Android Based Double Authentication Security System

A.Santhosh Kumar
Santhosh.allenki@gmail.com
ECE Department, Guru Nanak Institute of Technology,Hyderabad

Pallavi Pasunoti
ppasunoti@gmail.com
ECE Department, Guru Nanak Institute of Technology,Hyderabad

Onteru Aishwarya
onteruaishwarya036@gmail.com
ECE Department, Guru Nanak Institute of Technology,Hyderabad

Lavudya Ranjeeth Raj
Akashchowhan1410@gmail.com
ECE Department, Guru Nanak Institute of Technology,Hyderabad

Abstract— **This project focuses on creating a secure access control system using double authentication through an Android-based application and embedded hardware. Traditional door locking systems are vulnerable as they rely on a single control method. In this system, the first level of authentication is done by sending a password from an Android app to the door system via Bluetooth using the HC-05 module.**

Once the primary password is successfully verified by the Arduino microcontroller, the system prompts for a second level of authentication. This involves entering a one-time password (OTP) using a 1x4 keypad. Only when both the Android password and the keypad input are correct does the system allow access, which is indicated by a servo motor unlocking the door.

The system components include Arduino Uno, Bluetooth module HC-05, servo motor, keypad, and a 16x2 LCD display. This double authentication method offers enhanced security and is suitable for homes, offices, and restricted areas.

Keywords—Double-authentication,Android Application, Bluetooth HC-05, Secure Door Lock System

I. INTRODUCTION

In today's world, security has become a major concern in both residential and commercial spaces. Traditional door locking systems are often manually operated and lack advanced protection against unauthorized access. This creates a need for improved systems that provide better security through modern technology. An effective solution is to implement access control systems that combine software and hardware-based authentication methods.

This project introduces a double authentication security system that uses an Android application and a keypad to control door access. The first level of authentication requires the user to send a password through a mobile app over Bluetooth. If the password is correct, the system proceeds to the second level, where the user must enter an OTP (One-Time Password) using a keypad. Only when both credentials are validated will the door be unlocked.

The system is built using an Arduino Uno microcontroller, which controls the entire process. A Bluetooth module (HC-05) handles wireless communication with the mobile app, and a 1x4 keypad is used for manual password input. A servo motor acts as the locking mechanism, and a 16x2 LCD display shows system status such as "Access Granted" or "Wrong Password." This setup ensures both user convenience and enhanced security.
By combining wireless and physical authentication, this system offers better protection against unauthorized entry. Even if one level of security is compromised, the second layer acts as a safeguard. This makes the solution ideal for secure applications such as homes, office cabins, lockers, and server rooms where security is critical.

II. EXISTING SYSTEM

The existing door security systems typically rely on single-level authentication methods such as keys, RFID cards, or keypad-based passwords. While these systems offer basic access control, they are vulnerable to security breaches if a key is lost, a password is guessed, or a mobile device is compromised. Most of these systems lack a second verification step, making it easier for unauthorized individuals to gain access. Additionally, they often do not provide real-time feedback or user authentication logs, which limits their effectiveness in high-security applications. This highlights the need for a more advanced and reliable system with dual authentication.

III. PROPOSED SYSTEM

The proposed system introduces a double authentication mechanism to enhance door security using both a mobile application and a keypad. In this system, the user first sends a password from an Android app via Bluetooth (HC-05) to the Arduino-based control unit. If the password is correct, a one-time password (OTP) is generated and must be entered through a keypad for the second level of authentication. Only after both passwords are validated does the system activate a servo motor to unlock the door. This method adds a strong layer of security, reducing the risk of unauthorized access even if one password is compromised. The integration of hardware components like the Arduino, LCD, Bluetooth module, keypad, and servo DT11 sensor motor ensures reliable performance and user interaction.

Ultimately, this combination of wireless convenience and hardware-based verification offers a more robust solution for access control.

IV. METHODOLOGY

The Android-based double authentication security system works by combining wireless and manual input methods to ensure secure access. The process begins with the user sending a primary password through an Android application. This password is transmitted via Bluetooth using the HC-05 module to the Arduino microcontroller, which acts as the brain of the system. The Bluetooth communication allows for wireless control, eliminating the need for physical keys or remote controllers.

Once the primary password is received, the Arduino checks its validity. If the password is correct, the system proceeds to the second stage of authentication. At this point, a randomly generated OTP (One-Time Password) is displayed on the Android application. The user is required to enter this OTP using a 1x4 keypad connected to the system. This secondary step ensures that even if someone gains access to the mobile app, they still cannot unlock the door without the correct OTP.

If the OTP entered through the keypad matches the one sent by the system, the Arduino sends a signal to the servo motor to unlock the door. The system also provides real-time feedback on a 16x2 LCD display, showing messages such as "Access Granted" or "Wrong Password." This immediate feedback improves user experience and makes the system more interactive and transparent.

The combination of these technologies—Bluetooth for wireless communication, keypad for manual input, and LCD for display—ensures that the system is secure, user-friendly, and reliable. The use of Arduino simplifies hardware control, while the double-layered authentication minimizes the chances of unauthorized access, making it suitable for use in homes, offices, and restricted zones.

The security system's methodology is centered on a dual-layer authentication process, combining the convenience of an Android application with the added security of a physical keypad.

This combination of software and hardware-based authentication aims to provide a more robust security solution than relying on a single method.

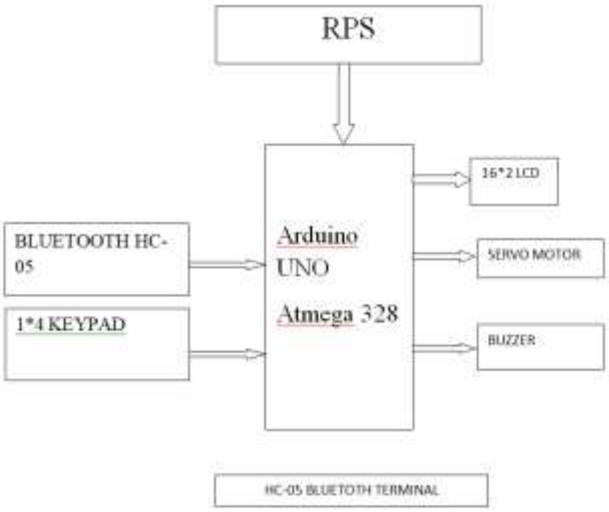

FIG 1 Block Diagram of Proposed System

Applications

Home Security: Smart locks with 2FA are used in residential homes, where users unlock the door using a password or PIN along with an OTP or biometric scan for added security.

Office Buildings: Many office buildings use 2FA for secure entry, where employees swipe a key card or use a fingerprint, followed by a PIN or passcode for double authentication.

Hotels: Some hotels use 2FA for room access, where guests enter a code or use a mobile app and then confirm with a secondary authentication method like an OTP or fingerprint.

Smart Apartments: In apartment complexes, residents may use 2FA to enter common areas or individual units, combining a keycard or mobile app with additional authentication.

Secure Facilities: Government or military facilities use 2FA to restrict access, requiring both physical keys and biometrics for entry.

Garage Door Openers: Some advanced garage door systems use 2FA, where users need a mobile app and a PIN or password to open the door remotely.

V. HARDWARE DETAILS

Arduino Uno:

The Arduino/Genuino Uno is a microcontroller board featuring the ATmega328P. It provides 14 digital input/output pins (6 of which can function as PWM outputs), 6 analog inputs, a 16 MHz quartz crystal, a USB connection, a power jack, an ICSP header, and a reset button. This board includes all the necessary components to support the microcontroller, allowing it to be easily connected to a computer via a USB cable or powered by an AC-to-DC adapter or battery.

ATmega328P Microcontroller:

The ATmega328P is a high-performance, low-power 8-bit AVR RISC-based microcontroller. It integrates 32KB of ISP flash memory with read-while-write capabilities, 1024B of EEPROM, 2KB of SRAM, 23 general-purpose I/O lines, 32 general-purpose working registers, flexible timer/counters, internal and external interrupts, a serial programmable USART, a 2-wire serial interface, an SPI serial port, a 10-bit A/D converter, a programmable watchdog timer, and power-saving modes. The microcontroller operates between 1.8-5.5 volts and achieves high throughput by executing powerful instructions in a single clock cycle.

Bluetooth Module (HC-05):

While the document provides general information about Bluetooth, it doesn't give a detailed paragraph specifically about the HC-05. The document mentions that the project includes a Bluetooth (HC-05) module, which is connected to the Arduino through a UART interface.

Servo Motor:

A servomotor is a rotary or linear actuator that allows for precise control of angular or linear position, velocity, and acceleration[cite: 325]. It consists of a motor coupled to a position feedback sensor and requires a sophisticated controller. Servomotors are employed in applications like robotics, CNC machinery, and automated manufacturing.

Keypad:

The document describes a 4x3 matrix keypad connected to the Arduino digital pins. Matrix keypads are interfaced by connecting both ends of the switches to the port pin, using the microcontroller to provide the ground. By pulling one column pin low and checking the row pins, the system can determine which switch is pressed.

Power Supply:

The power supply section provides +5V for the system components, using an IC LM7805 voltage regulator. It typically involves a transformer to step down the AC voltage, a diode rectifier to convert AC to DC, a capacitor filter for smoothing, and a regulator circuit to remove ripples and maintain a stable DC voltage.

VI. SOFTWARE DETAILS

The Android-based double authentication security system relies on specific software tools and languages. Firstly, the Arduino IDE (Integrated Development Environment) is essential as the platform for writing and compiling the code that will be uploaded to the Arduino microcontroller. Secondly, Embedded C language is the programming language used to instruct the Arduino to perform its functions, such as processing input from the keypad and controlling the servo motor. Lastly, while not extensively detailed in this document, an Android application is a necessary component of the system to handle the primary password authentication.

Arduino IDE:

The Arduino IDE is a software application that provides the tools necessary to create and manage Arduino programs, or "sketches". It features a text editor for writing code, a message area to display feedback and errors, a console for output, and a toolbar with convenient buttons for common actions like verifying, uploading, saving, and opening sketches. The Arduino IDE simplifies the process of programming the Arduino board, allowing developers to write code, check for errors, and upload the program to the microcontroller.

Embedded C:

Embedded C is the programming language at the heart of the Arduino's functionality within this security system. It's used to precisely control the Arduino's hardware components and define the system's behavior. Through Embedded C, developers instruct the microcontroller how to interact with the Bluetooth module, servo motor, and keypad, enabling it to manage password authentication, door control, and communication protocols. This language allows for direct manipulation of the microcontroller's registers and memory, which is crucial for embedded systems where resource efficiency and real-time performance are often critical.

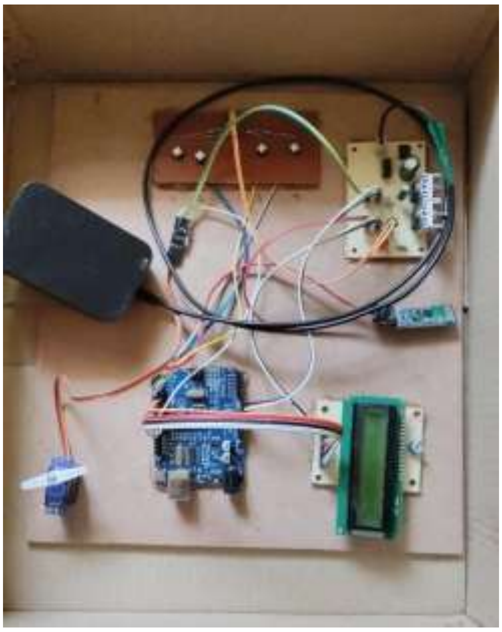

FIG 3 Prototype of Proposed System

VII. CONCLUSION

The prototype is the initial step in creating a two-factor authentication (2FA) system, allowing developers to demonstrate the functionality and usability of the system. By creating a working model, it's easier to test and refine how both factors (something you know and something you have) work together to ensure security. This stage also helps in identifying potential vulnerabilities and optimizing the user experience before full-scale implementation.

Next, moreover, the implementation of 2FA significantly strengthens security by requiring more than just a password. This added layer, whether it's an OTP, a biometric scan, or a physical device, makes it much more difficult for attackers to bypass. Even if a password is compromised, the second factor serves as an additional barrier, ensuring that only authorized users can gain access.

In conclusion, 2FA systems offer a proven solution to increasing security across various platforms, from banking apps to workplace systems. The prototype serves as the foundation for developing a secure, user-friendly authentication system, ensuring that sensitive data is well-protected. With the continuous rise in cybersecurity threats, adopting and refining 2FA will remain crucial in safeguarding personal, financial, and organizational information.

ACKNOWLEDGEMENT

This project stands as a testament to the unwavering support and invaluable contributions of numerous individuals, without whom its fruition would not have been possible. We extend our heartfelt gratitude to the mentors, educators, and technical experts whose guidance and assistance have been instrumental in transforming our vision into reality.

First and foremost, we express our profound appreciation to Mr.A.Santhosh Kumar, Assistant Professor in the Department of Electronics and Communication Engineering, whose unwavering guidance has been pivotal throughout the course of this dissertation.

We are immensely grateful to G.Praveena Reddy, Project Coordinator, and our entire faculty for their ceaseless encouragement and unwavering support, which have served as the driving force behind the completion of this project.

Our sincere thanks extend to Dr. S. P. Yadav, Head of the Department of Electronics and Communication Engineering, whose invaluable suggestions have greatly contributed to the success of this endeavor, serving as a constant source of inspiration.

We also extend our gratitude to Dr.K.Venkata Rao, Principal, for his continuous support and valuable guidance throughout this journey.
We acknowledge with deep appreciation the support and encouragement received from Dr. H.S. Saini, Managing Director of Guru Nanak Group of Institutions, whose unwavering belief in our abilities has been a source of motivation.

Additionally, we express our gratitude to our parents, friends, and all those who have provided encouragement and support along the way. Their belief in us has been a driving force behind our efforts.

Lastly, we extend our thanks to all other staff members, both teaching and non-teaching, for their timely assistance and contributions, which have facilitated the progress of this project.

REFERENCES

IEEE Xplore – Search for papers on **Bluetooth-based authentication systems** and **secure access control**.
Springer Link – Look for research articles on **IoT-based security systems** using Bluetooth modules.
ScienceDirect – Contains studies on **embedded security systems** and **wireless authentication**.
Example Paper:
"Bluetooth-Based Smart Lock System with Multi-Factor Authentication" – Discusses authentication using Bluetooth and a secondary security layer.

2. Books & Learning Resources
“Arduino and Bluetooth HC-05 for Beginners” – Covers interfacing HC-05 with microcontrollers.
“Android App Development for Security Systems” – Provides insights on developing Android applications for authentication.
“Wireless Security and Privacy” – Explains security vulnerabilities in Bluetooth communication.

3. Online Tutorials & Documentation
HC-05 Bluetooth Module Guide (Arduino Official Documentation)
MIT App Inventor for Bluetooth Apps (MIT App Inventor)
Arduino Forum Discussions (Arduino Forum) – Look for real-world implementations of Bluetooth-based security systems.