**Journal of Engineering for Development**

*Journal of Engineering for Development, Vol. 18(1), March (2026) pp. 180 – 193*

# MULTI-SENSOR FUSION–BASED INTRUSION DETECTION SYSTEM USING PIR, MICROWAVE, AND MAGNETIC SENSORS

**[1,2]Musa, A; *[1]Isa, A.A.; [1]Balogun, M.O.; [1]Ayinla, W.M.,** and **[1]Abdulfattah, K.**

[1]Department of Electrical and Computer Engineering, Kwara State University, Malete, Nigeria,
[2]Institute for Intelligent Systems, University of Johannesburg, South Africa
*Corresponding Author's Email: abdulrahman.isa@kwasu.edu.ng

## ABSTRACT

*Intrusion detection systems (IDS) deployed in residential and small commercial environments frequently suffer from high false alarm rates and inconsistent reliability when relying on a single sensing modality. To address these limitations, this study presents the design and experimental validation of a multi-sensor fusion–based embedded intrusion detection system comprising of three layers that integrates Passive Infrared (PIR), microwave radar, and magnetic reed switch sensors within an ESP32 microcontroller architecture to enhance detection reliability without relying on machine learning algorithms or cloud-based processing. The experimental performance analysis under controlled setting resulted in 86% and 91% for PIR and microwave sensors and a false positive rate of 12% and 15% respectively, but in comparison the proposed multi-sensor fusion technique shows an accuracy of 99% and a false positive of 1%. This represents a 15.1% improvement over PIR-only operation and a 93.3% reduction in false alarms compared with microwave-only detection. The system maintained a response time below 2 seconds (1.6 s in fusion mode) while operating at a moderate power consumption level of approximately 160 mA, making it suitable for battery-powered deployment. Overall, the results demonstrate that a structured hardware-level sensor fusion architecture can deliver near-ideal detection performance in lightweight embedded systems. The proposed multi-sensor fusion technique is a practical and better system compared to data-intensive AI-based instruction frameworks.*

**Keywords:** Embedded Systems, ESP32, False Alarm Reduction, Intrusion Detection System, Multi-Sensor Fusion, Physical Security, Real Time Monitoring

*Article Information:*
*Received 26 February, 2026*
*Revised 12 March, 2026*
*Accepted 23 March, 2026*
*Available online 15 April, 2026*
*Website:* https://jedev.com.ng/

## 1.0. Introduction

Security is a major critical challenge in several infrastructure such residential, commercial, and industrial. In recent years, several reported unauthorized access, theft and vandalism to both private and public buildings has exposed the weakness in convection surveillance monitoring systems (Chasdi, 2025; Hafez, 2024; Zada *et al*., 2026). In the last decade video surveillance such as the popular closed-circuit television (CCTV) were deployed for monitoring and surveillance but they depend mostly on passive recording of events or activities and also monitoring by human. In many real-world situations, the dependent on human monitoring of live feeds delay in the real time identification of intrusion events and the initiation of appropriate responses (Bing *et al*., 2001). In general CCTV is best suited for analyzing and evaluating past event than for detecting and evaluating real time occurrence of threats, event or other suspicious activities. As security challenges continue to grow, there is need to come up with an intelligent instruction detection system that is capable of automatically detecting anomaly and suspicious activities with delay and reported to appropriate quarters in real time basic. (Anwar *et al*., 2017; Chasdi, 2025; Heidari and Jabraeil Jamali, 2023; Thakkar and Lohiya, 2022).

Sensor-based intrusion detection systems (IDS) is a practical alternative surveillance system developed to serve as a complement to camera-based surveillance. Most previous monitoring systems rely primarily on visual observation but sensor-based IDS continuously track environmental changes and trigger alerts when predefined thresholds are exceeded (Al-Hashemi *et al*., 2024). Motion sensors, vibration detectors, acoustic sensors, and magnetic switches are some of the sensing devices deployed to detect unauthorized activities within both private and public buildings, because they are relatively inexpensive, easy to deploy, and adaptable to different security scenarios (Nosiri *et al*., 2018). Moreover, when integrated into embedded or Internet-of-Things (IoT) platforms, sensor-based IDS can perform localized decision-making with minimal computational overhead and relatively low power consumption (Al-Anzi, 2022; Bocu and Iavich, 2022; Y. Kumar and Kumar, 2023; Racherla *et al*., 2024).

Passive Infrared (PIR) sensors are most widely used for motion detection because of their simple configuration, less costs and low power consumption; they operate by evaluating the variations in infrared emitted by objects (human being) (Godase, 2025; Verma *et al*., 2021); these make them highly suitable for residential security applications. These characteristics make them especially suitable for indoor residential security applications (Summerlot, 2024). In practice, limitations identified in PIR sensors are highly dependent on line-of-sight and also sensitivity to environmental conditions; such as temperature variations, airflow disturbances and changes in lighting conditions sometimes trigger false alarms (Cozens *et al*., 2025). All these are some of the limitations of achieving a reliable intrusion detection when using a single sensing device or sensor.

Another sensing device is the microwave motion sensor that works on the principle of doppler radar principles, microwave signals is transmitted and the characteristics of the reflected waves are studied. The microwave sensors have the capability of detecting movement through obstacles such as glass and thin walls (Nanzer, 2017); making them to have ability to monitor larger areas and partially obstructed environments more effectively. However, the movement

of other objects that are not of concern or environmental disturbances like increase in wind speed usually has an effect on microwave sensors which may lead to high false alarm rates (Al-slemani and Zengin, 2023; Myagmar-Ochir and Kim, 2023). For perimeter security, magnetic reed switches are employed because they can easily detect doors and windows opening but they cannot detect anomaly within the environment once as instruction as already taken place or occurred (Islam, 2025). Although while most of each of the deployed sensing device are capable of detecting instruction and movement within the environment, none of them is capable of total and consistent reliable instruction detection in all operational conditions.

Several studies have explored the application of machine learning and artificial techniques for intrusion detection. For instance, Alshahrani *et al*. (2022), Chua and Salam (2023) and Zhang *et al*. (2022) effectively show from their studies that supervised learning models can greatly improve detection accuracy in network-based IDS. Patel (2024), Rajasekar *et al*. (2025) and Reis (2025) proposed an AI-driven intrusion detection framework techniques designated for high-speed communication networks such as 5G systems, while Hussain *et al*. (2026) investigated sensor fusion within cyber–physical security environments. All these points towards improvements especially in classification performance but they are dependent on large labeled datasets, high computational resources and often retraining of the models. Such requirements are impractical for low-cost embedded security systems deployed in homes or small commercial facilities where computational resources and energy budgets are limited (Sayeduzzaman *et al*., 2024).

Energy efficiency further complicates the design of practical sensor-based intrusion detection systems. There must be a balance between continuous environmental monitoring, battery consumption as well as operational cost. Tekin *et al*. (2023) emphasized that achieving this balance remains a key design challenge in IoT-based IDS implementations. Similarly, Ahmad *et al*. (2022) shows that environmental variations effect sensor calibration and long-term reliability. In resource-constrained environment, high computationally intensive AI-based detection systems often increase latency and system complexity. Many practical security applications require lightweight hardware-based detection approaches that prioritize reliability, responsiveness, and affordability.

Sensor fusion has emerged as a promising strategy for addressing the limitations of individual sensing technologies. By combining multiple sensors together, fusion-based systems can cross-validate detected events and significantly reduce the likelihood of false alarms (Albarrak *et al*., 2026). Kumar *et al*. (2023), for instance, demonstrated that integrating multiple sensing modalities improves detection accuracy in IoT-based monitoring applications. It worth mention that most of the existing studies surveillance system are simulation based not real time embedded systems designed for deployment in an environment. In addition, implementation of PIR sensors, microwave radar sensors, and magnetic switches as a single monitoring system for evaluating detection accuracy, response time and false alarms rates under controlled experimental settings is not readily available.

The gap amongst the proposed sensor fusion techniques and real-world embedded deployment necessitate the need for practical experimental investigation. Previous studies do not consider ablation evaluation of each of the sensor prior to fusion integration, making it difficult to

quantify the actual performance improvement achieved through multi-sensor coordination. Also, communication and alert mechanisms — such as GSM-based notifications and GPS-enabled location tracking — are often treated as auxiliary system components rather than integral parts of the security architecture (Singh *et al*., 2024).

To address these challenges, this study presents the design and experimental implementation of a multi-sensor fusion intrusion detection system based on an ESP32 embedded architecture. The proposed system integrates Passive Infrared (PIR) sensors, microwave radar sensors, and magnetic reed switches in order to exploit their complementary sensing capabilities. PIR sensors provide thermal motion detection, microwave radar enables penetrative motion sensing across partially obstructed environments, and magnetic switches ensure reliable perimeter monitoring of entry points. A structured cross-verification logic is implemented to reduce false alarms while maintaining real-time responsiveness. In addition, GSM communication enables immediate SMS notifications, while GPS integration provides location awareness to support rapid situational response.

## 2.0. Methodology

### 2.1. Material Selection and System Design

The proposed intrusion detection system (IDS) was developed as a multi-sensor embedded security platform designed to enhance detection reliability through the integration of complementary sensing technologies. The system comprises of three layers; sensing, processing, and alert and communication layer.

The sensing layer includes a Passive Infrared (PIR) sensor, a microwave radar sensor, and a magnetic reed switch. These sensors were selected to provide diverse detection capabilities that collectively improve intrusion verification. The PIR sensor detects variations in infrared radiation produced by human body heat, the microwave radar sensor identifies motion using Doppler-based microwave reflections, and the magnetic reed switch monitors the opening of doors or windows to provide perimeter protection. The processing layer is implemented using an ESP32 microcontroller, which serves as the central control unit responsible for data acquisition, sensor fusion logic, and system decision-making. The microcontroller one used because it is most compatible with embedded IoT application and low power consumption. The alert and communication layer consists of a GSM module, a GPS module, and an audible buzzer. The GSM module will enable the transmission of real-time SMS alerts when intrusion events are confirmed, allowing remote monitoring by the system owner. The GPS module provides location information that can assist in identifying the exact location of the security system during emergency notifications. In addition, the buzzer serves as a local alarm mechanism that provides immediate audible alerts when an intrusion is detected.

The overall system design aims to provide a cost-effective, energy-efficient, and scalable security solution capable of real-time intrusion detection and remote notification. By combining multiple sensing modalities with structured cross-verification logic, the system reduces false alarms while maintaining fast response times. Table 1 presents the major hardware components used in the system and the rationale behind their selection. Component selection was guided by several practical considerations, including local availability,

compatibility with 3.3 V logic levels, affordability, ease of integration with the ESP32 platform, and suitability for real-world deployment.

**Table 1**: Materials and component selection for the proposed IDS system.

| **Component** | **Model/Type** | **Function** | **Reason for Selection** |
|---|---|---|---|
| PIR Sensor | HC-SR501 | Detects infrared motion | Low power, human-body sensitivity |
| Microwave Radar | RCWL-0516 | Doppler motion sensing | Penetrative detection capability |
| Magnetic Reed Switch | Normally-closed | Door/window breach detection | Reliable perimeter monitoring |
| Microcontroller | ESP32 Dev Module | Central control unit | Dual-core processing, low power |
| GSM Module | SIM900D | SMS alert transmission | Wide network compatibility |
| GPS Module | NEO-6M | Location tracking | Real-time positional data |
| Buzzer | 110 dB | Audible alarm | Immediate local alert |
| Power Source | 7.4V Li-ion Battery | System power | Rechargeable and portable |

## 2.2. System Circuit Design and Integration

The system was initially prototyped on a breadboard to verify electrical connections and validate sensor signal responses. Each sensor output was interfaced with designated GPIO pins of the ESP32 microcontroller. Pull-up and pull-down resistors were incorporated where necessary to stabilize signal readings and prevent floating input states. The PIR sensor and microwave radar module were set as digital input device; they are in logical HIGH state when motion is occurs within their sensing radii while the magnetic reed switch as employed as a normally closed circuit producing an output in logic state too when door or window were opened. Communication between the ESP32 and the external modules was carried out through the serial communication using the Universal Asynchronous Receiver–Transmitter (UART) interface. Alert messages and location coordinates are provided by the GSM and GPS module respectively.

The power usage was regulated to ensure stable system operation using a voltage regulator module; providing two regulated power output of 5 V and 3.3V that is adequate for the different incorporated hardware. After the breadboard prototype stage, the whole system was transferred to a Veroboard. Figure 1 shows the circuit diagram of the proposed IDS system while Figure 2 show the assembly of each of the components on a Veroboard.

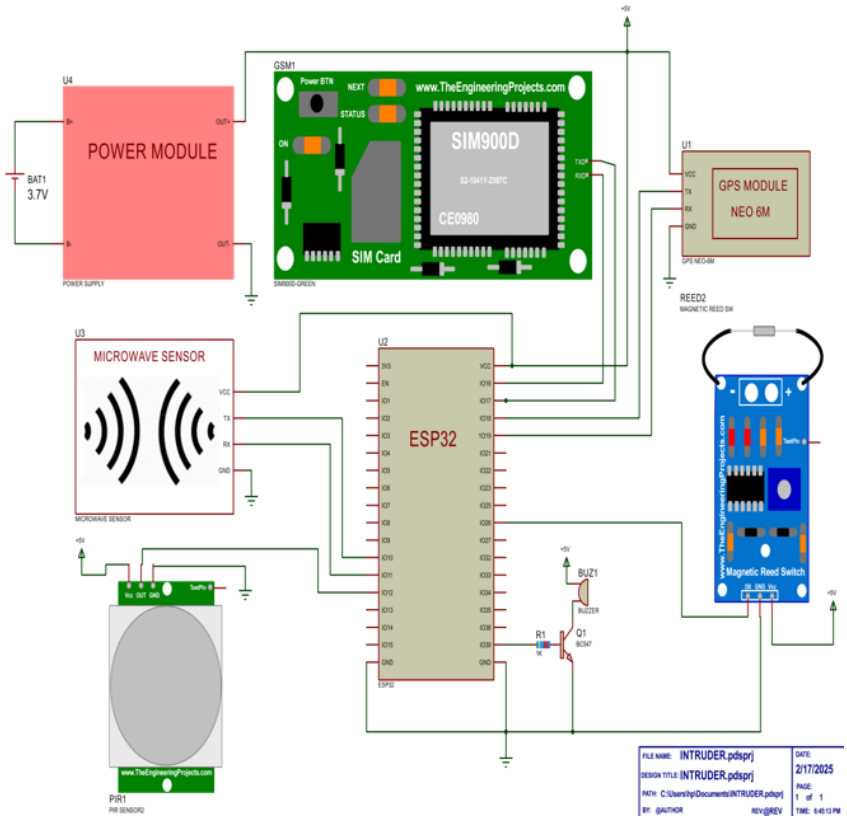



**Figure 1: The circuit diagram of the proposed IDS system**



**Figure 2: The assembly of each of the components on a Veroboard**

## 2.3. Detection Logic and Sensor Fusion Strategy

To ensure reliable intrusion detection, a structured detection algorithm was implemented within the ESP32 firmware. For sensitivity and reliability, two modes were defined for the proposed IDS. Single sensor detection is the first mode, activation of any of the sensor in single sensor mode will immediately trigger the system which ensure potential movement are detected

quickly leading to maximum sensitivity of the system. However, frequent background disturbances may result in higher false alarm rates. The second mode is the multi-sensor verification mode, which was implemented to reduce false positives. This mode is configured to confirm detection within a time window of 5 - 10 seconds if at least two independent sensors detect any activity.

## 2.4. Software Development and Embedded Programming

The system firmware was developed using Embedded C within the Arduino Integrated Development Environment (IDE) configured for the ESP32 microcontroller platform. The software architecture was designed to support real-time monitoring and efficient system operation. The program flow consists of several sequential stages. Figure 3 shows the flowchart describing the program logic implemented within the embedded processor.

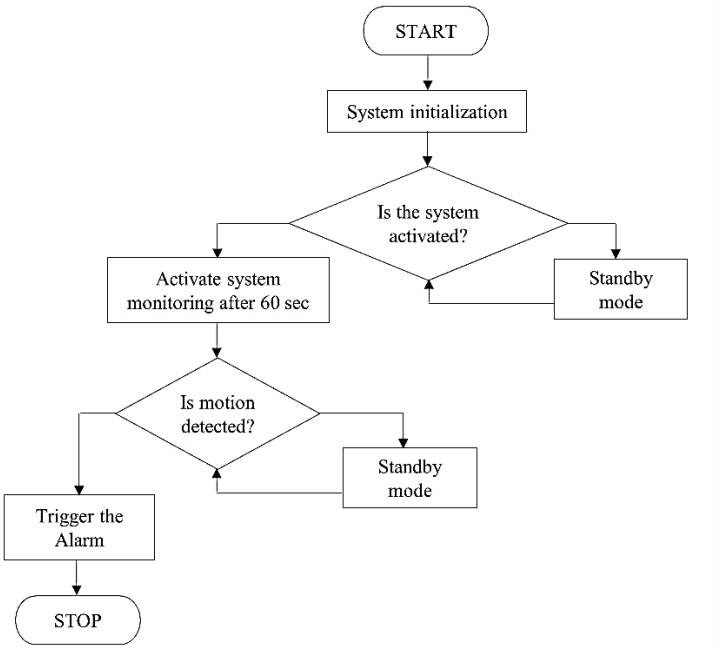



**Figure 3: Flowchart of the program implemented in the embedded processor.**

## 2.5. Experimental Setup and Performance Evaluation

The performance of the proposed intrusion detection system was evaluated under controlled indoor conditions designed to simulate realistic intrusion scenarios. Experiments were conducted in a residential room environment in order to approximate practical deployment conditions. Several test scenarios were considered during the evaluation process, including; human movement across the sensor detection range, simultaneous movement of two individuals, door opening and closing events, motion occurring behind glass surfaces, airflow disturbances, sudden changes in lighting conditions and non-human movement simulations (e.g., objects or pets) (Abbasi *et al*., 2023; De *et al*., 2022; Mahalle *et al*., 2024). Each test scenario was repeated five times to ensure consistency and reliability of the experimental observations.

System performance was evaluated using the performance metrics using equations (1) and (2).

$$\text{Detection Rate (\%)} = \frac{\text{Correct intrusion detection}}{\text{Total intruction events}} \times 100 \quad (1)$$

$$\text{False Positive Rate (\%)} = \frac{\text{False Alarm}}{\text{Total non} - \text{intruction events}} \times 100 \quad (2)$$

Response time was defined as the time interval between the occurrence of an intrusion event and the activation of the alarm system. This parameter was measured using a stopwatch with millisecond precision. Also, power consumption was monitored using a digital multimeter under both idle and active operating conditions in order to estimate the system's overall energy efficiency and suitability for battery-powered deployment.

## 3.0. Results and Discussion

This section shows the empirical outcomes derived from the assessment of the proposed intrusion detection system (IDS). Initially, the performance efficiency of each individual sensor was evaluated in isolation, thereafter that of the proposed fusion was also conducted. Detection rate, false positive rate, response time and power consumption results were presented in this section.

Figure 4 shows the detection rate of the individual sensors in comparison with full sensor fusion. There is a trend increase in performance from isolated sensors to sensor fusion. This increase in performance substantiates the efficiency of sensors fusion and high detection rate in full fusion sensors points towards more robust interactions among the sensors.

Figure 5 depicts the false positive rate across various sensor configurations. The graphical representation indicates that standalone microwave sensing generates the highest frequency of alerts. Conversely, the fusion modes significantly diminished false alarm occurrences. The notable reduction from 15% (microwave alone) to 1% (full fusion) shows the success of the cross-verification algorithm in differentiating between real intrusion attempts and environmental perturbations. This reduction is important for practical implementation, as an excess of false alarms may induce alarm fatigue and reduce system reliability.

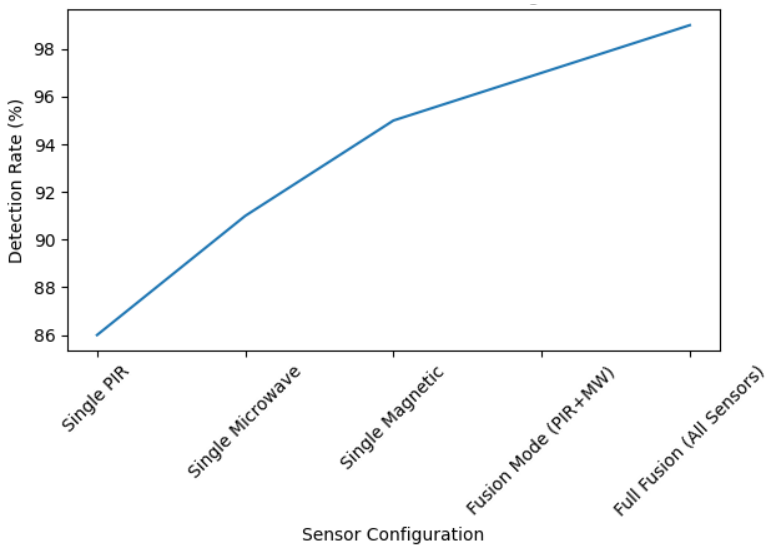



**Figure 4: Detection rate of the standalone sensors with full sensor fusion**

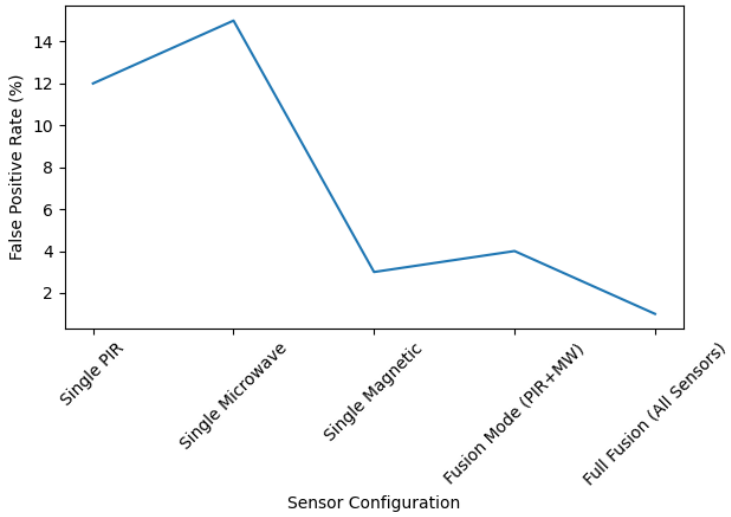



**Figure 5: False positive rate across sensor configurations**

Figure 6 illustrates the response time across different sensor configurations. This indicate that the response time of magnetic sensing is 1.2 s which is the highest followed closely by microwave (1.5 s) and PIR (1.8 s). Fusion modes introduce a marginal latency due to decision confirmation intervals; nonetheless, response times remain below 2 seconds across all configurations. The slight increase in response time for the full fusion mode (1.6 s) is deemed acceptable in light of the substantial enhancement in detection reliability. In practical security applications, a sub-2-second response is regarded as operationally effective.

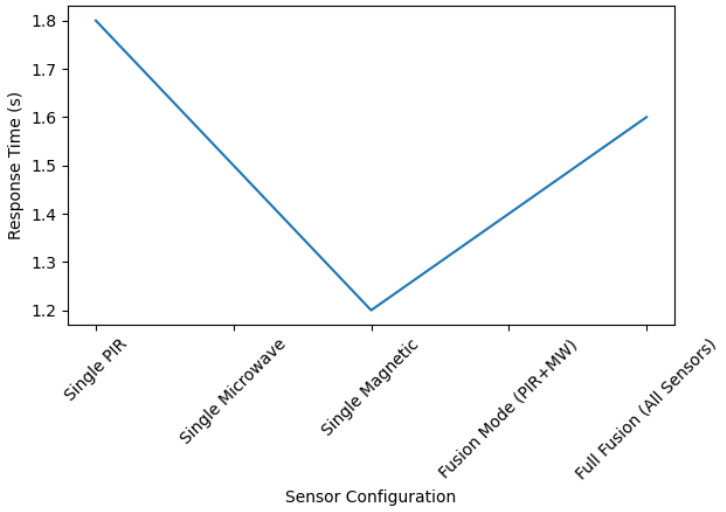



**Figure 6: The response time across sensor configurations**

Figure 7 presents the power consumption associated with various sensor configurations. The power analysis indicates that standalone magnetic sensing exhibits the least current consumption (110 mA), whereas full fusion is the highest current (160 mA). The increased in power consumption observed under fusion modes can be due to the concurrent activation of sensors and that associated with GSM communication.

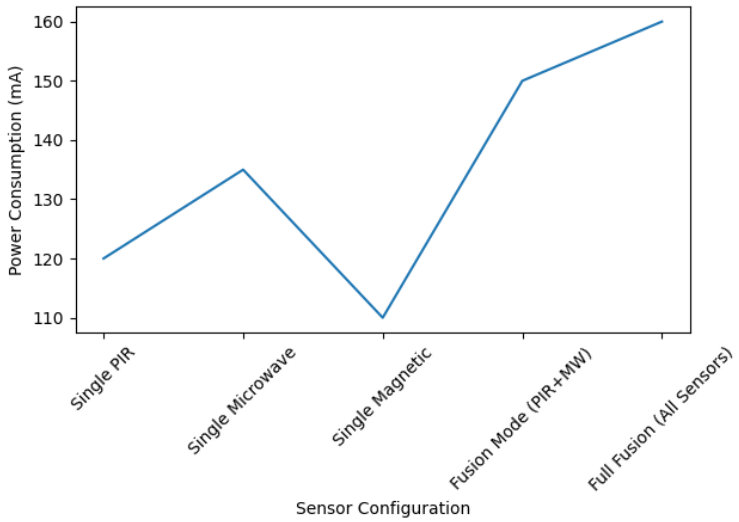



**Figure 7: The power consumption across sensor configurations**

To assess the performance of the proposed multi-sensor intrusion detection system within the broader context of existing research, a comparative analysis was undertaken against representative hardware-based and AI-driven intrusion detection systems reported in recent scholarly literature (Navardi *et al*., 2025; Tummala *et al*., 2025). In the past, standalone-based intrusion detection systems were proposed because of less cost and minimal energy requirement. for instance Godase (2025) reported instruction detection accuracies between 80 % and 90% with a false alarm rate beyond 10% under varying environmental settings. Also, Royo *et al*., (2023) reported a very high sensitivity but with a very high false positive rate due to environmental noise. AI-based IDS systems show rates exceeding 95% but require larger labeled datasets, substantial computational resources, and ongoing model retraining (Raja, 2025; Sharma and Bairwa, 2025). it is worth noting that in a resource constrained framework, such complexity will lead to an increase in power consumption, increase detection time rates and also increase cost of the system.

In contrast, the proposed IDS system has a 99% detection accuracy with has low as a 1% false positive rate value and a response time of below 2 seconds. More critically, the reduction in false alarm rates from 15% (when utilizing microwave alone) to 1% in full fusion mode signifies a considerable enhancement in operational efficacy, especially in practical applications where erroneous alerts can undermine user confidence.

## 4.0. Conclusion and Recommendations

This study presents the design and empirical validation of an embedded intrusion detection system based on multi-sensor fusion, which combines Passive Infrared (PIR), microwave radar, and magnetic reed switch sensors within an ESP32 framework. The proposed cross-verification procedure achieved a 99% detection accuracy with a 1% false positive rate, thereby surpassing the performance of isolated sensing configurations while maintaining a response time of less than 2 seconds and consuming moderate power. The findings validates that a methodically structured hardware-level sensor system can significantly enhance detection reliability without dependency on machine learning or cloud-based computational resources. It also establishes a

practical, low-complexity alternative to data-intensive IDS approaches, particularly suitable for residential and small commercial deployment.

In addition, the study shows that sensor fusion integration as a scalable foundation for future embedded security systems. Future research will focus on adaptive threshold optimization under dynamic environmental conditions and also hybrid edge-intelligence frameworks that incorporate lightweight contextual learning without significant computational overhead may further enhance detection resilience.

**Acknowledgement**

The authors gratefully acknowledge the Tertiary Education Trust Fund (TETFund), Nigeria, for the financial support provided through the Institution-Based Research (IBR) Grant, which made this research possible. We also deeply appreciate the Management of Kwara State University (KWASU), Malete, Nigeria, in providing the enabling academic and institutional environment towards the successful execution of this research. The support and facilities provided by both institutions are deeply appreciated.

**References**

Abbasi, A., Queirós, S., da Costa, N. M., Fonseca, J. C., and Borges, J. (2023). Sensor fusion approach for multiple human motion detection for indoor surveillance use-case. *Sensors*, *23*(8), 3993.

Ahmad, A., Potluri, P., Yeruva, A. R., Satyasriram, P., Harizan, S., Kumar, R., and Alsekait, D. M. (2022). Energy Efficient Intrusion Detection in a heterogeneous environment of Wireless sensor networks. *NeuroQuantology*, *20*(13), 1493–1503.

Al-Anzi, F. S. (2022). Design and analysis of intrusion detection systems for wireless mesh networks. *Digital Communications* and *Networks*, *8*(6), 1068–1076.

Albarrak, M., Salonitis, K., and Jagtap, S. (2026). Natural language processing (NLP)-based frameworks for cyber threat intelligence and early prediction of cyberattacks in Industry 4.0: A systematic literature review. *Applied Sciences*, *16*(2), 619.

Al-Hashemi, S. Q. Y., Naghmash, M. S., and Ghandour, A. (2024). Enhancing motion detection in video surveillance systems using the three-frame difference algorithm. *Mesopotamian Journal of Computer Science*, *2024*, 167–175.

Alshahrani, E., Alghazzawi, D., Alotaibi, R., and Rabie, O. (2022). Adversarial attacks against supervised machine learning based network intrusion detection systems. *Plos One*, *17*(10), e0275971.

Anwar, S., Mohamad Zain, J., Zolkipli, M. F., Inayat, Z., Khan, S., Anthony, B., and Chang, V. (2017). From intrusion detection to an intrusion response system: Fundamentals, requirements, and future directions. *Algorithms*, *10*(2), 39.

Bing, Z., Yunhong, G., Bo, L., Guangwei, Z., and Tian, T. (2001). A practical algorithm for exception event detection for the home video security surveillance. *2001 International Conferences on Info-Tech and Info-Net. Proceedings*, *3*, 202–208.

Bocu, R., and Iavich, M. (2022). Real-time intrusion detection and prevention system for 5G and beyond software-defined networks. *Symmetry*, *15*(1), 110.

Chasdi, R. J. (2025). Future trends for cyber security for smart cities and homes. In *Computer and information security handbook* (pp. 1457–1478). Elsevier.

Chua, T.-H., and Salam, I. (2023). Evaluation of machine learning algorithms in network-based intrusion detection using progressive dataset. *Symmetry*, *15*(6), 1251.

Cozens, A. E., Johnson, S. D., and Lee, T.-C. (2025). A systematic review of sensors to combat crime and routes to further sensor development. *Frontiers in Chemistry*, *13*, 1568867.

De, P., Chatterjee, A., and Rakshit, A. (2022). Pir-sensor-based surveillance tool for intruder detection in secured environment: A label-consistency-based modified sequential dictionary learning approach. *IEEE Internet of Things Journal*, *9*(20), 20458-20466.

Godase, V. (2025). A comprehensive review on PIR sensor-based light automation systems. *International Journal of Image Processing and Smart Sensors*, *1*(1), 22–29.

Hafez, A. I. (2024). Anticipating and Addressing Unconventional Future Crimes: A Mechanistic Analysis in the Context of Technological Advancements. *Police Thought*, *33*(1).

Heidari, A., and Jabraeil Jamali, M. A. (2023). Internet of Things intrusion detection systems: A comprehensive review and future directions. *Cluster Computing*, *26*(6), 3753–3780. https://doi.org/10.1007/s10586-022-03776-z

Hussain, M. A., Meruga, V. B., Rajamandrapu, A. K., Varanasi, S. R., Valiveti, S. S. S., and Mohapatra, A. G. (2026). Generative AI Sensor Fusion for Secure Digital Twin Ecosystems: A Standardization-Aligned Framework for Cyber-Physical Systems. *IEEE*

Islam, S. (2025). *Smart Security System: Design, Implementation, and Evaluation*. https://www.academia.edu/download/124418383/Smart_Security_System.pdf

Kumar, K. K., Ramaraj, E., and Geetha, P. (2023). Multi-sensor data fusion for an efficient object tracking in Internet of Things (IoT). *Applied Nanoscience*, *13*(2), 1355–1365.

Kumar, Y., and Kumar, V. (2023). A Systematic Review on Intrusion Detection System in Wireless Networks: Variants, Attacks, and Applications. *Wireless Personal Communications*, *133*(1), 395–452.

Mahalle, P. N., Takale, D. G., Sakhare, S., and Regulwar, G. B. (Eds.). (2024). *Machine Learning for Environmental Monitoring in Wireless Sensor Networks*. IGI Global.

Nanzer, J. A. (2017). A review of microwave wireless techniques for human presence detection and classification. *IEEE Transactions on Microwave Theory and Techniques*, *65*(5), 1780–1794.

Navardi, M., Gao, S., Walczak, M., Camacho, F., and Mohsenin, T. (2025). Meta reasoning for Edge-Cloud Collaborative LLM Planning for Efficient Autonomous Navigation. *ACM Transactions on Embedded Computing Systems*, 3765750.

Nosiri, O. C., Akwiwu-Uzoma, C. C., Nmaju, U. A., and Elumeziem, C. H. (2018). Motion detector security system for indoor geolocation. *International Journal of Engineering and Applied Sciences (IJEAS)*, *5*(11), 24–30.

Patel, N. (2024). AI-powered intrusion detection and prevention systems in 5G networks. *2024 9th International Conference on Communication and Electronics Systems (ICCES)*, 834–841.

Racherla, S., Sripathi, P., Faruqui, N., Kabir, M. A., Whaiduzzaman, M., and Shah, S. A. (2024). Deep-IDS: A real-time intrusion detector for IoT nodes using deep learning. *IEEE Access*, *12*, 63584–63597.

Raja, M. S. R. S. (2025). The rise of ai-driven network intrusion detection systems: Innovations, challenges, and future directions. *International Journal of AI, BigData, Computational and Management Studies*, *6*(1), 1–9.

Rajasekar, L., Kumar, A., Singh, R., Pongiannan, R. K., Palanikumar, S., and Pemila, M. (2025). AI based Intrusion Detection for 5G Networks. *2025 5th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS)*, 1398–1403.

Reis, M. J. (2025). AI-driven anomaly detection for securing IoT devices in 5G-enabled smart cities. *Electronics*, *14*(12), 2492.

Royo, I., Fernández-García, R., and Gil, I. (2023). Microwave resonators for wearable sensors design: A systematic review. *Sensors*, *23*(22), 9103.

Sayeduzzaman, Md., Hasan, T., Nasser, A. A., and Negi, A. (2024). An Internet of Things-Integrated Home Automation with Smart Security System. In A. K. Tyagi (Ed.), *Automated Secure Computing for Next-Generation Systems* (1st ed., pp. 243–273). Wiley.

Sharma, S. B., and Bairwa, A. K. (2025). Leveraging AI for intrusion detection in IoT ecosystems: A comprehensive study. *IEEE Access*.

Singh, K. U., Chaudhary, V., Sharma, P. K., Kumar, P., Varshney, N., and Singh, T. (2024). Integrating GPS and GSM Technologies for Enhanced Women's Safety: A Fingerprint-Activated Device Approach. *2024 International Conference on Automation and Computation (AUTOCOM)*, 657–662.

Summerlot, J. P. (2024). *Outposts in the Culture War: Improving Resilience to Man-Made Threats at Museums and Libraries*.

Tekin, N., Acar, A., Aris, A., Uluagac, A. S., and Gungor, V. C. (2023). Energy consumption of on-device machine learning models for IoT intrusion detection. *Internet of Things*, *21*, 100670.

Thakkar, A., and Lohiya, R. (2022). A survey on intrusion detection system: Feature selection, model, performance measures, application perspective, challenges, and future research directions. *Artificial Intelligence Review*, *55*(1), 453–563.

Tummala, B. M., Kumar, M. D. P., and Nagurbasha, S. (2025). Real-Time Parking Slot Detection and Enhanced Security System for Public Parking Using IoT. *2025 International Conference on Inventive Computation Technologies (ICICT)*, 1779–1785.

Verma, M., Kaler, R. S., and Singh, M. (2021). Sensitivity enhancement of Passive Infrared (PIR) sensor for motion detection. *Optik*, *244*, 167503.

Zada, M. N. H., Rahimi, N., Akhlaqi, H., and Mohammadi, H. (2026). Exploring the Role of Information Technology in Modern Security and Crime Detection Systems. *Gameology and Multimedia Expert*, *3*(1), 10–17.

Zhang, C., Jia, D., Wang, L., Wang, W., Liu, F., and Yang, A. (2022). Comparative research on network intrusion detection methods based on machine learning. *Computers* and *Security*, *121*, 102861.