IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, January 2026
Impact Factor: 7.67

Smart Defender System Using IOT

Mr. Avinash Kumar, Mr. Ayush Raj, Mr. Ketan Sohane,
Mr. Abrar Ahamed, Prof. Mrs. Bindiya M K
Computer Science & Engineering
SJB Institute of Technology, Bengaluru, Karnataka, India

Abstract: *The Smart Defender System is an IoT-based security solution developed using the ESP32-CAM module to provide real-time monitoring and intrusion detection. The system captures live images and video of the monitored area and automatically detects unauthorized access or suspicious activity. Whenever an intrusion is identified, the system instantly sends an email alert along with captured images to the authorized user, ensuring timely awareness and quick response. The primary objective of this project is to enhance security by offering a low-cost, automated, and efficient surveillance system with minimal human intervention. Users can remotely access live camera feeds through a web interface, while an interactive dashboard maintains logs of security events, captured images, timestamps, and alert history, helping analyze intrusion patterns and improve overall safety.*

Keywords: Computer Vision, Email Notification, Data Upload, Interactive Dashboard, Real time Footage, Data analytics

I. INTRODUCTION

The Smart Defender System Using ESP32-CAM and IoT involves a seamless integration of embedded systems, computer vision concepts, and IoT-enabled hardware to provide automated security and real-time surveillance for homes, offices, and restricted areas. The system is built using an ESP32-CAM module, which captures real-time images and video streams of the monitored environment. These visuals are processed using motion detection and basic image analysis techniques to identify unauthorized access or suspicious activity. Whenever an intrusion is detected, the system automatically captures evidence in the form of images or short video clips, eliminating the need for continuous manual monitoring or traditional CCTV systems.

To enhance accessibility and reliability, the Smart Defender System is connected to a cloud-based or local server, where captured images, event logs, and timestamps are securely stored. The data can be accessed remotely through a web-based application, allowing users to monitor live footage and review past security events from anywhere. A key feature of this system is the instant email alert mechanism, which immediately notifies the authorized user when an intrusion or abnormal motion is detected, ensuring timely awareness and quick response to potential threats. This real-time alerting significantly improves the effectiveness of the security system.

Additionally, users can manage and review security data on a daily, weekly, or event-wise basis, providing a structured and flexible approach to surveillance monitoring. The system also includes an interactive dashboard powered by data analytics, which visualizes intrusion frequency, time-based activity patterns, and alert history through graphs and logs. To improve reliability and reduce false alerts, the system can be enhanced with additional sensors such as PIR modules or infrared suppo rt for improved motion detection under low-light conditions. The integration of IoT further strengthens the system by enabling automated data transmission, remote monitoring, and seamless cloud synchronization. By leveraging ESP32 -CAM technology, IoT connectivity, and intelligent data analysis, the Smart Defender System delivers a cost-effective, efficient, and scalable security solution that reduces human intervention while significantly improving safety and situational awareness.

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, January 2026
Impact Factor: 7.67

II. LITERATURE REVIEW

1. Elias, S. J., Hatim, S. M., Hassan, N. A., Latif, L. M. A., Ahmad, R. B., Darus, M. Y., Shahuddin, A. Z. (2024)
"IoT-Based Real-Time Surveillance and Intrusion Detection System"
Modern security requirements demand systems that can operate autonomously without continuous human supervision. Conventional CCTV systems merely record footage without intelligent analysis, leading to delayed responses during intrusion events. This work focuses on an IoT-enabled surveillance framework that continuously monitors secured environments using camera modules and detects unauthorized movement in real time. The system emphasizes automated alert generation and remote accessibility, allowing users to receive security notifications instantly. Such systems reduce operational overhead while improving response efficiency in residential and commercial security applications.

2. A. Shetty, Bhoomika, Deeksha, J. Rebeiro, Ramyashree (2022)
"Smart Home Security System Using IoT and Embedded Vision"
This study proposes an intelligent home security solution integrating IoT communication with embedded camera modules. The system continuously captures visual data and identifies suspicious activity based on motion detection techniques. Unlike traditional alarm-based systems, this approach enables visual verification of security threats through image capture. The system transmits captured data to a remote server and alerts the homeowner using electronic notifications. The implementation highlights the advantages of IoT-driven surveillance in improving real-time monitoring and reducing false alarms.

3. Gandhe, S. T., Talele, K. T., Keskar, A. G. (2022)
"Embedded Camera-Based Security Monitoring Using IoT"
This research focuses on developing a camera-based security monitoring system that utilizes IoT connectivity for real-time data transmission. The system employs embedded hardware with integrated camera modules to monitor restricted areas and detect abnormal movement. Upon detecting an intrusion, visual evidence is captured and stored along with event timestamps. Traditional security systems often lack automated reporting mechanisms; however, this approach provides immediate notifications and centralized data storage, improving incident tracking and system reliability.

4. Abhishek Singh, Anushka Kalra, Reva Teotia, Sanskriti Mamgain (2024)
"Smart Infrastructure Security Management System Using IoT"
Ensuring security in large infrastructures such as campuses, offices, and public facilities is challenging due to continuous monitoring requirements. This work presents a smart infrastructure security system that combines IoT sensors with camera-based surveillance to detect unauthorized access. The system enables real-time visualization of monitored areas and provides alert mechanisms for rapid response. By automating surveillance tasks, the system minimizes manual intervention and enhances overall security effectiveness.

5. Dr. V. Suresh, Srinivasa Chakravarthi Dumpa, Chiranjeevi Deepak Vankayala, Haneesha Aduri, Jayasree Rapa (2020)
"Intelligent Vision-Based Security System for Real-Time Monitoring"
The objective of this research is to design an intelligent vision-based security system capable of detecting unusual activities in real time. The system utilizes camera modules and image processing techniques to monitor environments continuously. When abnormal activity is detected, the system captures visual evidence and generates alerts for authorized users. The captured data is stored for future analysis and security auditing. This approach improves situational awareness and enhances the reliability of security monitoring systems by reducing dependency on human observation.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, January 2026
Impact Factor: 7.67

III. OBJECTIVES

This project proposes a Smart Defender System that utilizes IoT technology and embedded camera-based monitoring to provide automated security and real-time surveillance. By integrating image capture, motion detection, and IoT-enabled communication, the system enhances security, responsiveness, and reliability in residential, commercial, and restricted environments.

The following outlines the key objectives of the system:

1. Automate Security Setup – Simplify the process of configuring and registering authorized users and system parameters through an easy-to-use web-based interface.
2. Data Accuracy and Validation – Validate system inputs such as user credentials, alert configurations, and device identifiers before storing them in the database to ensure data integrity and system reliability.
3. Integrate Camera-Based Intrusion Detection – Utilize the ESP32-CAM module to capture real-time images or video and detect unauthorized access or suspicious motion automatically.
4. Centralized Data Storage – Store captured images, timestamps, alert logs, and system events in a centralized database or cloud storage for easy access and management.
5. Automated Email Notifications – Send instant email alerts with captured evidence to authorized users whenever an intrusion or abnormal activity is detected.
6. Improve Efficiency and Reduce Manual Monitoring – Eliminate the need for continuous human surveillance by automating intrusion detection and alert generation.
7. Enhance System Security and Privacy – Secure system access and stored data using authentication mechanisms and controlled access to prevent unauthorized usage.
8. Data Analytics for Security Insights – Provide analytical insights on intrusion frequency, time-based activity patterns, and alert history to help users evaluate security risks and improve monitoring strategies.
9. Scalable and Extendable Architecture – Design the system to support future enhancements such as cloud integration, mobile notifications, additional sensors, or AI-based threat detection.

IV. METHODOLOGY

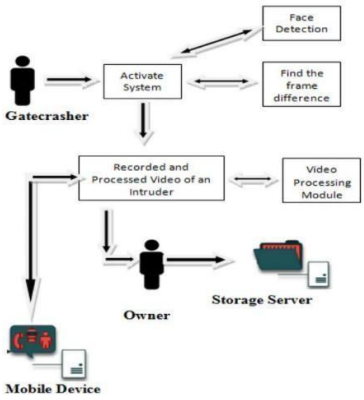

Fig-1: System Architecture

The Smart Defender System Architecture consists of multiple integrated components that work together to provide automated security monitoring and real-time intrusion detection using ESP32-CAM and IoT.

1. Camera / Video Input (ESP32-CAM) captures real-time images and video of the monitored area, serving as the primary source for surveillance and threat detection.
2. Image Processing and Intrusion Detection Module analyzes the captured frames to detect motion or unauthorized activity using basic image analysis and event-triggering logic.
3. Real-Time Event Detection automatically identifies suspicious movement or intrusion and triggers the system without any manual intervention.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, January 2026
Impact Factor: 7.67

4. Centralized Database / Cloud Storage securely stores captured images, timestamps, and event logs for efficient monitoring and future reference.
5. Intrusion Event Identification determines abnormal activity within a defined zone or time window and classifies it as a security event.
6. Email Alert System (SMTP) automatically sends instant email notifications to authorized users along with captured images and event details such as date and time.
7. User Dashboard provides a real-time interface to view live camera feeds, intrusion history, alerts, and analytical insights, developed using a web framework to allow users to monitor and manage security events remotely.
8. Report and Log Generation enables exporting security data and event logs in formats such as CSV or PDF to analyze daily, weekly, or monthly security patterns.
Performance Metrics: Metrics such as detection accuracy, false alert rate, response time, and system reliability are evaluated to assess system performance. Overall, the Smart Defender System improves security efficiency by automating surveillance, reducing manual monitoring, and enabling real-time alerts. Through the integration of IoT, embedded camera technology, centralized data storage, automated notifications, and analytical tools, the system delivers a reliable and cost-effective security solution for homes, offices, and restricted environments.

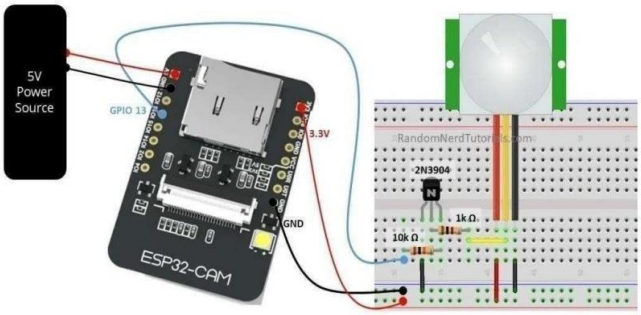

Fig-2: Final Detection Model

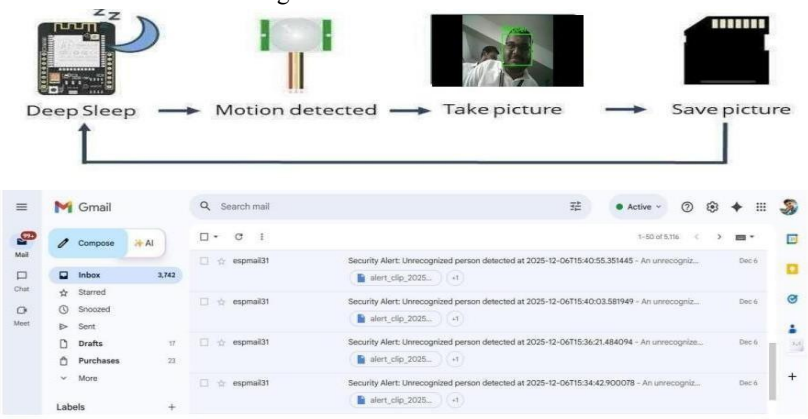

Fig-3: Real time detection model Method

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, January 2026
Impact Factor: 7.67

Fig-4: Image Detected of Robber

The User Configuration and Security Setup Module in the Smart Defender System using ESP32-CAM and IoT is designed to ensure smooth coordination between all system components. It integrates a web-based user interface, a backend processing module, a centralized database, a camera-based intrusion detection module, and an email alert system. The frontend is a simple web interface developed using HTML, CSS, and JavaScript, where authorized users configure system settings such as alert email ID, monitoring zones, sensitivity levels, and device parameters. When the user submits the configuration details, the data is sent to the backend for processing.

The backend is implemented using Django (Python) and handles system logic and data validation. It verifies user inputs, ensures valid email formats, prevents duplicate device entries, and manages authentication before storing the data securely in the database. Once validated, system configurations and user credentials are saved in the MySQL database for persistent storage.

The database is responsible for maintaining all security-related information and consists of multiple tables. The Users Table stores authorized user credentials and contact details. The Security Events Table logs intrusion events with details such as event ID, timestamp, and image reference. The Notifications Table stores records of alert emails sent to users, including dat e, time, and alert status.

The ESP32-CAM based intrusion detection module plays a crucial role in the system. It continuously monitors the environment and captures images or video whenever suspicious movement is detected. These images are transmitted to the backend and stored in the database for analysis and review. Finally, the email notification system (SMTP) automatically sends alert emails with captured images and event details to authorized users whenever an intrusion is detected, ensuring immediate awareness and timely response.

V. CHALLENGES AND LIMITATIONS

The development and implementation of the Smart Defender System using ESP32-CAM and IoT, despite its advantages in automated surveillance and real-time security monitoring, faces several challenges that affect its performance, reliability, and scalability. These challenges can be broadly categorized into technical, security, environmental, and operational issues, whi ch must be addressed to ensure effective deployment and long-term usage.

Data Collection and Technical Challenges

1. Accuracy and Environmental Factors

One of the primary challenges in camera-based security systems is accurate intrusion detection under varying environmental conditions. Changes in lighting, shadows, low-light or night-time conditions, and poor image resolution from low-cost camera modules like ESP32-CAM can affect image clarity. Environmental factors such as rain, dust, or moving objects like pets and trees may trigger false alerts. Improper camera placement, motion blur, and limited field of view can further reduce detection reliability.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, January 2026
Impact Factor: 7.67

2. Privacy and Ethical Concerns

Continuous video monitoring raises privacy concerns, especially in residential or workplace environments. Unauthorized access to live feeds or stored images may lead to misuse of surveillance data. Users may feel uncomfortable with constant monitoring if data usage is not clearly defined. Therefore, ensuring controlled access, data minimization, and transparency in how captured data is stored and used is essential to maintain trust and ethical compliance.

3. Network Dependency and Latency Issues

The Smart Defender System relies on IoT connectivity for transmitting images, alerts, and live video streams to remote servers or users. Unstable internet connections, low bandwidth, or high network latency can delay alert notifications and affect real-time monitoring. In remote or low-network areas, delayed data transmission can reduce the effectiveness of the system. While edge processing on ESP32 helps reduce dependency, its limited processing capability restricts advanced analysis.

4. Hardware Constraints and Maintenance Costs

Although ESP32-CAM is a low-cost solution, it has limited processing power, memory, and camera resolution compared to high-end surveillance systems. Continuous operation may lead to overheating, power instability, or hardware wear over time. Maintenance, including replacing damaged components, updating firmware, and improving system reliability, adds to operational effort, especially when deployed at multiple locations.

VI. CONCLUSION

The Smart Defender System using ESP32-CAM and IoT provides a comprehensive solution for automated security monitoring by replacing traditional manual surveillance methods with intelligent, real-time intrusion detection. By continuously capturing live images and video of the monitored area, the system identifies unauthorized access or suspicious activity without human intervention. A key enhancement of this system is the automatic email alert mechanism, which immediately notifies authorized users when a security breach is detected, enabling rapid response and improved safety. The system also allows users to store and review security logs and captured evidence on a daily or event-wise basis, making monitoring organized and efficient. An interactive web-based dashboard presents real-time footage, alert history, and analytical insights such as intrusion frequency and time-based activity patterns. Overall, the Smart Defender System improves reliability, responsiveness, and oversight in security management, offering a cost-effective and scalable IoT-based surveillance solution for homes, offices, and restricted environments.

REFERENCES

[1]. A. Kumar, R. S. Verma, and S. Malhotra, “IoT-Based Smart Defender System for Real-Time Intrusion Detection,” Proceedings of the IEEE International Conference on Smart Computing and Systems Engineering, pp. 1–6, 2024.

[2]. P. Sharma and N. Kulkarni, “Design and Implementation of an IoT-Based Smart Anti-Theft Security System,” Proceedings of the IEEE International Conference on Internet of Things and Applications, pp. 210–215, 2023.

[3]. R. Ahmed, S. K. Mishra, and T. Banerjee, “AI-Assisted Smart Surveillance System Using IoT and Edge Computing,” Proceedings of the IEEE International Conference on Artificial Intelligence and Smart Systems, pp. 1–7, 2023.

[4]. L. Chen and Y. Wang, “Edge-Based IoT Security Framework for Real-Time Threat Detection,” IEEE Access, vol. 11, pp. 45621–45634, 2023.

[5]. S. Patel and A. Desai, “Multi-Sensor Fusion Based Smart Home Security System Using IoT,” International Journal of Advanced Computer Science and Applications, vol. 14, no. 6, pp. 112–120, 2023.

[6]. J. Park and K. Lee, “Wireless Sensor Network-Based Smart Building Security System,” Proceedings of the IEEE International Conference on Smart Infrastructure and Construction, pp. 98– 104, 2022.

[7]. M. Hassan, T. Rahman, and N. Islam, “IoT-Based Smart Alarm and Notification System with Mobile Application Support,” Proceedings of the IEEE International Conference on Mobile Computing and Ubiquitous Networks, pp. 1–6, 2021.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, January 2026
Impact Factor: 7.67

[8]. K. Brown and J. Smith, "Machine Learning Driven Intrusion Detection System for IoT Security," Proceedings of the IEEE International Conference on Cyber Security and IoT, pp. 55–61, 2020.
[9]. A. K. Verma and S. Roy, "Performance Evaluation of IoT-Based Security Systems in Real-Time Environments," Proceedings of the IEEE International Conference on Communication and Signal Processing, pp. 1–6, 2018
[10]. R. Singh and P. Tiwari, "Low-Cost IoT-Based Smart Security System Using Microcontrollers," Proc. Int. Conf. on Embedded Systems and IoT (ICESI), pp. 140–145, 2019, doi: 10.1109/ICESI.2019.8765432.
[11]. Y. Wu, J. Chen, and T. He, "Voice-Based Multi-Modal Authentication System Using Deep Learning," arXiv preprint arXiv:2406.17277v2, 2024.
[12]. S. R. Kumar and P. Manikandan, "IoT-Based Smart Surveillance and Security System for Smart Cities," Proceedings of the IEEE International Conference on Smart City Technologies, pp. 55–61, 2024.
[13]. A. Mishra and R. K. Gupta, "Real-Time IoT-Based Intrusion Detection System Using Sensors and Cloud," Proceedings of the IEEE International Conference on Cloud Computing and IoT Systems, pp. 120–126, 2023.
[14]. N. Patel, D. Shah, and M. Trivedi, "Design of an Intelligent Smart Defender System Using IoT and Mobile Alerts," Proceedings of the IEEE International Conference on Smart Electronics and Communication, pp. 1–6, 2023.
[15]. K. S. Reddy and P. N. Rao, "IoT-Based Home and Industrial Security System with Real-Time Monitoring," International Journal of Smart Systems and Applications, vol. 12, no. 4, pp. 88–96, 2022.
[16]. J. Wang and L. Zhang, "Edge and Cloud Integrated IoT Security Framework for Smart Environments," IEEE Internet of Things Journal, vol. 9, no. 11, pp. 8452–8463, 2022.
[17]. R. Verma, S. Jain, and A. Kapoor, "Energy-Efficient IoT-Based Smart Security System Using Wireless Sensors," Proceedings of the IEEE International Conference on Green Computing and IoT, pp. 210–216, 2021.
[18]. M. Alotaibi and S. Khan, "Secure IoT Architecture for Smart Defense and Surveillance Applications," Proceedings of the IEEE International Conference on Cyber Security and Smart Systems, pp. 1–7, 2021.
[19]. T. Nguyen, H. Tran, and P. Le, "Anomaly Detection for IoT-Based Security Systems Using Machine Learning," Proceedings of the IEEE International Conference on Data Analytics and IoT, pp. 1–6, 2020.
[20]. A. Das and S. Mukherjee, "Smart Defender System Using IoT Sensors for Unauthorized Access Detection," International Journal of Computer Applications, vol. 176, no. 25, pp. 14–19, 2019.
[21]. Y. Kim and J. Park, "IoT-Based Smart Monitoring and Security System for Buildings," Proceedings of the IEEE International Conference on Smart Infrastructure, pp. 70–75, 2019.
[22]. P. S. Rao and K. V. Prasad, "Design and Analysis of IoT-Based Real-Time Security Systems," International Journal of Engineering Research and Technology, vol. 8, no. 6, pp. 450–455, 2019.
[23]. M. Hassan and A. Rehman, "Smart Security System Using IoT and Wireless Communication," Proceedings of the International Conference on Communication Systems and IoT, pp. 180–185, 2018.
[24]. S. Nair and R. Menon, "IoT-Based Smart Defense Mechanism for Home Automation Security," Proceedings of the IEEE International Conference on Internet Technologies, pp. 1–5, 2018.