IJARST
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

WIRELESS BIOMETRIC LOCK USING NODEMCU WITH THE IOT

P.VISAWA SANTHI[1], KONDAPALLI SAI PRAVEEN[2], VATTIKUTI AMRUTHA[3], KAMADI ANITHA[4], TELUKUTLA VENKATESH[5], C V V SATYANARAYANA[6]
[1]Assitant Professor, Dept. of ECE, PRAGATI ENGINEERING COLLEGE
[23456]UG Students, Dept. of ECE, PRAGATI ENGINEERING COLLEGE

ABSTRACT

Security has reliably been a huge stress for the families and the working environment condition, and for this concern various techniques are set up to address the issue. Most of the huge doorway locks security structures have a couple of departure statements that could be isolated to get to the best spots, and it makes a concern for a secured lifestyle and real working environment.

Smart home security plays a significant job which makes a difference to give better security in home application. The proposed project ‘IOT BASED WIRELESS BIOMETRIC LOCK USING NODEMCU’ is to convey a message to the door from a tablet or mobile device by using a Bluetooth system. This permits the individual to lock and open an entryway from inside or outside a house with a Bluetooth gadget accessible. The ideal motivation behind the work is in case the entryway isn't locked on the primary floor or some other floor, the client from the beginning can open the entryway or open the entryway from a cell phone or PC, which causes an individual to lessen its energy or save time. The latest Arduino board, a Solenoid lock or Servo motor, and a Bluetooth module standard protocol for wireless communication are the main components of the system. In order to open or close the door we need to confirm the biometric (Finger print) through our mobile phone app. If it is confirms then the blue-tooth module will receive the information from our phone. The n according to that received data the solenoid lock will be open or lock.

INTRODUCTION

The Internet of Things (IoT) has revolutionized the way we interact with technology and transformed our daily lives. One of the key areas where IoT has made a significant impact is in the field of home security. Traditional lock and key systems have their limitations, and with the advancement in technology, more innovative solutions are now available. In this project, we aim to develop an IoT based wireless biometric lock using NodeMCU that provides enhanced security to homes.

The proposed system is designed to replace traditional lock and key systems with a Bluetooth-based solution that allows users to control the door lock from their mobile device. The system uses biometric authentication to confirm the identity of the user and provide an added layer of security. The solenoid lock is controlled by the NodeMCU, which receives information from the mobile app via Bluetooth.

This project aims to provide users with a convenient and secure way to lock and unlock their doors, reducing the need for physical effort and improving the overall security of their homes. The use of IoT technology in home security systems is a rapidly growing field, and this project aims to contribute to this trend by providing an innovative solution that combines biometric authentication and wireless control to provide enhanced security.

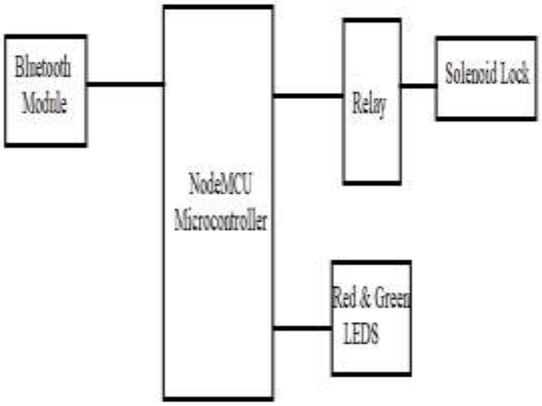

Fig.1: Block Diagram

SCHEMATIC DIAGRAM

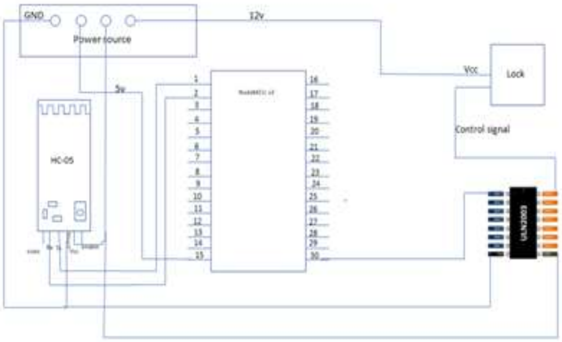

Fig.2: CIRCUIT DIAGRAM

PROPOSED SYSTEM

The system consists of several components, including a biometric sensor, an HC-05 Bluetooth module, a NodeMCU board, a ULN2803A driver chip, and a solenoid lock. The biometric sensor captures the user's fingerprint data and sends it to the HC-05 Bluetooth module over serial communication. The HC-05 module is connected to the NodeMCU board, which receives the fingerprint data and processes it using the code uploaded to the board.

The NodeMCU receives 5v power supply from the power circuit unit to drive the proposed system. The HC-05 Bluetooth module is also powered by the 5v from the power circuit unit. The solenoid lock is powered by 12v source from the power circuit unit.

Connection of HC-05 to Mobile Device

The HC-05 Bluetooth module is first paired with the mobile device by using the default pin ‘1234’ or ‘0000’ . Then the Android application is used to connect to the board by following the below process:

- Open the android application and tap on ‘scan’.
- It shows a list of paired/available nearby devices.
- Tap on the device that in the format: ‘HC-05’.
- Now device asks for your Finger Print ID.
- Place your finger on the finger print senor of the Device.
- The android application sends the authentication data to the Bluetooth module.

Connection of HC-05 to NodeMCU

The HC-05 Bluetooth module is connected to the NodeMCU microcontroller via pins. The RX pin of the HC-05 Bluetooth module is connected to the TX pin of the NodeMCU. The TX pin of the HC-05 Bluetooth module is connected to the RX pin of the NodeMCU micro-controller. The received authentication data from the android application will be sent to the NodeMCU through these pins.

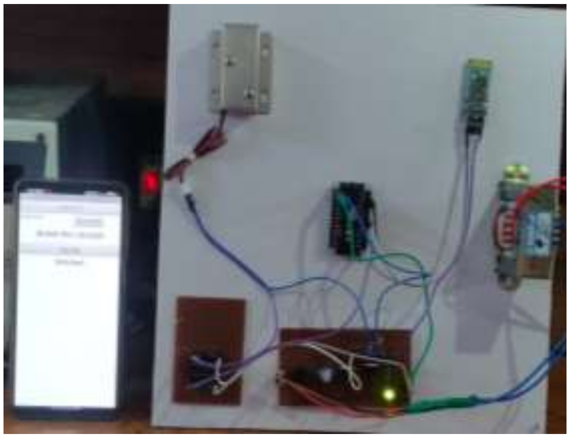

Fig.3: Photocopy Project

Connection of ULN driver to the NodeMCU

The ULN driver is connected to NodeMCU micro-controller on the PIN D1. The received authentication data from the HC-05 Bluetooth module will be verified. If the data is verified, a signal ‘1’ will be sent to the ULN driver through PIN D1. If it is not verified a signal ‘0’ will be sent to the ULN driver through PIN D1.

Connection of ULN driver to Solenoid Lock

The control PIN of the solenoid lock is connected the ULN driver. Based on the signal received from the PIN D1 of the NodeMCU micro-controller. If signal ‘1’ is received the ULN driver sends a signal to the solenoid lock on the control PIN to open the lock. If a signal ‘0’ is received the ULN driver sends a signal to close i.e lock the solenoid lock.

ADVANTAGES

The biometric lock using IoT Node MCU has several advantages, including:

1.Improved Security: The biometric authentication system used in this project is more secure than traditional lock and key systems or even keypad-based systems. Biometric data is unique to each individual, making it difficult to forge or replicate, thus enhancing security.

2.Convenience: The system eliminates the need for keys or passwords, making it convenient for users to access their homes, offices, or other settings. Users can also remotely control the lock and monitor access through the IoT connectivity feature.

3.Cost-effective: The Node MCU board is an affordable and versatile microcontroller board, making the project cost-effective compared to other access control systems.

4.Customizable: The project can be customized to suit specific needs and requirements. The machine learning algorithm can be trained to recognize multiple users, and the lock mechanism can be adapted to work with different types of doors or gates.

5.Future-proof: The project has a promising future scope with potential advancements in technology, as discussed earlier.

APPLICATIONS

1. Home Security: The biometric lock can be used to secure the entry points to a home, providing an added layer of security beyond traditional locks and keys. Homeowners can enroll family members' biometric data and provide access to trusted individuals while restricting access to outsiders. In addition,

the IoT connectivity feature allows remote access control and monitoring of the lock status, which can be particularly useful when homeowners are away from home.

2.Office Security: In a commercial setting, the biometric lock can be used to restrict access to sensitive areas within an office, ensuring that only authorized personnel can enter. For example, the biometric lock can be installed on doors leading to the server room, confidential files storage, or executive offices. User management can be done remotely, granting or revoking access privileges as necessary.

3.Laboratories: In a laboratory setting, the biometric lock can be used to restrict access to hazardous materials or equipment, preventing unauthorized personnel from entering. For example, access to the radiation room, chemical storage, or biohazard labs can be controlled using biometric authentication. The IoT connectivity feature can also be used to monitor the access logs, ensuring that the laboratory is used only by authorized personnel.

4.Hospitals: In a hospital setting, the biometric lock can be used to restrict access to patient rooms, ensuring that only authorized personnel can enter and reducing the risk of infection. Patient data and medical equipment can also be secured using biometric authentication, reducing the risk of data breaches and theft. The IoT connectivity feature can be used to remotely monitor the lock status and access logs, ensuring that the hospital operates securely.

5.Schools: In a school setting, the biometric lock can be used to restrict access to certain areas of the campus, such as the computer lab or administrative offices, ensuring that only authorized personnel can enter. In addition, the biometric lock can be used to control access to the dormitories and campus facilities, improving campus safety and security. User management can be done remotely, enabling school administrators to manage access privileges as necessary.

CONCLUSION

In conclusion, the biometric lock using IoT Node MCU is a secure and convenient way to control physical access to various settings. The project involves capturing biometric data and storing it in a secure database, processing the biometric data using a machine learning algorithm to authenticate users, and controlling the lock/unlock mechanism using the Node MCU board. The project has several potential applications, including home security, office security, laboratories, hospitals, schools, and banks, where physical access control is necessary for safety and security. The IoT connectivity feature of the project allows for remote access control and monitoring, enhancing the system's usability and convenience. Overall, the biometric lock using IoT Node MCU is a reliable and effective solution for physical access control.

FUTURE SCOPE

The biometric lock using IoT Node MCU has a promising future scope with potential advancements in technology.

Here are some future scopes that could enhance the project:

1.Multi-Factor Authentication: The project currently uses biometric authentication as the primary means of access control. However, future iterations of the project could incorporate additional authentication factors, such as passwords or smart cards, to improve the system's security.

2.Cloud Integration: The project currently stores the biometric data on a local database. However, future versions of the project could store the data on a cloud platform, allowing for easier management and scalability.

3.Improved Machine Learning Algorithms: The current machine learning algorithm used for authentication can be further optimized for accuracy and efficiency. The use of more advanced algorithms such as deep learning can improve the accuracy of the system and reduce the false positive rate.

4.Integration with Smart Home Devices: The biometric lock can be integrated with other smart home devices such as security cameras or smart speakers, enhancing the overall home security system.

REFERENCES

1. "NodeMCU Documentation" - Official documentation for NodeMCU, which includes tutorials and examples of how to use the board for IoT projects.
2. "Biometric Security and Privacy: Opportunities & Challenges" - A research paper that discusses the benefits and challenges of using biometric authentication for security purposes.
3. "Internet of Things: Principles and Paradigms" - A book that provides an overview of the Internet of Things (IoT) and its applications.
4. "Python Machine Learning" by Sebastian Raschka and Vahid Mirjalili - A book that covers machine learning techniques using the Python programming language.
5. "Mastering Blockchain" by Imran Bashir - A book that provides an introduction to blockchain technology and its applications.