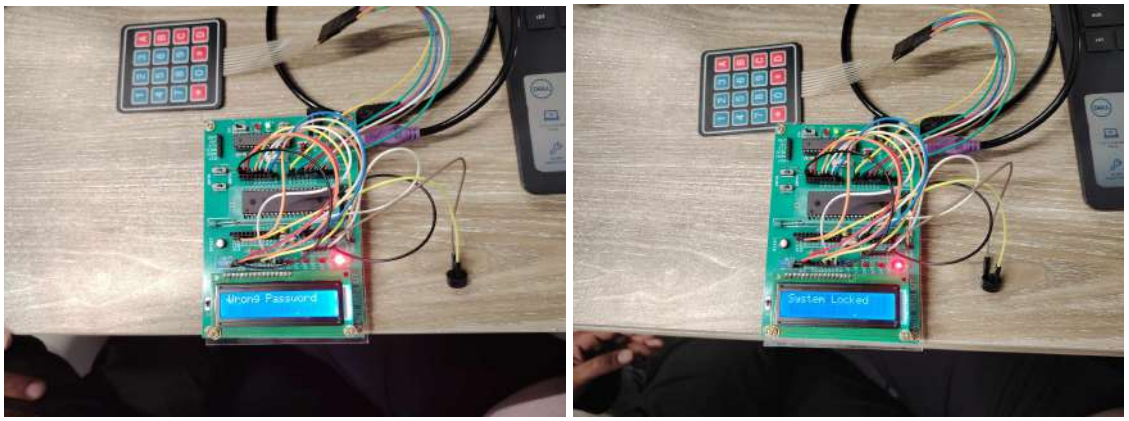

Fig: Admin password setup (Hardware Representation)

The system operates through three key scenarios: normal access, multiple failed attempts, and admin mode for password reset, each playing a vital role in maintaining security and functionality. In the normal access case, the system validates the correct password, granting access and displaying a success message. In the event of multiple failed attempts, the anti-theft mechanism locks the system and triggers an alert to prevent unauthorized access. The admin mode for password reset allows authorized users to update the password for future access. Together, these cases create a secure environment, balancing user convenience with robust protection against unauthorized access.

X.Applications

The password security system with an anti-theft system offers a versatile and scalable solution for security. In residential settings, it can be used to enhance safety by controlling doors, gates, and safes. This makes it ideal and suitable for homes, offices, and personal lockers. From a commercial and office usage point of view, it can be used to secure official spaces, server rooms, and employee lockers. This system can also be used with educational institutions by providing controlled access to labs, examination rooms, and admin areas. Moreover, healthcare facilities can benefit from establishing the ability to restrict access to pharmaceutical storage, equipment storage rooms, inventory storage rooms, and critical areas like ICUs, which are prone to biohazard,s where specific biosafety protocol following personnel is needed. Furthermore, this system can also be used in

financial institutions, protecting vaults and confidential records. Lastly, the system can seamlessly integrate with smart home ecosystems and potential IOT applications like remote monitoring and response. To sum up, the system can be applied in various security-prone environments seamlessly.

XI. Future scope

Future Work and Alternatives:

The future work for this project involves enhancing its efficiency, stability, and usability. One of them is to improve code design by implementing state machines or modular models, which in turn makes the system scaleable and easy to maintain. Possible ways of avoiding the current keypad system are the use of an RFID-based security system, in which RFID tags will operate as contactless keys and will be more convenient. In general, to achieve the best security and convenience, a new type of security system that integrates passwords and RFID tags can be designed. To enhance the full features of the system one more identification step could be made by connecting the IoT system to a Wi-Fi module like ESP8266/ESP32 for remote monitoring and control. It could allow such things as notifying, for instance, by an SMS or an application alert, during failed tries or unauthorized access. Other features like incorporating a camera module to take pictures or record videos at any point in time that is considered risky may also be incorporated to boost security. The gathered information can be saved in the system or a cloud space for further analysis and enhances the concept of the safety system.

The project can also benefit from usability enhancements and broader functionality. Adding voice assistance would guide users during operations, improving accessibility for diverse user groups. Conducting user testing is essential to gather feedback and iterate on the design to improve its reliability and ease of use. Cross-linkage with other existing solutions can reveal functional deficits and potential for improvement. Real system tests, for instance, response time measurement for unlocking or buzzer activation time after a series of incorrect attempts are sure to put the system to its best performance. More extended durability testing is to be conducted on the individual components to substantiate this endurance. Additional features that could be incorporated include an elf-checking ability that tells users of other hardware failures like a bad buzzer or an LCD. Concerns related to society and culture can be solved by expanding the language support interface to include multiple languages on the LCD. Ethical issues should also be met by making sure that password as well as other user information is well protected from anyone who may try to steal it. Last but not least, we can reach the concept of environmental sustainability by integrating low-power, energy-efficient components making the system ideal for battery-powered systems and minimizing the environmental effects on the new system.

XII. References

1. Sari, R. F., & Wibowo, S. (2023). The Keypad Passcode Design Analysis on Smart Lock Door System IoT Based. *International Journal of Advanced Computer Science and Applications*, 14(5), 123-130.
   ResearchGate

XIII. Appendices

A. Source code

```
#include <mega32.h>
#include <delay.h>
#include <alcd.h>
#include <string.h>
#define keypad_ddr DDRC
#define keypad_port PORTC
#define input_data PINC
#define new_password_button PINB.0
#define buzzer_pin PORTB.4
char *str;
int duration;

char password[9] = "21321007";
char admin_password[5] = "1234";
char input[9];
int input_index = 0;
int attempt_count = 0;
int reset_mode = 0;
int admin_mode = 0;

void clear_input()
{
int i;
for (i = 0; i < 9; i++)
{
input[i] = '\0';
}
input_index = 0;
}

void lcd_display()
{
lcd_clear();
lcd_puts(str);
delay_ms(1000);
```

```
}

void lcd_display_message()
{
lcd_clear();
lcd_puts(str);
delay_ms(duration);
}

char scan_keypad()
{
    keypad_port = 0b11101111; // First row
    if (input_data.0 == 0) return 'A';
    if (input_data.1 == 0) return '4';
    if (input_data.2 == 0) return '7';
    if (input_data.3 == 0) return '*';

    keypad_port = 0b11011111; // Second row
    if (input_data.0 == 0) return '1';
    if (input_data.1 == 0) return '5';
    if (input_data.2 == 0) return '8';
    if (input_data.3 == 0) return '0';

    keypad_port = 0b10111111; // Third row
    if (input_data.0 == 0) return '2';
    if (input_data.1 == 0) return '6';
    if (input_data.2 == 0) return '9';
    if (input_data.3 == 0) return '#';

    keypad_port = 0b01111111; // Fourth row
    if (input_data.0 == 0) return '3';
    if (input_data.1 == 0) return 'B';
    if (input_data.2 == 0) return 'C';
    if (input_data.3 == 0) return 'D';

    return '\0'; // No key pressed
}

void main(void)
{
int i;
keypad_ddr = 0xF0;
DDRB.0 = 0;
DDRB.4 = 1;
DDRD = 0xFF;
lcd_init(16);
```

```
clear_input();
lcd_display_message("Enter Password", 1000);

while (1)
{
char key = scan_keypad();
PORTD = 0b00000001;

if (new_password_button == 0)
{
if (!admin_mode) {
lcd_display("Enter Admin Pass");
clear_input();
admin_mode = 1;
}
delay_ms(200);
}
if (key != '\0')
{
if (key == '*')
{
if (input_index > 0)
{
input_index--;
input[input_index] = '\0';
lcd_gotoxy(input_index, 1);
lcd_putchar(' ');
lcd_gotoxy(input_index, 1);
}
} else if (key == '#')
{
if (admin_mode) {
if (strcmp(input, admin_password) == 0)
{
lcd_display("Admin Verified");
admin_mode = 0;
reset_mode = 1;
lcd_display("Enter New Pass");
} else {
lcd_display("Wrong Admin Pass");
admin_mode = 0;
}
clear_input();
} else if (reset_mode)
{
```

```
for (i = 0; i < input_index; i++)
{
password[i] = input[i];
}
password[input_index] = '\0';
reset_mode = 0;
lcd_display("Password Set");
lcd_display_message("Enter Password", 1000);
} else
{
if (strcmp(input, password) == 0)
{
lcd_display("Access Granted");
attempt_count = 0;
PORTD = 0b00000010;
delay_ms(5000);
lcd_display_message("Enter Password", 1000);
} else {
attempt_count++;
if (attempt_count >= 3)
{
lcd_display("System Locked");
PORTB.4 = 1;

while (1);
} else {
lcd_display_message("Wrong Password", 1000);
lcd_display_message("Enter Password", 1000);
}
}
}
clear_input();
} else {
if (input_index < 8)
{
input[input_index++] = key;


lcd_gotoxy(input_index - 1, 1);
lcd_putchar(key);
delay_ms(500);


lcd_gotoxy(input_index - 1, 1);
lcd_putchar('*');
}
```

```
}
delay_ms(200);
}
}
}
```

B. Google Drive link (of the hex file and schematic): ***https://drive.google.com/drive/folders/1VWKaZDLxmyMerMATFMsup-S1Vr7UMLkP?usp=sharing***