International Research Journal of Education and Technology

Peer Reviewed Journal

ISSN 2581-7795

IoT-Enabled Smart Perimeter Security Fence

R. Krishna Kumar
Assistant Professor
Department of Electrical and Electronics Engineering
Karpagam College of Engineering
Coimbatore, Tamil Nadu, India

S. Arunkarthick
Department of Electrical and Electronics Engineering
Karpagam College of Engineering
Coimbatore, Tamil Nadu, India
Email:

S. K. Kavitharan
Department of Electrical and Electronics Engineering
Karpagam College of Engineering
Coimbatore, Tamil Nadu, India
Email:

K. K. Dharun
Department of Electrical and Electronics Engineering
Karpagam College of Engineering
Coimbatore, Tamil Nadu, India
Email:

A. G. Vishal
Department of Electrical and Electronics Engineering
Karpagam College of Engineering
Coimbatore, Tamil Nadu, India
Email:

Abstract **–** The fast evolution of Internet of Things (IoT) technology has helped to implement intelligent and automated security systems for the boundaries of agricultural fields, industrial areas, forest areas, and restricted zones. The traditional security measures, such as fences, are not efficient in providing security. To overcome these problems, this paper proposes a solar power-based IoT smart security fence using the ESP32 microcontroller. The proposed system includes different types of sensors such as PIR sensor for detecting intruders, vibration sensor to detect tampering of the fence, smoke sensor to detect fire, and others. The sensor data are continuously sensed and processed using the ESP32 microcontroller. The ESP32 microcontroller helps to make decisions in real time. The detected events are displayed using an LCD display. The sensor data are also sent to the cloud using the IoT platform. The detected events are sent to the cloud using the IoT platform. The LCD provides an immediate alarm using a buzzer. The proposed system uses solar power with battery backup to reduce power consumption. Experimental implementation proves the feasibility of reliable intrusion detection, efficient power management, and effective remote monitoring. The proposed system is a cost-effective, scalable, and energy-efficient approach for modern perimeter security applications.

Keywords: *Smart Perimeter Fence, IoT Security, Solar-Powered System, ESP32 Microcontroller, Remote Monitoring, Intrusion Detection.*

1. INTRODUCTION

Internet of Things is a rapidly changing technology that connects physical devices, sensors, and embedded systems to the internet and enables them to collect, process, and exchange data automatically. IoT systems use a set of devices consisting of sensing units, microcontrollers, communication units, and cloud platforms to achieve the goal of monitoring and controlling the physical environment. IoT systems reduce the need for human intervention and provide the ability to monitor the physical environment continuously. These features have made IoT a widely used technology in many applications, including smart cities, healthcare systems, industrial automation systems, agricultural systems, security systems, and many others.

Smart fencing systems are an innovative extension of IoT technology in the domain of IoT security systems. Smart fences are not only physical boundaries but also

ISSN 2581-7795

intelligent systems that use various types of sensor devices, such as motion detectors, vibration detectors, fire detectors, and smoke detectors, to monitor the fence and the surrounding environment. The sensor devices send the monitored data to the microcontroller, which processes the data and sends it to the remote monitoring system.

The increasing demand for smart perimeter security systems results from the increasing complexities in the security of agricultural lands, industrial areas, forest areas, and restricted zones. The conventional methods employed to secure such areas, such as surveillance and ordinary electric fences, are not efficient and often result in time-consuming and ineffective solutions. These methods cannot accurately determine the exact location of the intruders or the occurrence of environmental hazards such as fire at an early stage. This may result in serious consequences such as the destruction of crops, damage to equipment, and financial losses.

To overcome the difficulties, the IoT-based smart fencing system is an intelligent and reliable solution to the security system. Further, the use of low-power and high-performance microcontrollers, such as ESP32, allows for efficient processing of the data. The use of renewable energy sources, such as solar power, also allows for continuous system functionality, especially in remote areas where there is no connection to the main power grid. Overall, smart fencing systems ensure security, cost efficiency, and scalability, thus making them an efficient solution in modern security applications.

2. LITERATURE REVIEW

Recent research on smart security systems for perimeters using smart security systems revealed significant advancements in integrating IoT systems with microcontrollers to ensure efficient monitoring using smart decision-making. For example, Syahrani et al. (2025) proposed an IoT-based smart security fence system using an ESP32 microcontroller with the Blynk IoT system.The system was designed to provide efficient functionality, including the acquisition of real-time sensor data, mobile-based notifications, and remote control functionality. The results of the study indicate that microcontrollers can provide efficient IoT-based smart fence systems, which can monitor and communicate with other devices over wireless networks. The results of the study also indicate the effectiveness of cloud-based dashboards, which can provide efficient human oversight, especially in perimeter security applications. The results of the study also indicate the effectiveness of cloud-based dashboards, Machine learning and advanced data analytics have also been applied to enhance intrusion detection accuracy and robustness in perimeter security architectures. Pitafi et al. (2024) also proposed a novel machine learning model for the detection of perimeter intrusion using image datasets and deep learning architectures such as InceptionV3 with the incorporation of clustering algorithms. The results obtained using the machine learning model were better than the traditional methods, indicating the significance of using sensor data and pattern recognition algorithms to improve the discrimination between intrusion types in complex environments. Although the authors did not focus on the detection of intrusion using sensor data, the significance of using data fusion and intelligent processing algorithms in IoT security systems, especially when sensor data may be noisy or uncertain, cannot be overlooked.

The integration of renewable energy with IoT sensor networks has been investigated to overcome the power autonomy issues faced in remote perimeter security systems. Deekshitha Reddy et al. proposed an IoT-based electric fencing system with solar power, where the system would provide alert services in case of intrusions and also be integrated with the ThingSpeak cloud platform. The authors proposed the design of the system with the integration of solar power and battery backup to provide continuous power to the system, proving the feasibility of integrating renewable energy with IoT sensor networks to provide continuous services such as surveillance. The authors also proved the efficiency of the system in the utilization of power, which is an important factor in the implementation of smart agriculture and environmental monitoring systems.

ISSN 2581-7795

IoT security frameworks have also been a key area of interest for various studies in the recent past, particularly in the development of more robust intrusion detection systems and improving the resilience of IoT systems to cyber-physical attacks. In a study by Qaddos et al. (2024), the authors developed a novel IoT intrusion detection framework aimed at optimizing the security of IoT networks using a combination of behavioral analysis and anomaly detection mechanisms. This study highlights the potential for IoT systems, including the sensor network and communication links, to be secured from unauthorized access and malicious use. Although the study was conducted in the broader IoT security domain, the security principles can be adopted for the development of more robust perimeter security systems that utilize IoT-based sensor networks and wireless communication.

Literatures that specifically deal with embedded IoT controllers and real-time sensing have emphasized the significance of microcontroller platforms such as ESP32 in surveillance and monitoring. Sabit and Azlan (2025) have conducted an evaluation of the IoT security system using the ESP32 microcontroller and PIR motion sensor devices for the detection of intrusions in a real-time environment. From the evaluation, the low power consumption and the ability to communicate with the cloud platform for dissemination of the data have been established. Additionally, the ESP32 microcontroller has been established as a primary controller for the distributed security networks due to the ability of the ESP32 to interface with the different sensor devices using the inbuilt Wi-Fi protocol.

In addition to the above, the recent developments in the intrusion detection system for IoT networks have established the importance of using intelligent security models. Koroma et al. (2026) have conducted a study to determine the efficiency of using the ensemble learning and deep learning models to optimize the intrusion detection system, especially for IoT and IIoT networks. Based on the study, the efficiency of the different models has been established, and the study has demonstrated the efficiency of using the ensemble of the analytical models to optimize the efficiency of the intrusion detection system. This has established the importance of using the intelligent security models.

3. System Methodology

Figure 2 depicts the block diagram of the proposed IoT-based smart security fence. It comprises a solar panel and a battery as the PSU, various sensors as input devices, ESP32 as the CPU, and the alerting/communication module as the output device. The solar panel harnesses the energy from the sun and stores it in the battery for uninterrupted operation. The PIR sensor, vibration sensor, fire sensor, and smoke sensor sense the intruders and alert the ESP32 microcontroller. As soon as the ESP32 detects the intruders or any irregularities in the security fence, it alerts the alarm unit for immediate alerting and displays the status of the security fence on the LCD screen. In addition, it sends the alerting signals to the IoT platform using the Wi-Fi communication module embedded in the ESP32 microcontroller. This ensures the uninterrupted operation of the security fence using the solar panel and the battery for the uninterrupted operation of the security fence.

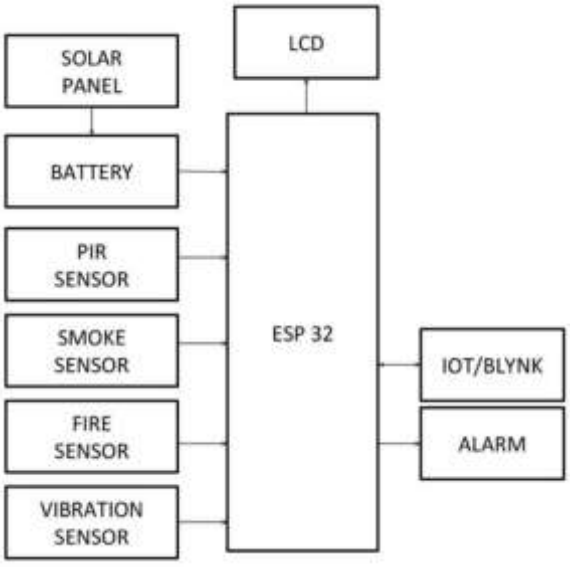

Figure 1 Block Diagram of the proposed system

Solar Panel

ISSN 2581-7795

The solar panel is used as the main source of energy for the smart perimeter security fence system. It converts the sunlight into electrical energy in the form of photovoltaic cells, which utilize the photoelectric effect. The DC voltage available from the solar panel is used to supply the ESP32 microcontroller, sensors, display unit, and communication devices during the daytime. Additionally, the solar panel charges the battery, which helps the system to function during low sunlight conditions. The use of solar energy also allows the system to be independent of the main power source, which is essential for agricultural fields, forest boundaries, and other remote areas. Moreover, the use of solar energy enhances the sustainability of the system, which results in less carbon emissions and operating costs.

Battery

The battery serves as the energy storage component in this system, which stores electrical energy produced by the solar panel. The battery provides a continuous and stable power supply to the ESP32 microcontroller, sensors, LCD display, and alarm unit during nighttime and on cloudy days. The battery provides uninterrupted power to the system, which can be used to monitor and process information and generate alarms irrespective of the environmental conditions. The battery provides a stable voltage supply to the components in the system, which protects them from being damaged by power fluctuations. The components can be powered by the solar panel and the battery to ensure uninterrupted operation.

PIR Sensor

The Passive Infrared (PIR) sensor is used for motion detection along the perimeter. The PIR sensor detects changes in infrared radiation emitted by warm objects. Therefore, when the object is moving within the range of detection of the PIR sensor, it sends a digital signal to the ESP32 microcontroller. The PIR sensor is commonly used in security systems because of its low power consumption, cost-effectiveness, and high detection reliability.

Smoke Sensor

The smoke sensor, which is usually an MQ series, can be MQ-2, MQ-4, or other MQ sensors, is used to detect the presence of smoke and other combustible gases near the perimeter fence. This type of sensor can detect the change in concentration of the gases and convert them into an electric signal. Early detection of the presence of smoke can help identify potential fire-related hazards, especially near agricultural fields, forest boundaries, and industrial zones. This can be done through the ESP32, which can then send alerts through the IoT platform and alarm unit.

Fire Sensor

The fire or flame sensor can detect infrared radiation, which is usually emitted by open flames. This type of sensor can constantly monitor the surrounding area for fire-related signals. This can provide a quick response to the presence of flames. When there is a fire, the fire sensor sends an alert signal to the ESP32, which can then send an instant notification. This can be very useful for preventing fire-related damage, especially in sensitive zones.

Vibration Sensor

The vibration sensor is used for the detection of physical disturbances. Physical disturbances include cutting, climbing, or tampering with the fence. The vibration sensor detects the vibrations in the fence. The vibrations are then converted to electrical signals. If there is any abnormal vibration in the fence, it will send out a warning signal. The vibration sensor is used to increase the robustness of the security system. The robustness of the security system is increased with the inclusion of the vibration sensor. The inclusion of the vibration sensor increases the security of the fence.

ESP32 Microcontroller

The ESP32 microcontroller is used in the development of the smart security fence. The ESP32 microcontroller is used as the main controller of the security fence. The ESP32 microcontroller receives input signals from all the sensors. The ESP32 microcontroller then processes the input signals. The ESP32 microcontroller then generates the response to

ISSN 2581-7795

the input signals. The ESP32 microcontroller has Wi-Fi and Bluetooth capabilities. The ESP32 microcontroller is used to control the LCD display unit. The ESP32 microcontroller is used to control the alarm unit. The ESP32 microcontroller is used to increase the robustness of the security system.

LCD Display

The information on the LCD display screen provides a real-time interface for monitoring the local system. The information includes the status of the sensors, intrusions, environment, battery percentage, and the operation of the system. The information enables users of the system at the local site to understand the status of the system and take the necessary actions. The LCD display screen enhances the transparency of the system.

IoT / Blynk Platform

The IoT platform, such as Blynk, helps to remotely monitor and control the perimeter security system using mobile devices and web interfaces. The sensor status and alert messages are sent to the cloud platform in real time using the ESP32 module's Wi-Fi capabilities. The users get instant alerts during intrusions, fires, smokes, and tamper situations. It also allows users to visualize system status and is highly scalable, which is beneficial for smart security system applications.

Alarm Unit

The alarm unit is used for alerting the user in the event of a breach, fire, or any other alarming condition. This alarm acts as a deterrent for anyone who attempts to breach the security of the system. The alarm is activated by the ESP32 module in the event of unusual readings from the sensors. This alarm is a dual alerting system for the security of the device.

4. Result and Discussion

Figure 2 illustrates the hardware prototype of the proposed IoT-based smart security fence system. The hardware configuration includes an ESP32 microcontroller connected to a customized PCB and a 16×2 LCD display for real-time monitoring. The hardware configuration also includes various sensors and LEDs connected to the PCB for monitoring the intrusion and hazard detection systems. The hardware configuration includes a 12V lithium-ion battery for storing power and a solar panel to provide the system with renewable energy and store power in the battery to provide continuous operation to the system. The hardware configuration also includes a relay and control unit to provide the system with the power to operate continuously. The wiring configuration represents the complete working model of the smart security system.

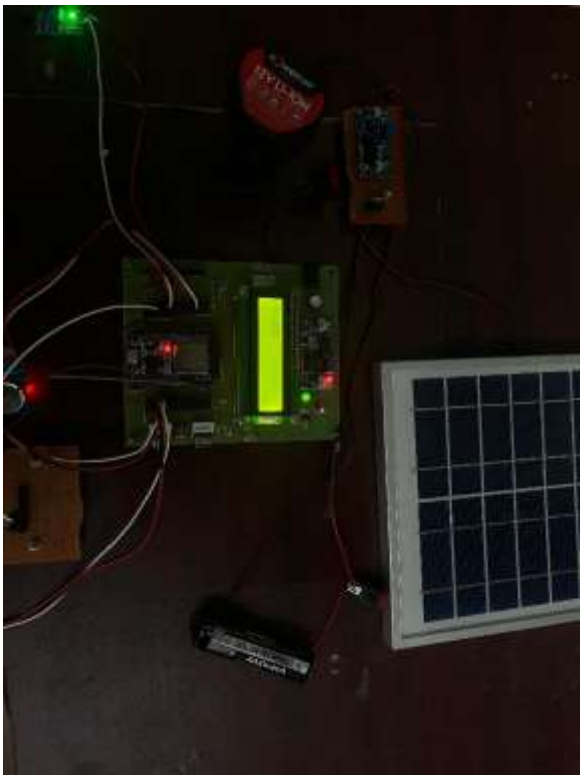

Figure 2 The hardware prototype of the proposed IoT-enabled smart perimeter security fence system

5. Conclusion

The proposed security system for a smart security fence that utilizes IoT technology offers an effective,

ISSN 2581-7795

sustainable, and intelligent solution to modern security fencing and protection challenges. The proposed security system utilizes a solar panel and a battery to ensure continuous operation in a remote area, and the ESP32 microcontroller allows for efficient data collection and communication with other devices wirelessly. The security system utilizes a series of sensors, including a PIR sensor, a vibration sensor, a smoke sensor, and a fire sensor, to ensure that there is comprehensive detection and alertness to security breaches and other hazards that may occur around the security perimeter. The proposed security system offers a number of advantages and benefits, including improved situational awareness and faster reaction to security breaches and other hazards that may occur around the security perimeter, and it can be used to protect various areas such as farms, industrial areas, forests, and borders. The proposed security system offers a practical example of the benefits that can be achieved by utilizing IoT technology and other technologies in security applications, and it can be further improved to offer more accurate and efficient security protection.

REFERENCES

[1] F. P. Syahrani, H. K. Saputra, S. Anori, W. Agustiarmi, F. T. Ayasrah, and P. V. Thanh, "IoT-Enabled Smart Fence: Remote Security and Monitoring Using NodeMCU ESP32 and Blynk," *Journal of Hypermedia & Technology-Enhanced Learning*, vol. 3, no. 1, pp. 1–15, Jan. 2025, doi: 10.58536/j-hytel.158.

[2] J. Arshad, M. A. Azad, K. Salah, W. Jie, R. Iqbal, and M. Alazab, "A Review of Performance, Energy and Privacy of Intrusion Detection Systems for IoT," *arXiv preprint*, Dec. 2018.

[3] H. B. Jatiyoso, M. F. Riadi, A. Atturoybi, A. Mardamsyah, and H. Tjahjadi, "Development of PIR Sensor-Based Security System and IoT-Based ESP-32 Wrover CAM Module for Monitoring Military Headquarters and Vital Objects," *Jurnal Mandiri IT*, vol. 14, no. 1, pp. 191–197, Jul. 2025, doi: 10.35335/mandiri.v14i1.437.

[4] R. W. Anwar, M. Abrar, A. Salam, and F. Ullah, "Federated Learning With LSTM for Intrusion Detection in IoT-Based Wireless Sensor Networks: A Multi-Dataset Analysis," *PeerJ Computer Science*, vol. 11, Art. e2751, Mar. 2025, doi: 10.7717/peerj-cs.2751.

[5] A. Biju and S. W. Franklin, "Dual Feature-Based Intrusion Detection System for IoT Network Security," *International Journal of Computational Intelligence Systems*, vol. 18, Art. 66, Mar. 2025, doi: 10.1007/s44196-025-00790-y.

[6] S. Murthy Andhe and J. M. Dasari, "IoT Based Home Security: Experimental Prototype Case Study Using ESP32 and Arduino IoT Cloud," *International Journal of Creative Research Thoughts (IJCRT)*, vol. 13, no. 6, pp. 1–8, Jun. 2025.

[7] "IoT-Based Real-Time Object Detection System for Crop Protection and Agriculture Field Security," *Journal of Real-Time Image Processing*, vol. 21, Art. 106, Jun. 2024, doi: 10.1007/s11554-024-01488-8.

[8] R. W. Anwar, M. Abrar, A. Salam, and F. Ullah, "Federated Learning With LSTM for Intrusion Detection in IoT-Based Wireless Sensor Networks: A Multi-Dataset Analysis," *PeerJ Computer Science*, vol. 11, Art. e2751, Mar. 2025, doi: 10.7717/peerj-cs.2751.

[9] Institutional authors, "IoT Security: A Deep Learning-Based Approach for Intrusion Detection and Prevention," IEEE, 2023.

[10] Institutional authors, "Revolutionizing Security Measures for Enhanced Perimeter Protection and Intrusion Detection," IEEE, 2024.