DESIGN AND DEVELOPMENT OF A PASSWORD-PROTECTED SMART WIRELESS LOCKING SYSTEM USING IDE ENVIRONMENT AND IOT ANALYSIS

[1]Sowmya Chowdar Y Malinidi, [2]Bhagya Lakshmi Medaka,[3]Ganga Sukanya Mallela, [4]Gopalam Asritha

[1,2,3]Assistant Professor, [4]UG Student, [1,2,3,4]Department of Electronics and Communication Engineering, Rishi MS Institute of Engineering and Technlogy for Women, Kukatpally, Hyderabad.

ABSTRACT

This project recommends employing an OTP (On Time Password) based Bluetooth-enabled digital wireless locking mechanism to increase security. We generate a different password each time we try to access the locker system. To avoid security problems in this situation, a DIY smart lock mechanism must be used, and an app must be created to control the switch mechanism. The programme was developed using MIT App Inventor (a web application), and coding blocks were used to initialise the Bluetooth list so that it could connect to the proper smart phone. Here, an Arduino UNO (microcontroller board based on the ATmega328P) is being used, and it functions in line with a programme made in the Arduino IDE (Integrated Development Environment). The Arduino should upload the code since the programming language is comparable to C. The app fragment consists of a lock icon, a Bluetooth icon, and a key icon. When we connect Bluetooth (Hc05) and press the lock icon, the device ID is sent to the circuit. If the ID matches the ID initialized in the Arduino code, the OTP loop is triggered. After successfully mapping the OTP, unlock the lock by pressing the key icon. This is indicated by a lit LED light. This is an IOT (Internet of Things) based application that keeps sensitive data safe and avoids risks from internal and third-party sources.

Keywords*:* OTP (On Time Password), DIY (Do It Yourself), MIT App Inventor (Web Application), Bluetooth Hc-05, IOT (Internet of Things), IDE (Integrated Development Environment), USB (Universal Serial Bus).

1. INTRODUCTION

A worldwide information network made up of "things" like smart devices, sensors, and actuators, or even smaller networks with their own identities and the ability to self-configure within a given range, is what is referred to as the Internet of Things (IoT) the ability to decide for themselves, either individually or collectively. A future, in which everything and everyone will be connected to the internet through whatever device they own, be it a computer, smartphone, or other consumer item, is heralded by the development of the Internet of Things. IoT network objects may also connect with one another via a variety of technologies, including WiFi, Bluetooth, near field communication, and more.

One of the most common uses of IoT technology is to support smart home systems. Newer smart home systems are a good model for how IoT architectures behave, as objects in a house are wirelessly connected to gateways to communicate with each other and the occupants of the house. Since smart home systems are designed to improve the comfortable quality of life for residents, using IoT can at least make it easier to control and monitor household appliances.

Smart home systems can be classified into at least one type according to their function: healthcare, entertainment, energy and/or security. Among these characteristics, security becomes one of the most important factors when installing the system. Improve safety in your home A smart home can be accomplished in a number of ways, including but not limited to installing smart custom door locks. There have been several examples of smart door lock implementations such as: B. Camera based access control systems, passwords, smart cards and proximity or location detection. Each of the above methods has advantages and disadvantages, such as: B. Interoperability score of the device.

In this study, a Bluetooth-based smart door lock was designed. The ultimate goal of this research is to develop a door lock system that requires no manual user input, is convenient and secure. However, the scope of this paper is limited to exploring the feasibility of using Bluetooth for location-based locking to achieve the above goals. Furthermore, the scope of this document is mainly limited to the lock hardware aspect, and only briefly describes the server and Android application code that handles Bluetooth tracking. This device is part of a smart home system we designed, which also includes Arduino UNO, Servo Motor, Breadboard, Resistor, LED, MIT App Inventor, Bluetooth HC05, Jumper Wire, HIW Battery.
The smart home is controlled through an Android-based app, as described. This document describes the design and implementation of smart locks and test results.This paper is divided into the following parts: The first part introduces the research background. Section II discusses the methodology, including: prominent research limitations, developed system specifications, hardware, system workflow, protocol design, Android, and servers. Section III reports the research results, while research findings and future work are reported in Sections IV and V, respectively.

2. SYSTEMDESIGN

2.1 Research Limitation:

This work focuses more on Hardware section, including defined circuit blocks, electronicsCircuits and their assembly, including software parts-flowcharts, Android applications and show Bluetooth serverBrief, later will be developed in detail for others publications. This test borders on the functional test as the motor moves in the locked and unlocked state of the door.

2.2System Specification:

Since the designed system is part of an MIT application, it is a web application. The application is developed using two-tab designers and blocks. By using the designer panel, we can draw symbols such as Bluetooth, key and lock icons separately, and use the block panel to write block coding. For hardware design, let's take the Arduino Uno as an example, an open-source microcontroller board with 6 analog pins and 14 digital I/O pins. It has an ATmega328p chip that stores data. The HC-05 Bluetooth module has 6 pins - EN, VCC, GND,TX, RX and status. HC-05 Bluetooth module can use in master or slave configuration, making it a great configuration Wireless Communication Solutions. The servo motor has three pins, namely VCC, GND, and control pins, which obey the servo mechanism.

Fig. 1: Servo Motor Fig. 2: Bluetooth HC05

Fig. 3: Arduino UNO

Fig. 4: MIT App Inventor

2.3 Hardware Design

In the Bluetooth HC05, the VCC and GND pins are connected to the +ve and -ve terminals of the 9V HIW battery, and the GND pin is shorted to the Arduino board's GND pin. And the TX and RX pins are reverse connected to the RX and TX pins of the Arduino Uno board. In the servo motor, the PWM pin is connected to the 9th pin of the Arduino board, the VCC pin is connected to the 5V in the board, and the GND pin connected to the GND pin of the Arduino board. The anode of the LED is connected to pin 12 of the board through a 1 k Ohm resistor, and the cathode is shorted to GND of the board.

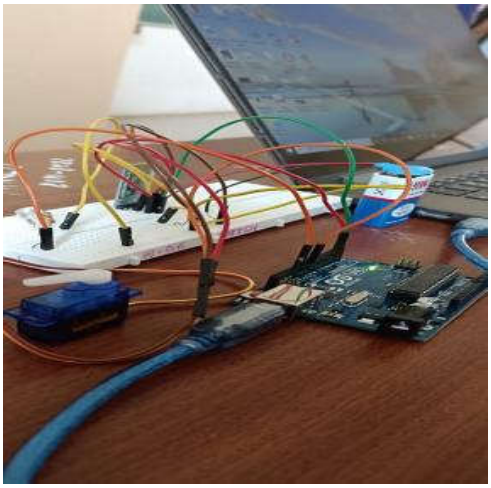


Fig. 4: Hardware Design

2.4 System Workflow

This section provides the work flow of the entire process in the fig. In this flow chart every step is explained and the order is also explained accordingly.

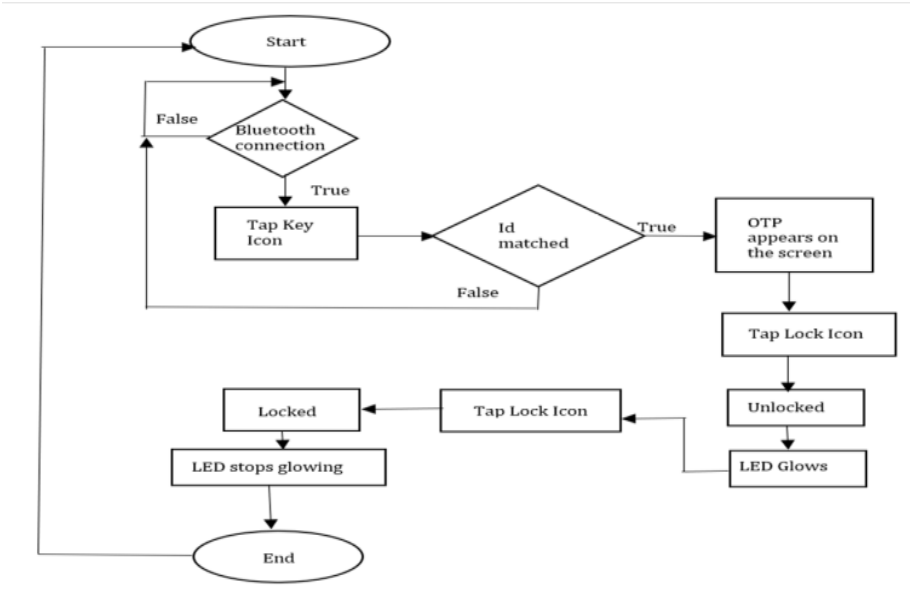


Fig. 5: Flow Diagram of OTP based smart wireless locking system.

2.5 Android Application

The door lock works by having the Android App ,which is the user interface for
the entire system, periodically collect the information about the Bluetooth clients present within the range. The list picker picks the desired client and establish connection. The app layout consists of three icons namely Bluetooth, key, lock. Text labels are placed next to Bluetooth icon and lock icon to avoid confusion. All these are achieved with the help of MIT App inventor.

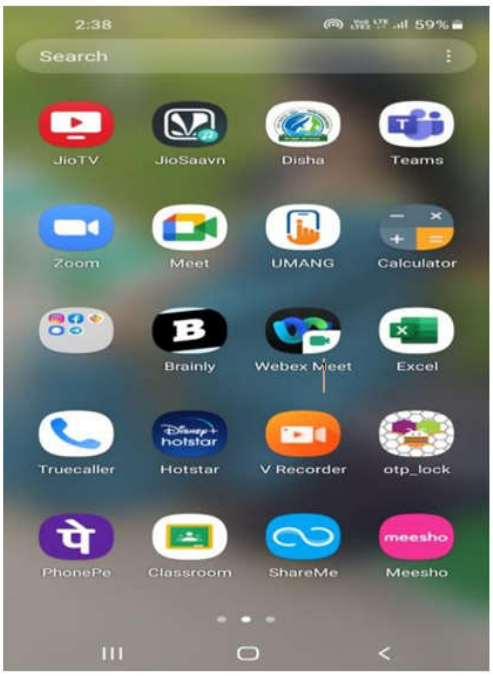


Fig. 6: Otp_lock icon is the Android App.

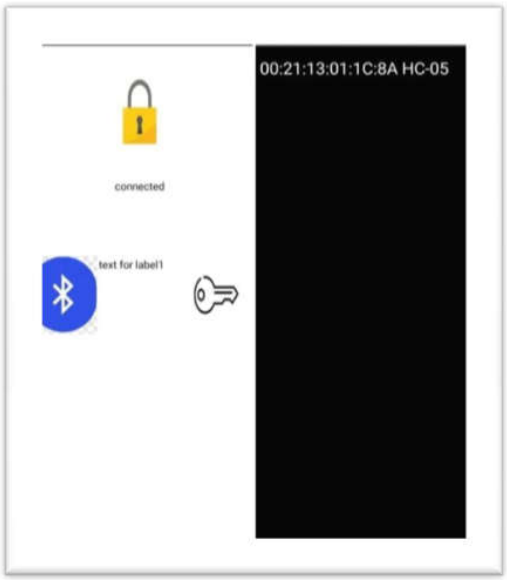


Fig. 7: Android App for OTP based smart wireless locking system.

3. RESULTS AND DISCUSSION

3.1 Implementation

Based on the block diagram from fig. 2 the system works.

The block diagram shows the system connections, the main part is the Arduino UNO, which is the microcontroller. The code is thrown into the Arduino UNO.

When powered, the Bluetooth module is activated and communicates with the app. After the Bluetooth connection is successful, start the execution.

When a button is pressed in the application, an OTP is generated if the standard code in the application matches the code in the Arduino UNO.

Press the lock icon to unlock the door lock through the counterclockwise rotation of the servo motor, and the LED light will turn on at the same time, indicating that the lock has been opened. Also, to lock, press the lock icon again, the LED will stop glowing and the servo motor will rotate clockwise.

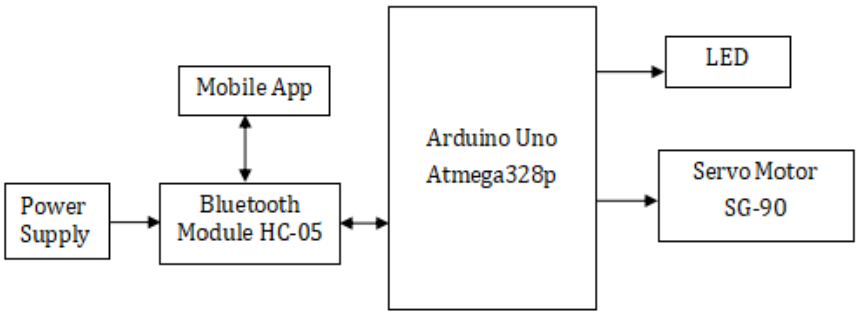


Fig. 8: Block Diagram of OTP Based Smart Wireless Locking System.

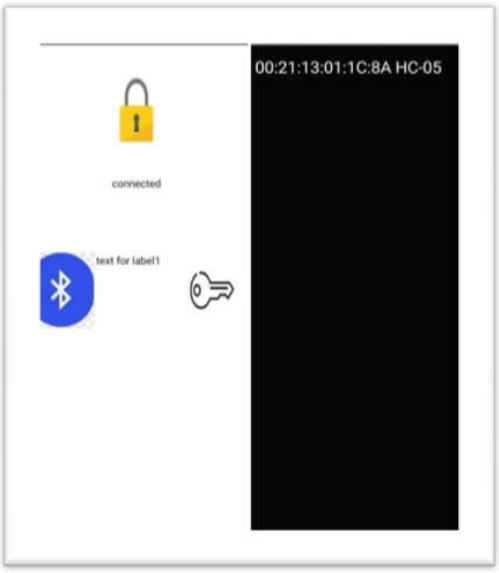
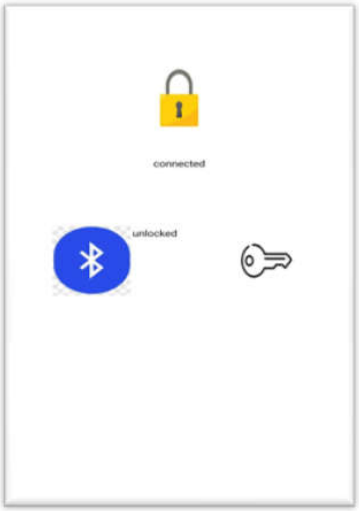
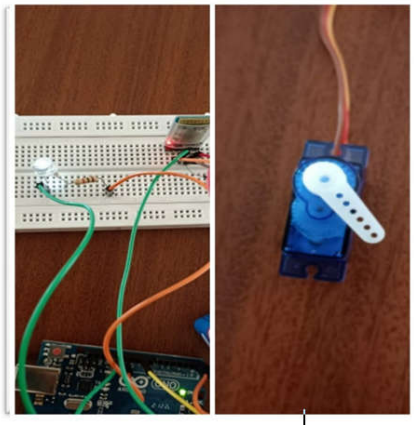


Fig. 9: The OTP appearance in the app.

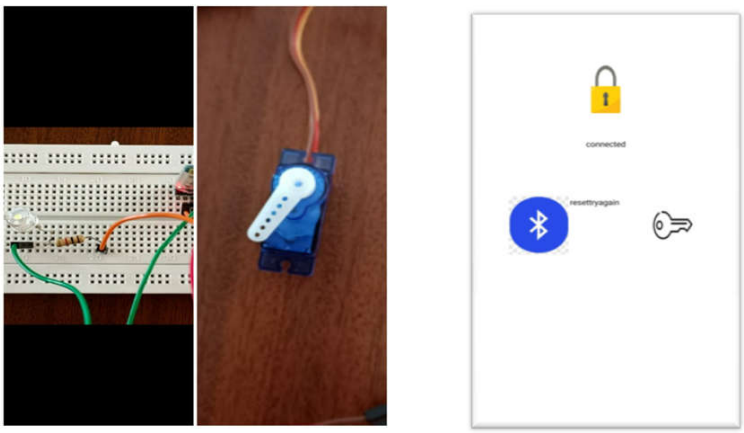


(a)



(b)

Fig. 10: a and b represent the unlocking results.



(c) (d)

Fig. 11: c and d represent the locking results.

3.2 Functional Test

The system was tested with the help of servo motors. When the Bluetooth module is turned on at 9600bps baud rate (set using Arduino encoding), it will connect to our android Bluetooth within that range. Based on the observations (pedal movement of the servo motor and LED light on), the developed door lock system works fine. It can lock and unlock intelligently

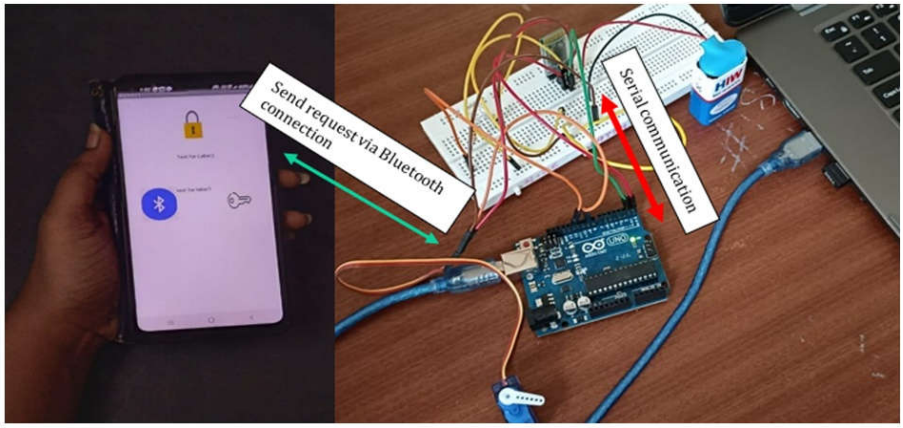


Fig. 9. Functional testing for the OTP Based Door Lock System

CONCLUSION

This article describes the construction of an OTP-based smart door lock prototype that is controlled by Bluetooth. The technology makes use of an Android app on the user's smartphone. This programmed is used to transmit commands to the main circuit and to receive answers. The door lock may be operated by pairing with the Android app through Bluetooth, according to the test findings. More study is still needed to improve system quality, reinforce the locking mechanism, and increase the security of Android apps. If we integrate the Android APP with security features like fingerprints and passwords, we can create a secure smart lock system in the next stage of development.

FUTURE SCOPE

In the next stage of work, if we use the Android APP to interface with security such as fingerprints and passwords, we can achieve the effect of providing a secure smart lock system.

REFERENCES

1. Pooja K M, Chandrakala K G , Nikhitha M A, Anushree P N " Finger Print Based BankLocker Security System", International Journal of Engineering Research &Technology(IJERT),Issue -2018.
2. Md. Maksudur Rahman1, Dr. Mohammed Sowket Ali & Md.Shoaib Akther "PasswordProtected Electronic Lock System for Smart Home Security" International Journal of Engineering Research & Technology (IJERT) Vol. 7 Issue 04, April-2018.
3. Nepal case study-https://www.researchgate.net/figure/Nepal-Bulgary-rate-per-100-000populationUNODC2015_fig1356785
4. Base Paper 2018 , GSM based Technology- https://www.researchgate.net/publication/333514568_IoT-Enabled Door Lock System.
5. A-Novel-Behavioural-Biometric-based-Authentication-Scheme-for-Smart-Lock-Systems-https://dl.acm.org/doi/abs//10.1145/3345336.3345344
6. A smart lock system using WIFI security https://ieeexplore.ieee.org/document/7560143.
7. Design of Smart Lock System for Doors with Special Features using Bluetooth Technologyhttps://ieeexplore.ieee.org/document/8350767
8. Y.C. Yu, "A Practical Digital Door Lock for Smart Home", Proc. of the IEEE Int. Conf. on Consumer Electronics (ICCE), pp. 1-2, 2018.
9. S. Jensen, "Proximity Door Locking", Master Thesis, Technical University of Denmark.
10. T. Adiono, M.Y. Fathany, S.F. Anindya, S. Fuada, and I.G. Purwanda, "Wirelessly Control for RGB Lamp End-Device: Design andImplementation,"IEEE Region 10 Conf. (TENCON), pp. 2066-2070, October
11. Adiono, S.F. Anindya, S. Fuada, and M.Y. Fathany, "Curtain Control Systems Development on Mesh Wireless Network of the Smart Home," Bulletin of Electrical Engineering and Informatics (BEEI), Vol. 7, No. 4, pp. 615-625, December 2018.