International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 2, Mar-Apr 2026
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Reporting System for Security Guard Using IOT

Chetna Ahire[1], Kshitija Kale[2], Samruddhi Bhavle[3], Sakshi Mahulikar[4]
(sakshimahulikar5998@gmail.com)

----------**********----------

Abstract:

The "Reporting and Alert System for Security Guard using IoT" is an innovative solution designed to improve the safety, accountability, and efficiency of security personnel deployed in various organizations and premises. Traditional manual reporting methods often lead to delays, miscommunication, and lack of real-time updates, which can affect overall security management. This system overcomes these limitations by integrating Internet of Things (IoT) technology to automate monitoring and alert functions. It utilizes a fingerprint sensor for secure authentication of security guards, ensuring that only authorized personnel can access and record their activities. The ESP8266 Wi-Fi module enables real-time data transmission to a centralized system, allowing supervisors to remotely monitor guard movements and duty status. LED indicators provide visual status updates for system operations. In case of emergencies, missed checkpoints, or suspicious activities, the system generates instant alerts to concerned authorities, ensuring quick response and improved security. Additionally, all activities are digitally recorded for future reference, auditing, and performance evaluation. This IoT-based system offers a reliable, cost-effective, and scalable approach to modern security management, enhancing transparency, reducing manual effort, and ensuring better control over security operations. Overall, this IoT-based system provides a cost-effective, scalable, and efficient solution for modern security management. It not only minimizes human intervention but also enhances reliability, transparency, and responsiveness in security operations, making it suitable for deployment in offices, campuses, industries, and smart city environments.

Keywords— **Fingerprint Sensor, LED, ESP8266 Wi-Fi Module, IoT, Security System, Real-Time Monitoring, Alert System**

----------**********----------

I. INTRODUCTION

In today's organizations, industries, and residential complexes, security is of prime importance to ensure the safety of people and assets. The security guards are entrusted with the responsibility of guarding the premises, preventing unauthorized entry, and reporting suspicious activities. But the traditional methods of supervision and reporting have resulted in various issues of inefficiency, delay, and lack of information in real

moreover, in most cases, the supervisors are not aware of the precise location and condition of the security guard during the course of their duty hours. this has resulted in critical safety and accountability issues. to overcome these issues, the idea of developing an iot-based reporting and alert system for security guards has been conceived.

PRESENT THEORIES AND PRACTICES

The "Reporting and Alert System for Security Guard using IoT" is a modern technological solution developed to enhance the effectiveness, reliability, and transparency of security operations in organizations, campuses, industries, and residential areas. With the rapid advancement in embedded systems and wireless communication, traditional security methods are being replaced by smart, automated systems. This project is based on the concept of the Internet of Things (IoT), where physical devices are connected to the internet to collect, transmit, and process data in real time.

The core idea behind this system is to monitor the activities of security guards and provide instant alerts in case of irregularities or emergencies. In conventional systems, guards manually record their attendance and patrol details, which can lead to human errors, negligence, or manipulation. These systems lack real-time monitoring, making it difficult for authorities to ensure proper security management. To overcome these issues, the proposed system integrates IoT technology with biometric authentication and wireless communication modules.The system primarily consists of a fingerprint sensor, ESP8266 Wi-Fi module, microcontroller, LED indicators, and a centralized monitoring platform. The fingerprint sensor plays a crucial role in ensuring secure and accurate identification of security personnel. Each guard is registered in the system with a unique fingerprint, which is used for authentication during duty check-ins and checkpoints. This eliminates the possibility of proxy attendance and ensures accountability.

The ESP8266 Wi-Fi module is responsible for establishing communication between the hardware system and the cloud or central server. It enables real-time data transmission, allowing supervisors to monitor guard activities remotely through a web or mobile interface. The microcontroller acts as the brain of the system, processing inputs from the fingerprint sensor and controlling data flow to the Wi-Fi module. LED indicators provide visual feedback to the user, such as successful authentication or system status.

The working principle of the system involves multiple checkpoints installed at different locations within the premises. Security guards are required to authenticate themselves using the fingerprint sensor at each checkpoint within a specified time interval. Once the fingerprint is verified, the system logs the guard's identity, time, and location, and transmits this data to the central server. This creates a digital record of the guard's patrol route and ensures that all checkpoints are covered.

In case a guard fails to report at a checkpoint within the designated time, the system automatically generates an alert. Additionally, an emergency button or predefined condition can trigger immediate notifications to supervisors or control rooms. These alerts can be sent via mobile applications, SMS, or email, ensuring quick response to potential threats or issues. This real-time alert mechanism significantly improves the responsiveness and efficiency of the security system.

From a theoretical perspective, this project combines concepts from embedded systems, wireless communication, and IoT architecture. The system follows a typical IoT framework consisting of sensing, connectivity, data processing, and application layers. The fingerprint sensor acts as the sensing component, the ESP8266 provides connectivity, the microcontroller handles data processing, and the monitoring platform represents the application layer. This layered architecture ensures scalability and flexibility, allowing the system to be expanded with additional sensors or features in the future.

In terms of practical implementation, several important considerations must be addressed. First, proper placement of checkpoints is essential to ensure complete coverage of the area. The fingerprint sensor must be calibrated and tested for accuracy under different environmental conditions. Network connectivity should be stable to avoid data transmission delays or failures. Power supply management is also critical, especially if the system is deployed in large outdoor areas.

Security and data privacy are important aspects of this system. Since biometric data is sensitive, it must be securely stored and transmitted using encryption techniques. Access to the monitoring system should be restricted to authorized personnel only. Regular maintenance and software updates are necessary to ensure system reliability and protection against vulnerabilities.

The system offers several advantages, including improved accountability, real-time monitoring, reduced manual effort, and enhanced security. It is cost-effective and scalable, making it suitable for various applications such as corporate offices, educational institutions, hospitals, and industrial

facilities. However, challenges such as network dependency, initial setup cost, and environmental factors affecting hardware performance must be considered.

PROBLEM STATEMENT

In many organizations and residential areas, security guards rely on manual reporting systems, which are often inefficient and prone to errors. There is a lack of real-time monitoring of guard activities, making it difficult to ensure proper patrolling and accountability. Manual log entries can be manipulated or missed, leading to security risks. Communication delays between guards and supervisors can result in slow response during emergencies. Additionally, there is no reliable system to verify the presence and identity of guards at different checkpoints. The absence of automated alert mechanisms further reduces the effectiveness of security operations.

Following Conditions Shows The Real Time Example for Security Guard Using IOT

Imagine a company office at night:

A motion sensor detects movement at 2 AM. The camera automatically starts recording. The system sends an alert to the security guard's phone. The guard opens the app and sees a person inside.

The system: Turns on a siren Sends alert to police/security team Guard can even talk through a speaker (advanced IoT setup).

A. Figure For Reporting System For Security Guard Using IOT

The proposed system utilizes a Wi-Fi connection for transferring real-time data to cloud platforms like Thing Speak/Firebase. The proposed system utilizes a 5V power supply for efficient functioning. The proposed system can include other sensors like PIR sensors and temperature sensors for efficient functioning. The proposed system is efficient, reliable, and effective for smart security monitoring.

a) Hardware setup: The hardware for the proposed IoT-based reporting and alert system for security guards includes various components, including the ESP8266 microcontroller, fingerprint sensor, tactile switch, LCD display, and buzzer, which are connected together for efficient monitoring of security guard

b)Software development : In general, the software development for the proposed IoT-based reporting and alert system for security guards includes efficient programming of the microcontroller, including the ESP8266 microcontroller, using the Arduino software development board. The proposed system can be connected to cloud platforms like Thing Speak/Firebase using a Wi-Fi connection, utilizing MQTT and HTTP protocols for efficient communication. The proposed system utilizes a web interface for efficient monitoring of security guard activities. The proposed system utilizes efficient data logging and timestamping for efficient record-keeping.

c)Integration: The ESP8266 microcontroller is programmed to sense data from various devices, such as the fingerprint sensor, panic button, and motion sensor. These devices are integrated with the IoT cloud platform to monitor and raise alarms in real time.

d)Testing and deployment: For unit testing, individual modules such as the sensor, Wi-Fi module, buzzer, and display will be tested for proper functionality. For integration testing, combined hardware and software testing will be conducted to ensure proper communication among all modules.

e)Power management: The system operates using a 5V regulated DC power supply, which is used to power modules such as ESP8266, sensors, and display. Low power modes are implemented in the microcontroller to reduce power consumption in idle modes.

CONCLUSIONS

The Reporting and Alert System for Security Guards using IoT successfully enhances security management by enabling real-time monitoring, data recording, and instant alert generation. Through the integration of IoT components such as the ESP8266 microcontroller, sensors, and cloud connectivity, the system ensures efficient communication between guards and the control center. It minimizes human errors, improves accountability through guard identification (via RFID or fingerprint sensors), and allows for timely responses during emergencies. Overall, this system provides a reliable, automated, and cost-effective solution for ensuring the safety and efficiency of security operations in modern infrastructure

ACKNOWLEDGMENT

We express our sincere gratitude to our project guide for their valuable guidance and continuous support throughout this work necessary facilities to complete this project successfully.
We are grateful to our friends and classmates for their help and encouragement.
Finally, we thank our family members for their constant support and motivation.

REFERENCES

[1] A. Sultana and S. Katral, "Monitoring System for Security Guard Using RFID and IoT," *International Journal of Creative Research Thoughts (IJCRT)*, vol. 12, no. 12, Dec. 2024.

[2] V. R. Gannapathy and V. Narayanamurthy, "A Mobile and Web-Based Security Guard Patrolling, Monitoring and Reporting System to Maintain Safe and Secure Environment at Premises," *International Journal of Interactive Mobile Technologies (iJM)*, Jun. 2023, doi: 10.3991/ijim.v17i11.35483.

[3] M. S. Sangari and R. M. Raju, "Exploring the Workplace Challenges Faced by Night-Shift Security Guards in Madhavaram, Chennai," *IOSR Journal of Humanities and Social Science (IOSR-JHSS)*, vol. 30, no. 5, ser. 1, May 2025.

[4] R. U. Sheikh, P. A. Kale, and S. Sarfaraj, "A Review Paper on IoT Based Smart Security and Home Automation," *International Journal of Scientific Research in Science and Technology*, vol. 8, no. 3, 2021.

[5] M. A. A. Rakib and M. M. Rahman, "Fingerprint Based Smart Home Automation and Security System," *European Journal of Engineering and Technology Research*, vol. 7, no. 2, Apr. 2022.

