ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN 2321-2152
www.ijmece.com
Vol 12, Issue 4, 2024

IOT-BASED INTRUDER DETECTION WARNING SYSTEM VIA MAIL SERVER

[1]R ASHOK CHAKRAWARTHI 21tq1a0414@siddhartha.co.in [1]K BHAVANI 22tq5a0404@siddhartha.co.in [1]MD ABDUL MOMEEN 22tq5a0417@siddhartha.co.in [2]Mrs. A. Prutha Rani ambatiprutharani.ece@siddhartha.co.in
SIDDHARTHA INSTITUTE OF TECHNOLOGY & SCIENCES Korremula Road, Ghatkesar, Medchal-Malkajgiri (Dist)-500 088

ABSTRACT

The advent of the Internet of Things (IoT) has enabled the development of innovative solutions to enhance security systems. This project focuses on designing and implementing an IoT-based intruder detection and warning system that leverages a mail server for timely notifications. The system integrates sensors, microcontrollers, and communication modules to detect unauthorized access or intrusion in real-time. Upon detection, the system triggers alerts and sends detailed warning messages, including timestamp and location, to predefined email addresses via a secure mail server.The system employs a combination of motion detection sensors, such as Passive Infrared (PIR) sensors, and advanced algorithms to minimize false alarms while ensuring accurate detection. It incorporates IoT-enabled microcontrollers like Arduino or Raspberry Pi, which process sensor data and establish connectivity with the mail server through Wi-Fi or GSM modules. The notification mechanism ensures immediate awareness for users, even in remote locations, enhancing the overall response time and security measures.

I.INTRODCUTION:

In today's interconnected world, security remains a top priority for individuals and organizations alike. The rapid advancement of technology has paved the way for innovative solutions to enhance security systems, and the Internet of Things (IoT) plays a pivotal role in this domain. The integration of IoT with traditional security measures allows for smarter, more responsive, and efficient systems. One such application is an IoT-based intruder detection warning system that utilizes a mail server for instant alerts.This system leverages IoT-enabled devices to monitor premises and detect unauthorized access. It combines real-time sensing, data analysis, and communication technologies to notify property owners or authorities of potential threats. When an intrusion is detected, the system promptly sends an alert email through a mail server to the

designated recipients, ensuring that timely action can be taken to mitigate risks. Such systems are particularly beneficial for homes, offices, and restricted areas where conventional security measures might fall short in terms of immediacy and automation.

II.LITERATURE SURVEY

The advent of IoT has revolutionized security mechanisms, offering enhanced monitoring, automation, and connectivity. Traditional intruder detection systems relied heavily on manual operations, CCTV monitoring, and alarm-based notifications. However, with IoT-enabled devices, security systems have transitioned towards real-time detection, automated responses, and remote accessibility. Kumar et al. (2020) discussed the transformative role of IoT in home security, emphasizing its ability to connect sensors, cameras, and alarms to provide real-time insights. The study highlighted how IoT facilitates integration with cloud services, enabling data storage, analysis, and communication. IoT's real-time nature ensures that users are alerted promptly in case of any intrusion. Similarly, Smith et al. (2019) demonstrated the efficacy of IoT systems in commercial applications. Their research focused on the use of motion detectors and cameras to secure large premises, showcasing the scalability of IoT-based solutions. IoT-based intruder detection systems employ a variety of sensors and devices to identify unauthorized access. These include Passive Infrared (PIR) sensors, ultrasonic sensors, and cameras. The integration of these sensors with IoT platforms ensures real-time data collection and analysis.In a study by Patel and Singh (2021), the authors developed an IoT-enabled intrusion detection system using PIR sensors and Raspberry Pi. The system was designed to detect motion and trigger alerts through a mobile app. Although the system was effective, the authors noted that integrating a mail server could enhance its notification mechanism. Another relevant study by Johnson et al. (2020) explored the use of artificial intelligence (AI) in IoT-based intrusion detection. Their research showcased how AI algorithms could analyze sensor data to distinguish between actual intrusions and false alarms. While the system provided accurate results, its reliance on high computational power posed challenges for cost-effective deployment.The integration of email notifications in IoT systems is an innovative approach to improving alert mechanisms. Email provides a reliable and widely accessible platform for delivering alerts, ensuring that users can receive notifications instantly across multiple devices.

III.EXISTING METHOD

ISSN 2321-2152
www.ijmece.com
Vol 12, Issue 4, 2024

The need for efficient and intelligent security systems has grown exponentially with the increasing risks of unauthorized access and intrusion. Conventional security measures, such as CCTV cameras and manual monitoring, often fall short in providing real-time alerts and automated responses. IoT-based intruder detection systems bridge this gap by leveraging smart devices, sensors, and communication technologies to deliver efficient and responsive security solutions.

An IoT-based intruder detection warning system via a mail server offers a significant advancement over traditional security setups. These systems use motion sensors, cameras, and microcontrollers to detect unauthorized entry and immediately notify the concerned individuals through email alerts. The email notifications can include timestamped information, location details, and even multimedia attachments, enabling swift action against potential threats. Despite their advantages, these systems have certain limitations and challenges that must be addressed for broader adoption.

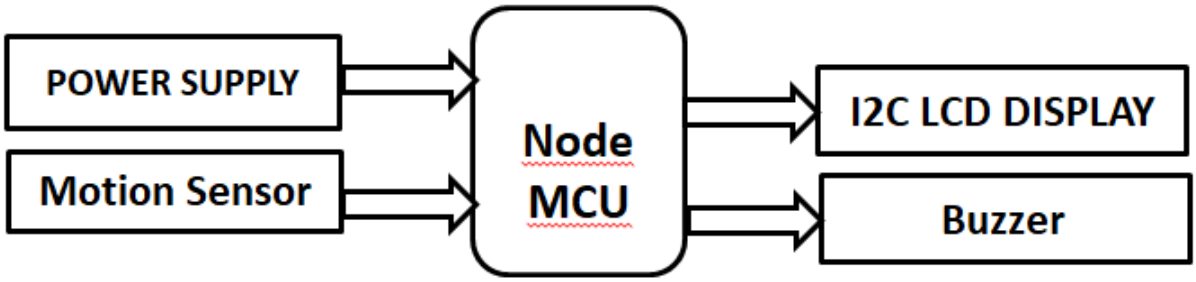

Fig.3.1: Existing system Block Diagram

IV.PROPOSED METHOD

The system primarily consists of an ESP8266 microcontroller, a PIR (Passive Infrared) sensor, an LCD display, and a buzzer. The ESP8266 acts as the central control unit, processing the data from the PIR sensor, which detects motion by sensing infrared radiation emitted by moving objects. When the PIR sensor detects motion, it sends a signal to the ESP8266, triggering an alert system.

ISSN 2321-2152
www.ijmece.com
Vol 12, Issue 4, 2024

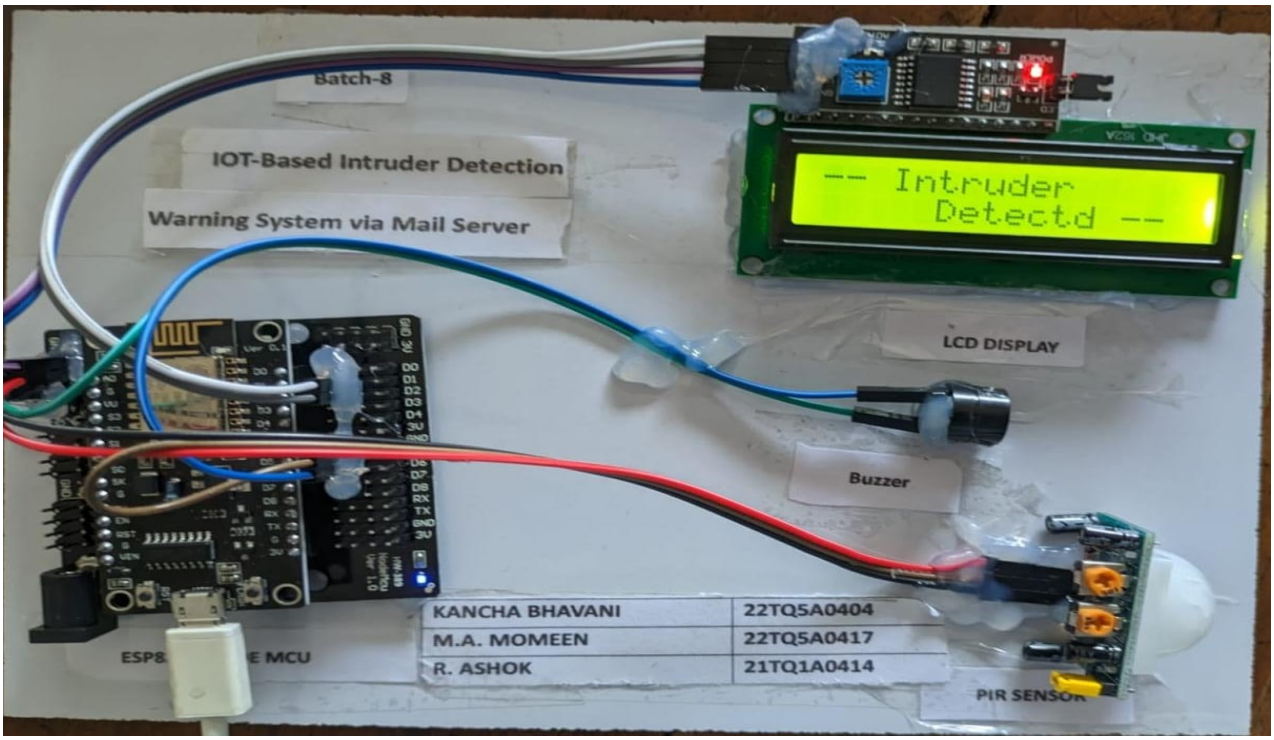

Fig.8.1:Project output

The LCD display is used to provide real-time feedback by showing messages like "Intruder Detected" when an unauthorized movement is identified. Simultaneously, a buzzer is activated to produce an audible warning, ensuring immediate on-site notification of the intrusion. The system is compact, energy-efficient, and capable of functioning autonomously, making it suitable for deployment in residential or commercial settings.In addition to local alerts, the system is programmed to send an email notification through a mail server, ensuring remote monitoring capabilities. The ESP8266 uses its Wi-Fi capabilities to connect to the internet and deliver a detailed warning email to predefined recipients. This dual-alert mechanism enhances the system's reliability and ensures that users are informed promptly, even if they are not physically present at the monitored location.

V.CONCLUSION AND FUTURE SCOPE

The IoT-Based Intruder Detection System provides a low-cost, efficient solution for property security. By combining a PIR sensor, NodeMCU, LCD, and buzzer, this system offers real-time intrusion alerts through both visual and audible means and notifies the owner via email.

This setup is easy to implement, making it accessible for small homes, personal properties, or low-budget security needs.

FUTURE SCOPE

Future improvements could enhance the system's functionality and reliability. Adding a GSM module would allow SMS alerts in areas without Wi-Fi, extending the system's reach. The integration of a camera for capturing images upon detection could provide visual verification, and storing data on a cloud platform would enable remote access to intruder records. Additionally, implementing mobile app notifications and geofencing could expand the system's usability, allowing users to manage multiple locations and receive alerts only when away from home. These upgrades would elevate the system's effectiveness, making it suitable for a wider range of security applications.

REFERENCES

[1]. R. K. Kodali, V. Jain, S. Bose and L. Boppana, "IoT based smart security and home automation system," 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 2016, pp. 1286- 1289, doi: 10.1109/CCAA.2016.7813916.

[2]. Mounica Jegurupati, "Home Security Alarm System Using Node MCU," SSRN, Oct. 2021, pp. 5, https://ssrn.com/abstract=3918382.

[3]. S. Lokesh, S. B. Patil and A. Gugawad, "Home Security and Automation Using NodeMCUESP8266," 2020 IEEE Bangalore Humanitarian Technology Conference (B-HTC), Vijiyapur, India, 2020, pp. 1-6, doi: 10.1109/BHTC50970.2020.9297917.

[4]. M. Pavithra, "IOT Home Automation with PIR Sensor Security using ESP8266 WI-FI Chip and GSM," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 8, Issue 6, June 2019, ISSN: 2278 – 1323.