# International Journal of Engineering Research and Science & Technology

IJERST

ISSN : 2319-5991

www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue 1, 2024

# Unauthorised Area Web Security Notification System Based on Fingerprint and Internet of Things (IOT)

Dr. D. Satyaraj, Mrs. D. Chitra, Ms. C. Sasikala, Dr. L. Vigneash

Associate Professor [4], Assistant Professor [1,2,3]

dsatyaraj@actechnology.in, chitra@actechnology.in, csasikala@actechnology.in, dr.vigneashl@actechnology.in

Department of ECE, Arjun College of Technology, Thamaraikulam, Coimbatore-Pollachi Highway, Coimbatore, Tamilnadu-642 120

## ABSTRACT

The many potential uses of wireless sensor networks (WSNs) have recently piqued the curiosity of many in the academic world. The old wired system has become too complicated and cumbersome to set up, so wireless networking has taken its place. A fundamental need is the necessity for security and control in commercial establishments such as banks, jewellery shops, electronics stores, etc. Extensive coverage, dependability, remote control, and real-time service need modifications to the quickly growing infrastructure. By incorporating wireless technology into security systems, appealing advantages and an intuitive user interface may be realised. This article details the installation of a new security system for the surveillance of financial institutions. Our company locations may be made more safer and more resistant to theft and other criminal acts by using Zigbee network connected security measures. A number of sensors, a microprocessor, a voltage regulator, and Zigbee modules make up this system. Various sensors are set up to detect the surroundings and notify the appropriate parties via the Internet of Things. When the sensors detect anything out of the ordinary, particularly at night, they will communicate with the WiFi module over the Zigbee network. The receiver module will communicate with the owner or another specified recipient once it receives a signal. The simplicity, adaptability, low data rate, low power consumption, and dependability of Zigbee technology make it a popular choice. Also, customers are required to use the biometric sensor by placing their finger on it whenever they enter the store or property. When validated, the NlodeMCU microcontroller's built-in Wi-Fi module will stop the warning signals and update the cloud app with the information given by the user.

## INTRODUCTION

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue 1, 2024

In today's rapidly evolving technological landscape, ensuring the security of physical spaces is paramount. One innovative solution is the integration of fingerprint recognition and the Internet of Things (IoT) in a Wireless Sensor Network (WSN) framework. This project aims to create a robust security alert system for unauthorized areas, leveraging the unique biometric identifier – fingerprints – and the seamless connectivity provided by IoT and WSN.

**The main Objectives are to:**

Develop a robust fingerprint recognition system.

Implement WSN for effective data communication.

Integrate IoT devices for seamless connectivity.

Design a centralized monitoring system for real-time analysis.

Test and validate the system's efficiency in unauthorized area detection.

**Finger Print Transmitting Section**

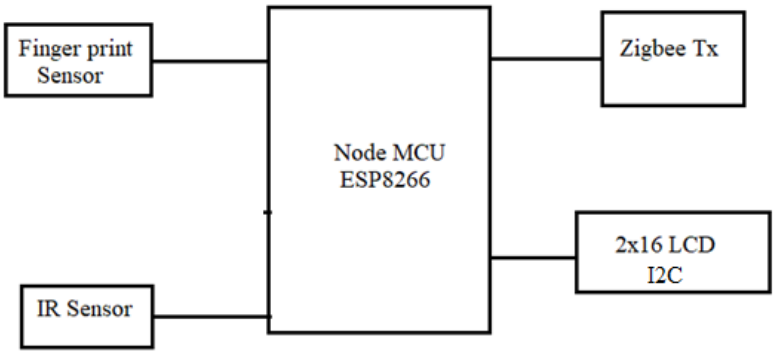
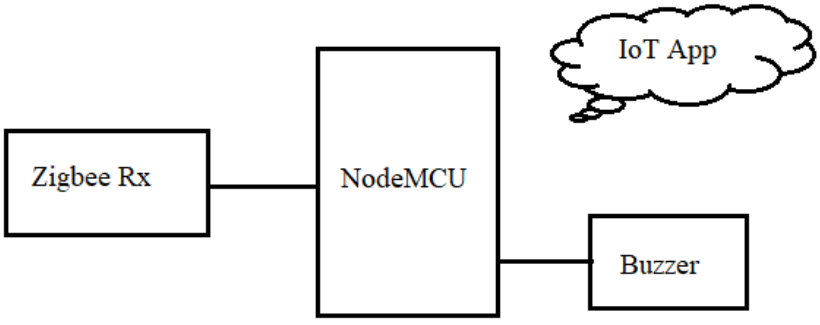



Figure.1 Block Diagram of Finger Print Transmitting Section

**IoT Receiver Section**



ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 1, 2024

Figure.2 Block Diagram of IoT receiver Section

## LITERATURE SURVEY

**1.Arbab Waheed Ahmad, Naeem Jan, Saeed Iqbal and Chankil Lee proposed Implementation of ZigBeeGSM based Home Security Monitoring and Remote-Control system.**

Home security and control is one among the essential needs of mankind from youth. But today it'sto be updated with the rapidly changing technology to make sure vast coverage, remote, reliability,and real time operation. Deploying wireless technologies for security and control in homeautomation systems offers attractive benefits alongside user friendly interface.

**2. P. Satya Ravi Teja, A. Sai Srikar, V. Kushal, K. Srinivasan proposed Photosensitive Security System for Theft Detection and Control using GSM technology.**

The proposed system consists of an LDR sensor which acts as an electronic eye for detecting the theft, and signaling procedure supported SMS using GSM (Global Systems for Mobile communications) technology. The GSM based communication helps the owner and anxious authorities to require necessary and timely action so as to stop the theft. The LDR (Light Dependent Resistor) circuit is interfaced employing a relay circuit with an Arduino microcontrollerboard. Efficacy of the proposed system are often seen in its immediate intimation regarding the incident. The proposed designed system is very effective and inexpensive. Index Terms— Arduino microcontroller, LDR, GSM module 300, Security system, Photosensitive.

**3. A. Alheraish are designed by Design and Implementation of Home Automation System.**

M2M Wireless communication of varied machines and devices in mobile networks could even bea fast-growing business and application area in industry, customer services, maintenance business,and security and banking areas. This paper presents design and implementation of remote systemby means of GSM cellular communication network. The design integrates the device to be controlled, the microcontroller, and therefore the GSM module in order that it is often used for a good range of applications. Detailed description and implementation of every design element are presented. To verify the operation of the M2M design, two home applications are practically testedusing PC-based environment.

**4. R.Anandan, Mr.B.Karthik and Dr.T.V.U.Kiran Kumar proposed Wireless home and industrial automation security system using GSM.**

The system is fully controlled by the 8-bit P89V51RD2 microcontroller are used. All the sensors and detect are interconnect to microcontroller by using various types of interface

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue 1, 2024

circuits. The microcontroller will continuously be monitoring all the type of sensors and if it senses any securityproblem detect then the microcontroller will send the SMS to the user mobile through Microcontroller to GSM modem. The Microcontroller also turns ON and OFF the electrical appliances in home as well as industry based on SMS received from the respective user.

## PROPOSED SYSTEM

Based on Zigbee network that monitor and control business security system using sensors deployed at different places in business place. A Zigbee based wireless sensor network for businesssecurity is described in which sensors sense suspicious activities and send signal to receiver. Transmitter consists of IR sensor and biometric sensor. There is $i^2c$ 16x2 LCD which is used to display the information of an employ. When a person enters into the office in abnormallythen these sensors are activated and ON the buzzer in receiver size. That will alert the owner. ZigBee receiver consist of NodeMCU, through this it transfers data using the Wi-Fi. It also consists of buzzer, when abnormal activates are done the buzzer will ON. The information is known through IOT application. The data is sent through the IOT app to the owner. Every time when a person enters into the office.

### Transmitter

Finger print module is connected to the NodeMCU . some pins are act as Transmitter and Receiver. When any person placed the finger on module it reads theridges on finger and analysis the data already stored in the memory. If it matches it allowsthe person or it not matches it will ON the buzzer.

### Receiver:

NodeMCU is connected to the power supply through the pins Vin and Ground. Power is distributed over the circuit.

Buzzer is connected to the NodeMCU to the pins of Ground and Digital pin . Zigbee module is connected to the NodeMCU by the pins .By default these are considered as UART pins. It is used for Long-distance wireless transmission.

Zigbee module is connected to the NodeMCU by the pins Tx and Rx. By default, these are considered as UART pins. It is used for Long-distance wireless transmission.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue 1, 2024

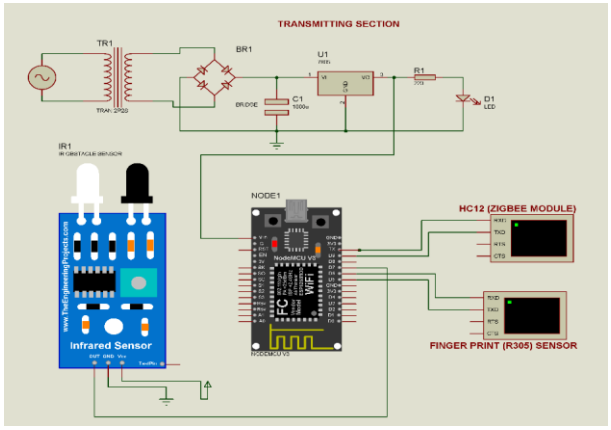



Figure.3 Transmitter Schematic Diagram

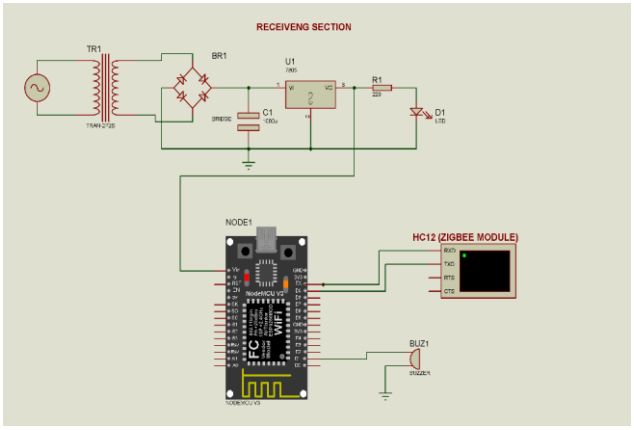



Figure.4 Receiver Schematic Diagram

## RESULTS


Figure.5 LCD Output

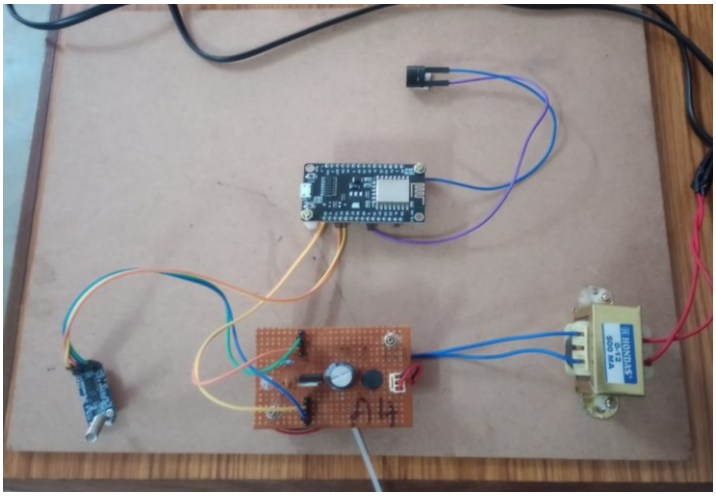


Figure.6 Working kit

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue 1, 2024

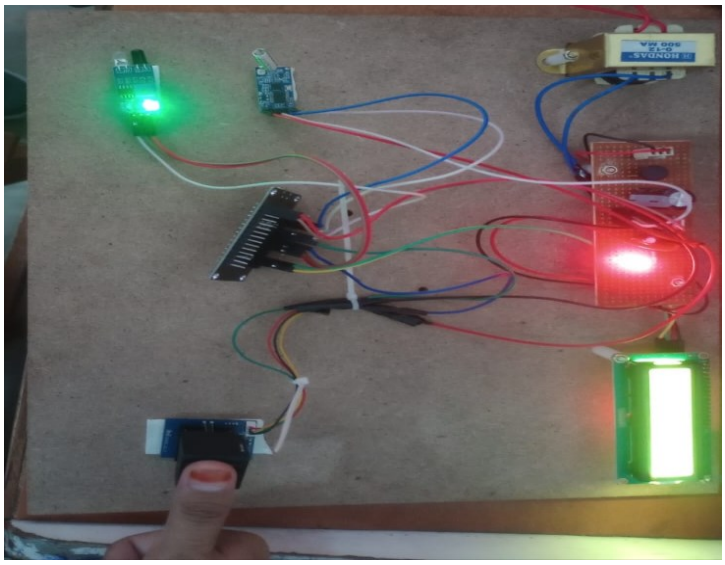


Figure.7 Testing

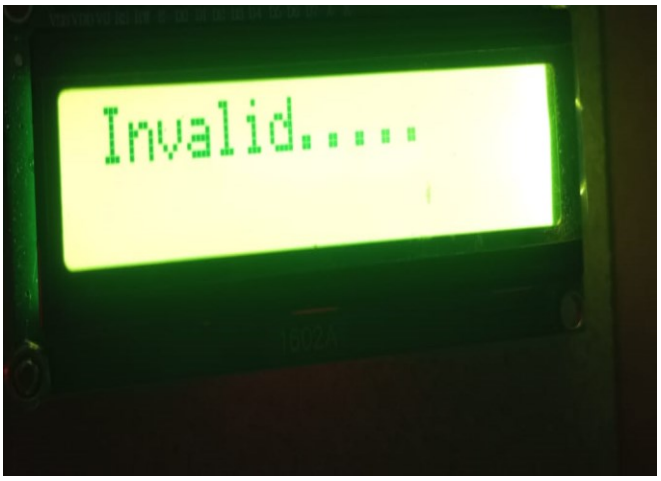



Figure.8 Invalid fingerprint

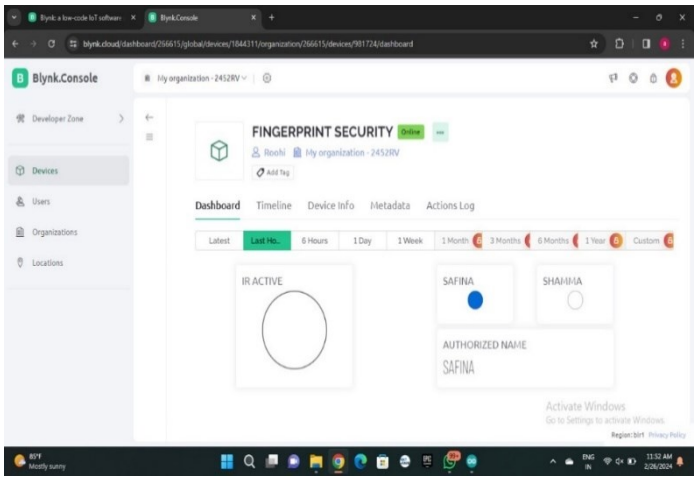



Figure.9 Blynk Output

## APPLICATIONS

**Fingerprint Authentication:** Each authorized person's fingerprint is scanned and stored in a database. When they need access to a secure area, they would authenticate themselves by scanning their fingerprint using a biometric scanner.

**IoT Integration:** The biometric scanner is connected to an IoT device, which can be a microcontroller or a small computer like a Raspberry Pi.

**Wireless Sensor Network (WSN):** WSN comprises interconnected sensor nodes deployed throughout the secured area.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue 1, 2024

**Unauthorized Access Detection:** If someone tries to access the area without proper authentication, the sensors detect the intrusion.

## ADVANTAGES

**Enhanced Security:** Fingerprint authentication adds an extra layer of security, as it is difficult to forge or replicate fingerprints.

**Real-time Alerts:** The system can instantly detect unauthorized access attempts and trigger immediate alerts, enabling swift response from security personnel to mitigate potential threats.

**Remote Monitoring:** Security personnel can monitor the secured area remotely through the IoT interface.

**Reduced False Alarms:** Wireless sensor networks can be programmed to distinguish between normal activities and actual security breaches.

## CONCLUSION

In conclusion, the integration of fingerprint biometrics and IoT technology in a Wireless Sensor Network-based security alert system for unauthorized areas offers a highly effective solution for enhancing safety and security. By leveraging fingerprint authentication, the system ensures reliable identification of authorized personnel while minimizing the risk of unauthorized access.

## FUTURE SCOPE

The future scope for the fingerprint and IoT-based security alert system for unauthorized areas using Wireless Sensor Networks is promising and multifaceted. Here are some potential avenues for further development and enhancement:

**1. Enhanced Biometric Authentication:** Future iterations of the system could incorporate advanced biometric authentication methods.

**2. Integration with Artificial Intelligence (AI):** Integration with AI algorithms could enable the system to continuously learn and adapt to new threats or patterns of behavior.

**3. Expansion of IoT Capabilities:** The system could be expanded to incorporate a wider range of IoT devices and sensors.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue 1, 2024

**4. Cloud Integration:** Integration with cloud computing platforms could enable centralized management and storage of security data.

## REFERENCES

1.Academic Databases: Explored databases like IEEE Xplore, ScienceDirect, ACM Digital Library, and Google Scholar. we searched for papers using keywords related to our project, such as "fingerprint biometrics," "IoT security," "Wireless Sensor Networks," and so on.

2.Books and Textbooks: Revised books authored by experts in the fields of biometrics, IoT, security systems, and Wireless Sensor Networks. Visited online bookstores or library catalogs and search for relevant titles.

3.Industry Reports and Whitepapers: Checked the websites of companies and organizations involved in biometrics, IoT, and security technology. They often publish reports and whitepapers authored by experts in the field.

4.Government and Regulatory Websites: Visited government websites and regulatory agencies that oversee security standards and protocols. Look for technical reports, guidelines, and publications authored by experts in the field.

5.Patents and Intellectual Property Databases: Searched for patents related to biometric authentication, IoT security systems, and Wireless Sensor Networks.