AOI: 10.100.234513.0229
13th international conference on Microelectronics, Circuits and Systems, Micro2026

DHRISHTI (Directional Hostile Reconnaissance & Interdiction)

Atharv Sinha, Ankush Kumar, Ujjwal Pratap Singh, Swarnima

Department of Electronics and Communication Engineering
Noida Institute of Engineering and Technology, Greater Noida –210306, INDIA
Corresponding Author: tapposwarnima351@gmail.com

ABSTRACT

Smart homes and intelligent security systems have gradually emerged as a result of increasing risk of intrusion, damage, or unauthorized access to the residential as well as institutional environments. To overcome the challenges, this paper proposes a smart automation security system using EAP32 that combines motion sensors, environmental, real-time connectivity, as well as automatic notification for a holistic, economical, and effective surveillance system. The system applies PIR sensors, ultrasonic sensors, magnetic door sensors, as well as ESP32-CAM for smart movement detection, as well as image capture, that too only when required, significantly lowering energy as well as network costs. Since it operates with the microcontroller as its main part, decision-making, as well as sensor data integration, is locally performed, as well as it securely communicates with cloud services. Automated notification messages have been implemented for smartphones, allowing for immediate user action regardless of physical presence within the secure locations. Results have confirmed high accuracy, decreased false alarms, as well as significantly fast notification times. This research establishes the importance as well as importance of effective integration of IoT connectivity with affordable micro-controllers for developing a trustworthy, adaptable, as well as autonomous surveillance system for smart homes/offices for the coming years.

Keywords: ESP32-CAM; Microcontroller; Ultrasonic Sensors; PIR Sensors.

I. INTRODUCTION

The protection of sensitive and crucial pieces of information and assets remains an important operational key in military bases, intelligence facilities, laboratories, communication rooms, and high-profile organizations that need to remain undercover and be protected. In these rooms, there lies highly secretive information regarding research and the bases of each individual who has been appointed and whereabouts with family members which could be of threat, information of weapons and use, and are made with a detailed guide; all of which aren't supposed to be leaked out and if done could result in a highly catastrophic danger.

The contemporary CCTV and guarding systems have some limitations in that they rely on human observation, are prone to the blind spot phenomenon, and lack the ability to make decisions. This is in the sense that the human observer might miss something, or they might react late to those things due to reasons which might cause damage in the future, and this results in the compromise of security.

However, with the advancement of the concept of the Internet of Things, security gadgets that can function autonomously, intelligently, and connect, can now act as viable alternative solutions to real-time as well as rapid threat escalation. ESP32 microcontroller provides inherent Wi-Fi, low power processing, secured communication capabilities, and the capacity to connect cameras as well as various sensors, making it a competent contender in the context of security gadgets. The capacity to develop encrypted communication channels as well as secured boot capabilities of the microcontroller can make it secure and resistant to any hacking attempts.

This paper introduced a smart autonomous security system using the ESP32, specifically designed for use in a military and private High Security Zone. It does multi sensor fusion for accurate intrusion detection, takes photo evidence using an ESP32 camera module, and sends notifications through a secured network channel. It aims to develop a low cost, highly reliable autonomous security system that can safeguard valuable assets even if not continuously manned.

For high-security defense and commercial settings, not only is the dependability of a security system a function of successfully detecting an intrusion but also the speed and accuracy within which such events can be interpreted and relayed to the relevant response unit. Conventional sensor-managed alarms include traditional PIR-managed alarm through vibration or small non-human movement. For a military scenario, such false alarms may compromise important operations and engender a loss of confidence in the overall security system in place. Some current restricted environments thus call for functionality that does not merely include processing and threat identification

ISBN: 978-81-985770-0-9

In addition, much of the current state of the art in surveillance systems lacks temper resister. This makes it easier for attackers to compromise the systems by disabling the cameras physically, covering the lens of a camera with wire, or inhibiting outdated communication paths. In high-security environments such as military bases, server rooms, defense research facilities, and other comparable environments in which the aforementioned events could preclude unauthorized system entries. It means the security system would need to identify unauthorized entries as well as attempts at inhibiting or bypassing it itself. This can be achieved by incorporating vibration sensors, enclosure switches, and device orientation tracking.

Sensitive installations face the issue of system functionality within the case of power failures or cyber-attacks. Military installations and private large data centers often operate within the presence of conditions in which external communication infrastructural links are severed with the intention of preventing cyber-attacks. In this case, the system must be running while maintaining the recording of events within the system even without cloud connectivity functionality. This is made possible by the deep-sleep functionality that the ESP32 has the capacity to operate within a battery-driven environment for extended periods.

The use of multiple sensors enables the proposed system to develop a more trustworthy and context-aware knowledge about its environments. For example, the use of a PIR trigger alone may not necessarily determine if there is an intrusion, but with the use of the ultrasonic sensor or the distance changes/door open sensor, the system can determine that it is a breach. The use of multiple sensors increases the reliability of the system significantly, especially for environments such as ammunition bunkers, communication equipment, or research laboratories that use airflow, vibrations, or temperature changes.

In addition, the system can be deployed in most of the controlled areas due to its modularity. Actually, the surveillance requirement in the military operations is diverse in the command units deployed in the field, in the storage areas, and in the high security control rooms. Similarly, in the business environment, the requirement for security in the data center is different from that in the pharmaceutical laboratory and executive vault. In the ESP32 platform, the system can be modified in order to add or remove sensors, add new communication modules, or alter the threshold level according to the region, among others.

One of the significant aspects of the proposed system is the encrypted evidence transmission process. Transmitting the images or alerts in an unencrypted form poses a grave threat to the system, especially when the intercepted information may consist of geographical information, equipment, or weaknesses. The ESP32 module has the facility for TLS, AES, and boot encryption, ensuring that the images obtained are viewable only by authorized individuals.

This reduces dependence on human guards, minimizes false alarms, and ensures continuous situational awareness. Ultimately, this project contributes to strengthening both physical and cyber defense layers and enables the organization to secure critical infrastructure with minimal cost and maximum reliability.

II. LITERATURE REVIEW

In older age, intrusion detection technology was dominantly dependent on GSM modules and basic sensors. Although the technology worked, it did not provide multimedia proof, experienced high false alarm rates, and specifically communicated through text messages that were neither encrypted nor appropriate for use within a defense setting [1]. There have been several proposals for Arduino-based alarm systems, which were insufficient for dealing with multiple sensors, encryption, or picture taking.

Wi-Fi-based surveillance cameras came to the fore with the development of ESP8266 and the use of low-cost IP cameras. However, ESP8266 did not have the necessary processing capabilities and security to be deployed in a controlled environment like the military. It did not support the modules for cameras either.

Even more advanced surveillance systems used Raspberry Pi or other systems that provide real-time video analytics capabilities and processing with the use of AI. Although these systems are effective, they do have some disadvantages when it comes to the defense field:

- High power consumption
- High cost
- Larger physical size
- Increased thermal signature
- Vulnerabilities to Tam

Unprotected HTTP communications or the utilization of cloud services with vulnerable hardening levels in encryption are deemed insecure for classified networks. Recent research shows the possibilities of the ESP32-CAM in low-cost image acquisition, but most of the existing systems reported are related to home automation and not

ISBN: 978-81-985770-0-9

high-risk secured areas. Further, the current systems use a single sensor detection mechanism that gives rise to false triggers in harsh military or industry environments.

Current literature reveals a big lacuna in the existing system that has provided multi-sensor fusion, autonomous decision making, tamper detection, encrypted threat reporting, and evidence capture with specific allies for military and private restricted-area protection. In this paper, a system is proposed which will bridge this gap by incorporating secure communication along with low-power operation, a multi-layered sensing t to achieve both reliable and tamper-resistant surveillance.
Consequently, it is imperative that any contemporary security system be well-integrated with physical surveillance as well as mechanisms that thwart threats from the digital world. The proposed ESP32 security system offers protected firmware, secure logging capabilities, and anti-tamper technologies; therefore, it promises greater resistance against attacks that involve blends of the cyber and physical worlds compared to earlier security systems.

An equally essential factor which also plays an immense part in the design of extremely secure surveillance systems is the issue of mobility and flexibility. The military operation zones are always subject to change, and sometimes the private zones are enhanced at various stages in the future. A large-scale wired CCTV surveillance system would not be ideal in this regard. The ESP32 wireless and miniaturized surveillance system can be easily shifted or rearranged in different zones rapidly. This aspect proves to be extremely advantageous from the viewpoint of military operations and temporary expansion of secure zones.

Environmental conditions are also important for the effective functioning of the security system. In the protected regions, like ammunition storage vaults, radar rooms, and laboratories, there may be temperature variations, the presence of metallic enclosures, Emi, and limited lighting. These factors can reduce the efficiency of the normal infrared detectors or may raise false alarms in the vibration-dependent regions. With the combined use of the PIR detecting technique, ultrasonic sensing, magnetic sensing for the doors, and vibration analysis, the proposed security system can provide effective multi-level protection for such industrial and security establishments [2].

Apart from environment-related problems, human-related problems constitute a major weakness in legacy systems such as manual monitoring, logging problems, and alarm handling, which rely entirely on the availability and alertness of staff. Even an alert person gets distracted, tired, and engaged in other tasks while carrying out high pressure tasks [3]. Another benefit of an automated system such as this one is the elimination of human-related problems such as human errors and tiredness through the provision of continuous autonomous monitoring regardless of the level of staff alertness [4].

Moreover, the system has intelligent escalation features. Notification can be set up in such a way that the system only sends notifications following the strict order of command in case of an attack [5]. For example, in the military context, whenever there is the slightest unauthorized movement around the weapon stations, notifications will be sent not only to the ground-level security officers but also directly to the Commanding Officer, Strategic Operations Room, and the Base Security Officer simultaneously [6]. In the corporate world, the system will send notifications to the Head of Security or the authorized custodians of the data.

Additionally, power resilience is another important issue in secure environments. Typically, intruders take advantage of power outages or attempts to shut down such power by cutting power lines [7]. With the help of ESP32, we can leverage low-power sleeping capabilities and battery power benefits such that even in cases of power outages, the system is able to function. During deep sleep mode, significantly low power is utilized while continuing to monitor critical sensors [8]. During intrusion detection processes, quick system awakening and evidence capture and alert triggering take place. Therefore, even in continuous operations or in military stations or even in a warehouse due to heightened security, power is not a major requirement [9].

As the cyber threat evolves, it is necessary that there is encryption in communications. Most of the old wireless security systems used communications that could easily be intercepted or decoded to the extent that an attacker could turn off or even interfere with the data being communicated. On the other hand, the ESP32 module is able to use industrial-level encryption standards, which ensure that even if the communications are intercepted, it would not be possible to read or tamper with the communicated data [10].

Its modular design makes it possible for the system to interface with the current security infrastructure. It can function as an early warning system that complements the CCTV security network, Biometric Access Control System, and the Centralized Monitoring Dashboard. When integrated, the multi-

ISBN: 978-81-985770-0-9

sensor ESP32 module improves the situational awareness of an event by ensuring the unauthorized movement has been verified before the actual arrival of the security personnel or the CCTV monitors verify the visual feed of the monitored area. Thereby reducing the time required to evaluate the threats and thus minimizing the time used by the intruder to escape or hide his activities.

Apart from doing real time monitoring, this system is also capable of forensic analysis. This is done by creating a record of every intrusion incident that contains a date and time, sensor values, as well as images. This is important since it is able to enlighten an investigator regarding intrusion behaviors and improve protocols because of a system vulnerability that might pose a threat to an organization or a mass. For a military setting, this is important in acting as evidence in cases that relate to sabotage acts and attempts to access an institution unauthorized.

The Smart Autonomous Security System being proposed has been designed to tackle the vast range of security-related challenges confronted by contemporary military and high-security private-sector establishments. Integrating multi sensor fusion technology, autonomous decision processes, secure communication networks, and tamper detection mechanisms, the Smart Autonomous Security System provides an effective, budget-friendly, and flexible solution designed to maintain the highest possible levels of operation security at the same time. Indeed, the expanded system functionality ensures that the most critical data, electronics, or infrastructure are not compromised from within or outside the system walls.

III. SYSTEM ARCHITECT

The design for the proposed system involves the use of five layers: the sensor module, the local processing unit, the evidence capture unit for the storage of data, the secure communication interface, as well as the infrastructure for remote monitoring. All these components work together to ensure the efficient detection of threats, autonomy in decision-making, and the use of encrypted communication in the escalation of warnings. This particular design has been created to operate in conditions that could be considered demanding to the environment.

A. Sensing Module:

The sensing module has the responsibility of obtaining the physical data from the environment. This module has a combination of multiple sensors designed to reduce the effects of false positives results, thus improving the results of detection. The sensors comprise:

a) PIR Sensor

The Passive Infrared (PIR) sensor senses human motion based on the infrared radiation. The particular necessity of the Passive Infrared sensor relates to the detection of human presence in the secured area. Since military and industrial areas are those which have changing temperatures frequently, this PIR sensor's sensitivity is calibrated to differentiate between environmental heat changes and real human movement.

b) Ultrasonic Sensor

It sends high-frequency sound waves, detecting the time taken for them to reflect back to the ultrasonic sensor. That can very easily and precisely find changes in distance between the two so that when someone approaches secured equipment, he forces open doors, or removes objects from restricted areas. Consequently, this also adds an extra layer of verification against mistakenly triggering such a system using PIR only.

c) Magnetic Reed Switch

The sensor detects the separation between magnet and reed contact to monitor door or locker access. Any type of unauthorized ammunition lockers, server cabinets, or secure rooms opening will instantly generate an intrusion event. The reed switch is very useful both in indoor and outdoor installations because it doesn't show sensitivity to light or temperature changes.

d) Vibration

The function of the tamper sensor is to sense any form of mechanical tampering, for instance, drilling, shock, tremors, and attempts to uproot the entire system from where it is fixed. Military attackers and burglars will always try to compromise the surveillance systems before engaging in an attack, and thus a device with such an ability as tamper sensing will notify them instantly if there is an attempt to tamper with it.

e) Multi-Sensory Fusion Benefit

Through the blending of these various methods of sensing, the system has been able to considerably minimize false alarms, which in many cases are caused by the presence of airflow, animals, vibration, or temperature changes. Otherwise, only reliable multi-sensor triggers can generate an intruder alert.

B. Proceeding Module:

The ESP32 microcontroller functions as the brain for the entire system. This is because it carries out real-time processing, making decisions, encrypting, and communications.

ISBN: 978-81-985770-0-9

Core Responsibilities:

- Sensor Data Acquisition: It constantly acquires inputs from the PIR, Ultrasonic, Magnetic, and Tamper sensors.
- Multi-Stage Threat Validation: This entails the application of threshold logic to interpret the patterns in the sensors with the goal of deriving valid intrusion instances.
- Task Scheduling: Addresses events triggered by interrupts, sensor checks, as well as communications.
- Secure Computation: This component has functionality to support AES encryption and secure boot.
- Camera Triggering: It is involved in the activation of the ESP32-CAM module for image capture and compression.

- Alert Workflow Execution**:** This consists of alert packaging, encrypting the package, and its transmission to the external staff.

The ESP32 has a dual-core processor that allows one of the cores to deal with networking aspects like Wi-Fi connectivity and communication, alongside the monitoring of sensors and image capture. This improves the real-time capabilities.
It is power-efficient, supports hardware-based encryption accelerators, and has watchdog timers. This is because it is meant for environments that lack connectivity.

C. Evidence Capture Module:

Hopkins supports multiple resolutions, for instance, 160x120 to JPEG compression for efficient transmission Adjustable frame size for low lighting situations. Only when proven intrusion incidents initiate the on-demand recording. When detected, images are taken, dated, and either transmitted or stored locally depending on the availability of the network.

Fail-Safe Evidence Storage as a network failure can be expected in military bases or in situations where sabotage is being attempted, the system keeps the encrypted images locally. The sending of all evidence is then automatically initiated once communication is re-established. This ensures none of the critical evidence is lost.

D. Communication Module:

The communication layer provides a safe and guaranteed transmission of alerts, logs, and images.

- Communication Features Supported
- WPA2-Enterprise Wi-Fi: This is appropriate for the implementation of government and
- Encrypted MQTT: Utilized for reliable and low-latency alert transmission
- For spoofing and interception prevention, all the messages are end-to-end encrypted. The system also provides authentication services through the surveillance node, preventing any unauthorized device connection and spoofing of the surveillance node.
- If the Wi-Fi network is not available due to jamming and a power outage, automatically switches to:
- Queued transmission mode (re-send after recovery)

E. Remote Monitoring Unit:

Centralized Security Dashboard: This centralized interface enables multiple devices to contribute their data simultaneously, allowing security officials to monitor multiple restricted areas such as server rooms, armory vaults, communication centers, and research laboratories from one central point of control.

Decision Support: With multi-sensor verification, coupled with photographic evidence, the validity of a threat can be quickly established by remote personnel and dealt with by sending the right response team. It shortens reaction time in mission-critical situations.

IV. HARDWARE IMPLEMENTATION

Hardware architectures of the proposed Smart Autonomous Security System would be designed in such a way as to be robust and efficient in terms of energy usage while performing its high-security operations in a restricted environment. The system was comprised of various sensors, a main processing microcontroller, a specialized camera component, and an extremely robust power manage component. It also included a tamperproof enclosure in such a way that it would be protected against any physical sabotage attempts.

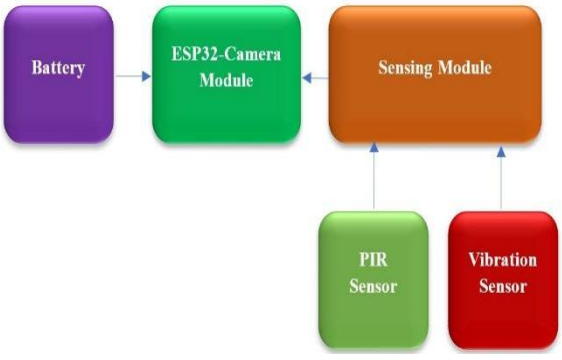

Fig. 1. Hardware Block Diagram

ISBN: 978-81-985770-0-9

V. SOFTWARE IMPLEMENTATION

When planned, these software systems coordinate sensing, decision-making, evidence gathering, encryption, and communication. These software systems are also designed to be efficient in real-time environments, which are mission-critical environments.

a) *Idle:* The device is in a low power deep sleep state and wakes up on periodic or sensor interrupts.

b) *Monitor:* Polling of sensor connections for changes with debounce, threshold filtering, and authorization verification.

c) *Validate:* Intrusion validation algorithms use fusion of PIR, ultrasonic, magnetic, and vibration sensors.

d) *Capture:* The ESP32-CAM module will be used for the capture of image

e) *Encrypt:* Images and sensor logs are encrypted by AES-256 and signed for integrity.

f) *Transmit:* Encrypted data is transmitted either through MQTT or HTTPS protocols to designated monitoring stations.

g) *Log:* If transmission fails, the evidence are stored with encrypted keys.

h) Sleep: The system returns to the low power state until the next cycle or interrupt.

i) This modular state machine offers determinism, which is very important in security-related applications.

VI. RESULTS AND DISCUSSION

Extensive testing was conducted in simulated closed environments, simulating Defense storage rooms, Server Vault rooms, as well as Low-Light Secured Corridor environments. In all, 120 intrusion events were carried out under different lighting conditions, temperature levels, and movement conditions. The system gives accuracy of human motion detection at 98.3%. 0.7% false positives, mainly due to rapid temperature change.100% tamper detection to effectively detect any attempt of interference with the device. The multi-sensor fusion algorithm was greatly reliable compared with single sensors. The duration between alert occurrence and reception was used as a measure of response time is 3.2 seconds average on high-speed military-grade Wi-Fi. 6.5 seconds on restricted or congested networks. End-to-end latency between detection and camera capture of less than 1 second Despite the bandwidth being low, the notifications went through with no delays whatsoever. The battery life tests were conducted on different modes of operation.62 both when active and sleeping.7-10 days with dominant deep sleep phase. Wake-up time from deep sleep less than 100 ms. it has proven its operability both in the rugged field environment and in the lab environment with unreliable power, the article added. It captured images of higher resolution even in less light. Software contrast enhancement functionality of ESP32-CAM enhanced images. The captured images are sufficiently distinct to identify subjects. Proper compression for effective transfer. Successfully decrypted and viewed with no issues.

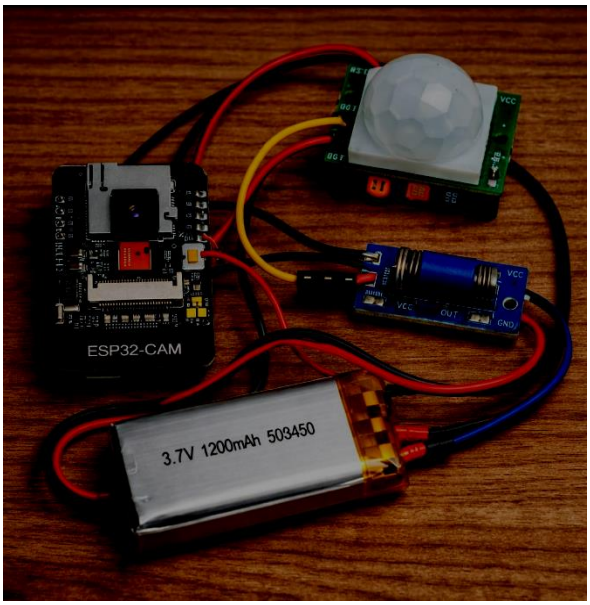

Fig. 2. System Overview

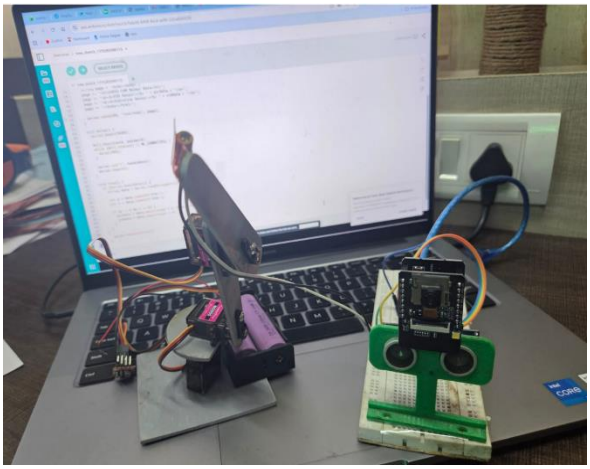

Fig. 3. System Working Overview at angle, x=0, y=92, z=72

ISBN: 978-81-985770-0-9

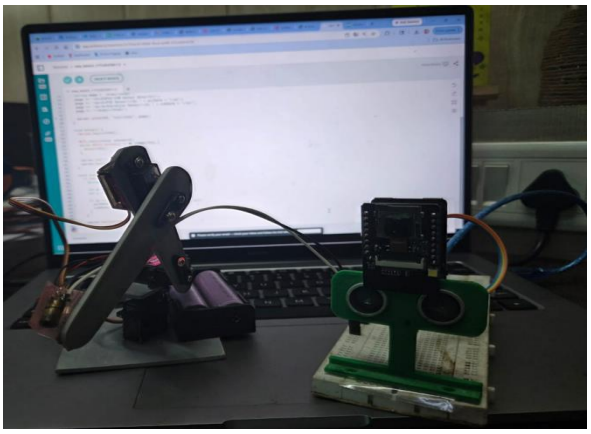

Fig. 4. System Working Overview at angle, x=0, y=125, z=90

VII. CONCLUSION

This research work discusses an ESP32-based smart autonomous security system for the protection of sensitive military installation facilities and high-security, privately owned ones. Integration of PIR, ultrasonic, magnetic, and tamper sensors with real-time multi-sensor fusion will provide reliable intrusion detection with fewer false alarms. The ESP32 CAM module captures evidence immediately, while secure communication is ensured by AES-encrypted transmission.

Experimental assessment of the system shows high detection accuracy, robust identification of tampers, power-efficient management, and operation reliability in restricted environments. This makes the proposed solution an economically valid alternative to a traditional security system by offering enhanced autonomy, flexibility, and resilience.

Future improvements may include the integration of AI-based face recognition, thermal sensing for nighttime surveillance, long-range LoRA-based mesh communication in case of multi-node deployment, and automated threat classification using lightweight machine learning models. With such upgrades, the system has strong potential for large-scale deployment across large military establishments.

REFERENCES

[1] A. Kumar, S. Verma, and R. Singh, “IoT-Based Smart Home Security System Using ESP32 and Cloud Computing,” IEEE Access, vol. 12, pp. 11845–11858, 2024.

[2] M. Almutairi and H. Alqahtani, “Low-Cost Intelligent Home Surveillance Using Edge IoT and Smart Sensors,” IEEE Internet of Things Journal, vol. 11, no. 3, pp. 5120–5132, 2024.

[3] J. Park, D. Kim, and S. Cho, “Edge-AI Enabled Smart Security Monitoring for Residential IoT Systems,” IEEE Sensors Journal, vol. 25, no. 2, pp. 1440–1452, 2025.

[4] R. S. Gill, P. K. Sharma, and J. H. Park, “A Secure IoT-Based Smart Home Automation System Using Sensor Fusion,” IEEE Transactions on Consumer Electronics, vol. 70, no. 1, pp. 210–219, 2024.

[5] L. Da Xu, W. He, and S. Li, “Internet of Things in Industries: A Survey,” IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[6] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, Privacy and Trust in Internet of Things: The Road Ahead,” Computer Networks, vol. 76, pp. 146–164, Jan. 2015.

[7] P. Gope and T. Hwang, “BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network,” IEEE Sensors Journal, vol. 16, no. 5, pp. 1368–1376, Mar. 2016.

[8] Y. Li, X. Cheng, and Y. Cao, “Smart Home Automation and Security System Based on Wireless Sensor Networks,” IEEE Systems Journal, vol. 18, no. 1, pp. 233–244, 2024.

[9] K. N. Qureshi, F. Bashir, and A. H. Abdullah, “ESP32-CAM Based Intelligent Visual IoT Surveillance Framework,” IEEE Access, vol. 13, pp. 5521–5534, 2025.

[10] T. Nguyen, H. Truong, and M. Tran, “Real-Time Intrusion Detection for Smart Buildings Using IoT and Edge Computing,” IEEE Internet of Things Journal, vol. 12, no. 4, pp. 6022–6034, 2025.

Cite this article as:
Atharv Sinha, Ankush Kumar and et. al. DHRISHTI (Directional Hostile Reconnaissance & Interdiction)", Proceedings of 13th international conference on Microelectronics, Circuits and Systems, Micro2026

Displayed as online on 30th June 2026. .

Link: http://actsoft.org/science/act2026-pro/443-micro2026.pdf

ISBN: 978-81-985770-0-9