



iJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** X **Month of publication:** October 2026

DOI: <https://doi.org/10.22214/ijraset.2026.85079>

www.ijraset.com

Call: ☎ 08813907089

E-mail ID: ijraset@gmail.com

Automatic Intrusion Detection Defense Device Using Embedded Systems

Nayana¹, Vauran M², Punith Sai K A³, Ullas S Mysorem⁴, Sunil⁵

Dept. of ECE, Sri Krishna Institute of Technology, Bengaluru, India

Abstract: Unauthorized access to restricted areas presents a significant security challenge, particularly in locations where continuous human surveillance is difficult. This paper presents the design and development of an Automatic Intrusion Detection and Defense Device Using an Embedded System. The developed prototype combines an Arduino UNO controller with an HC-SR04 ultrasonic sensor, servo motors, an ESP32-CAM, LEDs, and a buzzer. The ultrasonic sensor detects objects within a defined distance, while servo-based movement enables directional scanning. Sensor measurements are processed by the Arduino to determine whether an object satisfies the intrusion threshold. When detection occurs, the system activates visual and audible alerts, while the ESP32-CAM provides visual information about the monitored region. The ultrasonic sensor detects objects within a predefined range, while the servo mechanism enables scanning across different directions. The Arduino UNO processes the sensor data and determines whether an intrusion condition has occurred. When an object is detected within the specified range, the system provides visual and audible alerts through LEDs and a buzzer, while the ESP32-CAM enables visual monitoring of the detected area. A servo-controlled mechanism is incorporated to demonstrate an automated, safe and non-projectile response. The system is developed as a prototype to demonstrate the integration of sensing, processing, monitoring, alerting, and automated actuation in an embedded security application. Experimental testing can be performed at different distances and angles to evaluate the detection, scanning, alert, monitoring, and response functions of the system.

I. INTRODUCTION

Security systems are increasingly used to monitor restricted areas and identify unauthorized physical presence. Conventional surveillance approaches may require continuous human observation, which can be difficult to maintain in large or remotely located environments. Delayed identification of an unauthorized object or person may increase the possibility of security breaches, property damage, and risks to people within the protected area.

The development of embedded systems has enabled security applications to combine sensing, processing, communication, monitoring, and actuation within a single system. Sensor-based detection can continuously monitor a specified area and provide information to a microcontroller, which can then make decisions according to predefined conditions. Such automation can reduce dependence on manual surveillance and improve the speed of response.

The proposed Automatic Intrusion Detection and Defense Device Using an Embedded System is a prototype designed to demonstrate this concept. The system integrates an HC-SR04 ultrasonic sensor, Arduino UNO, servo motors, ESP32-CAM, LED indicators, and a buzzer. The ultrasonic sensor detects objects within a predefined range, while the servo mechanism enables the sensor to scan different directions. The Arduino UNO receives and processes the sensor information to determine whether an intrusion condition has occurred.

II. REVIEW SCOPE AND METHODOLOGY

The review emphasizes recent IEEE publications primarily from 2024 and 2025, supplemented by closely relevant IEEE work when it provides direct evidence for embedded deployment. Search themes included 'embedded intrusion detection', 'IoT intrusion detection', 'edge IDS', 'federated learning IDS', 'side-channel intrusion detection', 'host-based IDS', 'lightweight AI', and 'automatic response'. Papers were screened for relevance to one or more of the following dimensions: (i) embedded/IoT target, (ii) real-time or edge operation, (iii) ML/DL-based detection, (iv) privacy/distributed learning,

(v) resource efficiency, (vi) explainability, and (vii) practical deployment.

The review is not intended to claim that the selected papers constitute every IEEE publication on IDS. Instead, the selected set represents a focused and recent evidence base for designing an embedded automatic intrusion-defence device.

III. IEEE LITERATURE

A. *Deep-IDS for Real-Time IoT Nodes*

The developed prototype combines an Arduino UNO controller with an HC-SR04 ultrasonic sensor, servo motors, an ESP32-CAM, LEDs, and a buzzer. The ultrasonic sensor detects objects within a defined distance, while servo-based movement enables directional scanning. Sensor measurements are processed by the Arduino to determine whether an object satisfies the intrusion threshold. When detection occurs, the system activates visual and audible alerts, while the ESP32-CAM provides visual information monitored region.

B. *Federated Learning on Embedded Edge Devices*

Bhavsar et al. introduced FL-IDS for transportation IoT and used Raspberry Pi devices as clients with a Jetson Xavier server. The system combines logistic regression and CNN-based detection and was evaluated on NSL-KDD and Car-Hacking datasets. Reported overall accuracy reached about 94% and 99% in the two testbed configurations, respectively [4]. The results indicate that IDS processing can be distributed across embedded devices while keeping the original data at the local nodes. Nevertheless, such an architecture requires coordination between participating devices, which may increase communication overhead. However, an individual low-cost device still depends on federated coordination, and communication rounds can introduce latency and complexity unsuitable for isolated deployments.

C. *Side-Channel and Power-Based Intrusion Detection Domínguez*

Campos et al. investigated intrusion detection using device power consumption as a side channel. Machine-learning models were trained to distinguish normal behaviour from attack related power signatures. The authors report experiments involving custom datasets, previously unseen attacks, and live detection, while emphasizing simplicity, portability, and low resource demand [2]. This approach is highly attractive for embedded defence because it can monitor a device without requiring deep inspection of every network packet. A limitation is that power signatures can be influenced by workload, peripherals, operating conditions, and device heterogeneity, requiring robust calibration.

D. *Host-Based IDS for IoT*

Nallakaruppan et al. proposed an enhanced host-based IDS framework and compared machine-learning algorithms using fuzzy-based recommendation mechanisms. Decision Tree, Lite Gradient Boost, Xtra Gradient Boost, and Random Forest were reported to provide approximately 99% accuracy with strong precision, recall, and F1 performance [3]. The work is useful for an embedded project because host-side telemetry can be collected locally, reducing dependence on a network monitoring appliance. Nevertheless, the computational cost of ensemble methods and the lack of a complete automatic actuation/isolation layer remain practical concerns.

E. *Edge-Federated Learning for Heterogeneous IoT*

Mahadik et al. proposed an edge-federated learning IDS for heterogeneous IoT and focused on DDoS detection [5]. The study reflects the growing movement toward collaborative learning across heterogeneous edge nodes. The key advantage is improved scalability and privacy compared with centralized raw-data collection. The trade-off is additional model-training and communication overhead, which must be carefully controlled in battery-powered or low-memory embedded systems.

F. *Privacy-Preserving Federated IDS*

Vyas et al. surveyed privacy-preserving federated learning for IoT IDS, covering mechanisms such as homomorphic encryption, differential privacy, secure multiparty computation, and federated learning [6]. The survey establishes privacy as a major design dimension rather than a secondary feature. For an embedded defence device, privacy-preserving collaboration is useful when multiple devices need to learn jointly. At the same time, cryptographic protection and privacy noise can increase computation, latency, and model complexity.

G. *Dynamic Attack Detection with Ensemble Learning, Q-Learning and XAI*

Turaka and Panigrahy proposed a dynamic attack-detection approach that combines ensemble learning, Q-learning, and explainable AI [7]. The motivation is important for an automatic defence system because static classifiers may be inadequate against changing attack behaviour.

Adaptive decision-making and explanations can improve trust and enable safer automated response. The unresolved issue is how to implement such adaptive intelligence within a small microcontroller-class platform while maintaining deterministic behaviour.

H. IoT Intrusion Detection Surveys

Liao et al. reviewed deep-learning technologies for IoT IDS, comparing models, datasets, feature extraction, preprocessing, and experimental practices [8]. Abdulkareem et al. provided a broader survey of IoT and non-IoT network intrusion detection and identified publicly available datasets for research [9]. These studies show that deep learning has become a dominant direction, but they also highlight the continuing importance of dataset quality, feature engineering, and evaluation methodology.

I. 2025 Federated and Adaptive IDS Research

Recent 2025 IEEE Access publications further emphasize federated and adaptive IDS. Hamad et al. systematically analyzed 43 studies from 2020–2024 and identified challenges in dataset diversity, non-IID data, scalability, privacy, and adaptive detection [10]. Gutti et al. proposed HADA-FL, using SHAP-based feature stability and differential-privacy budgets to weight federated updates; the study reports 85–89% detection accuracy on Edge-IIoTset and CIC-BCCC-NRC TabularIoTAttack-2024 and improved robustness against adversarial perturbations compared with vanilla FedAvg [11]. Manzano et al. reported a federated framework using distributed storage and a diffusion model, with an average F1-score of 98.3% on a short BoT-IoT dataset [12]. Baich and Sael proposed dynamic ensemble aggregation with a lightweight CNN and local SMOTE for distributed IoT IDS [13]. Bilal et al. investigated federated learning with explainable AI for malicious-traffic detection [14]. These studies collectively move the field toward privacy, robustness, adaptation, and interpretability, but practical autonomous response at the embedded node remains underdeveloped.

IV. COMPARATIVE ANALYSIS OF REFERRED PAPERS

Table I summarizes the reviewed studies against the requirements of an automatic embedded intrusion-defence device. The comparison intentionally includes deployment orientation and response capability, because high detection accuracy alone does not establish suitability for a standalone defence device.

TABLE I. COMPARISON OF RECENT IEEE-RELEVANT IDS STUDIES

Ref.	Year	Core approach	Target / deployment	Main strength	Key limitation for embedded automatic defence
[1]	2024	LSTM / Deep-IDS	IoT node / edge server	Practical real-time orientation	DL inference still requires careful resource budgeting; response layer not central
[2]	2024	Power side-channel + ML	IoT devices	Low-intrusion, portable monitoring	Power signatures affected by workload/device variation; response not integrated
[3]	2024	Host-based ML ensembles	IoT hosts	~99% reported accuracy	Ensemble complexity; autonomous actuation/isolation not central
[4]	2024	Federated LR + CNN	Raspberry Pi / Jetson	Demonstrated embedded FL testbeds	Depends on FL coordination; response loop not integrated
[5]	2024	Edge federated learning	Heterogeneous IoT	Privacy and distributed learning	Communication/training overhead
[6]	2024	Privacy-preserving FL survey	IoT	Maps privacy mechanisms and research directions	Survey; no complete embedded defence implementation
[7]	2024	Ensemble + Q-learning + XAI	IoT networks	Adaptive detection and explainability	Adaptive complexity and deployment determinism
[8]	2024	Deep-learning IDS survey	IoT	Comprehensive model/dataset comparison	Survey; deployment/response gaps remain

[9]	2024	ML-based NID survey	IoT + conventional networks	Broad taxonomy and datasets	Survey; embedded response not implemented
[10]	2025	Systematic FL-IDS review	IoT	Identifies FL gaps, diversity and scalability issues	Review; calls for practical validation
[11]	2025	HADA-FL + SHAP + DP	ARM-class IoT simulation	Privacy and poisoning robustness	Higher system complexity; 85–89% reported accuracy indicates trade-offs
[12]	2025	FL + distributed storage + diffusion	IoT networks	98.3% average F1 on short BoT-IoT	Still primarily detection/learning; embedded response not demonstrated
[13]	2025	FL + dynamic ensemble CNN	IoT / IIoT	Lightweight CNN + local imbalance handling	FL scaling and communication remain concerns
[14]	2025	FL + XAI	IoT malicious traffic	Interpretability with distributed learning	Model/communication overhead; physical response not central

V. RESEARCH GAP ANALYSIS

- 1) **Detection–Response Separation:** The reviewed studies predominantly address detection, classification, monitoring, or alarm generation as individual functions. Comparatively fewer approaches combine physical detection, directional sensing, visual verification, alert generation, and an embedded response mechanism within one low-cost platform. Limited work integrates detection, directional identification, visual monitoring, alert generation, and automated response into a single low-cost embedded platform. The proposed system addresses this gap by establishing a continuous detection-to-response pipeline
- 2) **Limited Low-Cost Embedded Implementation:** A number of the reviewed approaches employ edge servers or computationally demanding learning algorithms. This creates an opportunity for a microcontroller-oriented design that performs basic intrusion detection and response using inexpensive hardware.
- 3) **Limited Physical Intrusion Detection:** A significant portion of recent IDS research focuses on cyber and network-based attacks, whereas comparatively less attention is given to detecting unauthorized physical presence. The proposed system addresses this area using an HC-SR04 ultrasonic sensor for real-time physical object detection.
- 4) **Limited Directional Detection:** In the proposed prototype, the ultrasonic sensor is mounted on a servo mechanism so that measurements can be obtained at multiple angular positions. This allows the approximate location of a detected object to be determined. The proposed system uses a servo-mounted ultrasonic sensor to scan different angular positions, allowing the approximate direction of a detected object to be determined.
- 5) **Insufficient Integration of Camera Monitoring:** Distance sensing provides information about object presence and position, but it does not provide visual confirmation. To supplement the ultrasonic measurements, the proposed system incorporates an ESP32-CAM for capturing the monitored region. The proposed system integrates an ESP32-CAM to provide visual monitoring in addition to ultrasonic detection.
- 6) **Limited Automated Response:** detecting an intrusion. The proposed system extends this functionality by incorporating a controlled servo-based safe response mechanism, thereby creating a more complete detection-and-response architecture. The proposed system extends the detection process by incorporating a controlled servo-based response

VI. IDENTIFIED RESEARCH OPPORTUNITY

The literature review indicates an opportunity for a compact embedded security platform that combines physical intrusion sensing with directional scanning, visual monitoring, local decision-making, alert generation, and controlled actuation. The reviewed studies predominantly investigate cyber-intrusion detection, machine-learning classification, federated learning, or network security. In contrast, the proposed work focuses on integrating physical sensing and automated response within a low-cost embedded prototype that combines low-cost sensing, real-time processing, visual monitoring, and a controlled response mechanism.

Existing studies largely concentrate on intrusion detection, machine-learning classification, privacy, or network-based security, while the integration of physical intrusion detection and automated response on a low-cost embedded platform remains comparatively limited.

The proposed system addresses this opportunity through a layered architecture consisting of (1) ultrasonic sensing, (2) servo-assisted scanning, (3) sensor-data acquisition and processing using Arduino UNO, (4) intrusion decision based on a predefined detection range, (5) LED and buzzer-based alert generation, (6) ESP32-CAM-based visual monitoring, and (7) a safe controlled mechanical response. This follows the project's functional sequence of detection, scanning, processing, alert and monitoring, and response.

VII. RECOMMENDED IMPLEMENTATION DIRECTION

- 1) Hardware: Arduino UNO is used as the main controller, with an HC-SR04 ultrasonic sensor, SG90 and MG996R servo motors, ESP32-CAM, LED, buzzer, resistors, and supporting wiring.
- 2) Intrusion Detection: The HC-SR04 measures the distance of objects within the monitored area.
- 3) Directional Scanning: The servo motor rotates the ultrasonic sensor across different angular positions to scan the surrounding region.
- 4) Data Processing: The Arduino UNO receives the sensor measurements and determines whether the detected object falls within the predefined intrusion threshold.
- 5) Decision Mechanism: When the measured distance satisfies the predefined detection condition, the controller initiates the corresponding alert and monitoring functions.
- 6) Alert Generation: An LED provides a visual indication and the buzzer provides an audible warning when an intrusion is detected.
- 7) Visual Monitoring: The ESP32-CAM captures the detected region, providing an additional monitoring capability.
- 8) Automated Response: The MG996R servo positions the controlled mechanism toward the detected direction and demonstrates a safe, non-projectile response.
- 9) System Testing: The prototype is tested at different distances and angles to evaluate detection accuracy, scanning, alert generation, camera monitoring, and response operation.
- 10) Future Enhancement: Lightweight AI-based classification, IoT connectivity, remote monitoring, sensor fusion, event logging, and adaptive decision-making can be incorporated in future versions.

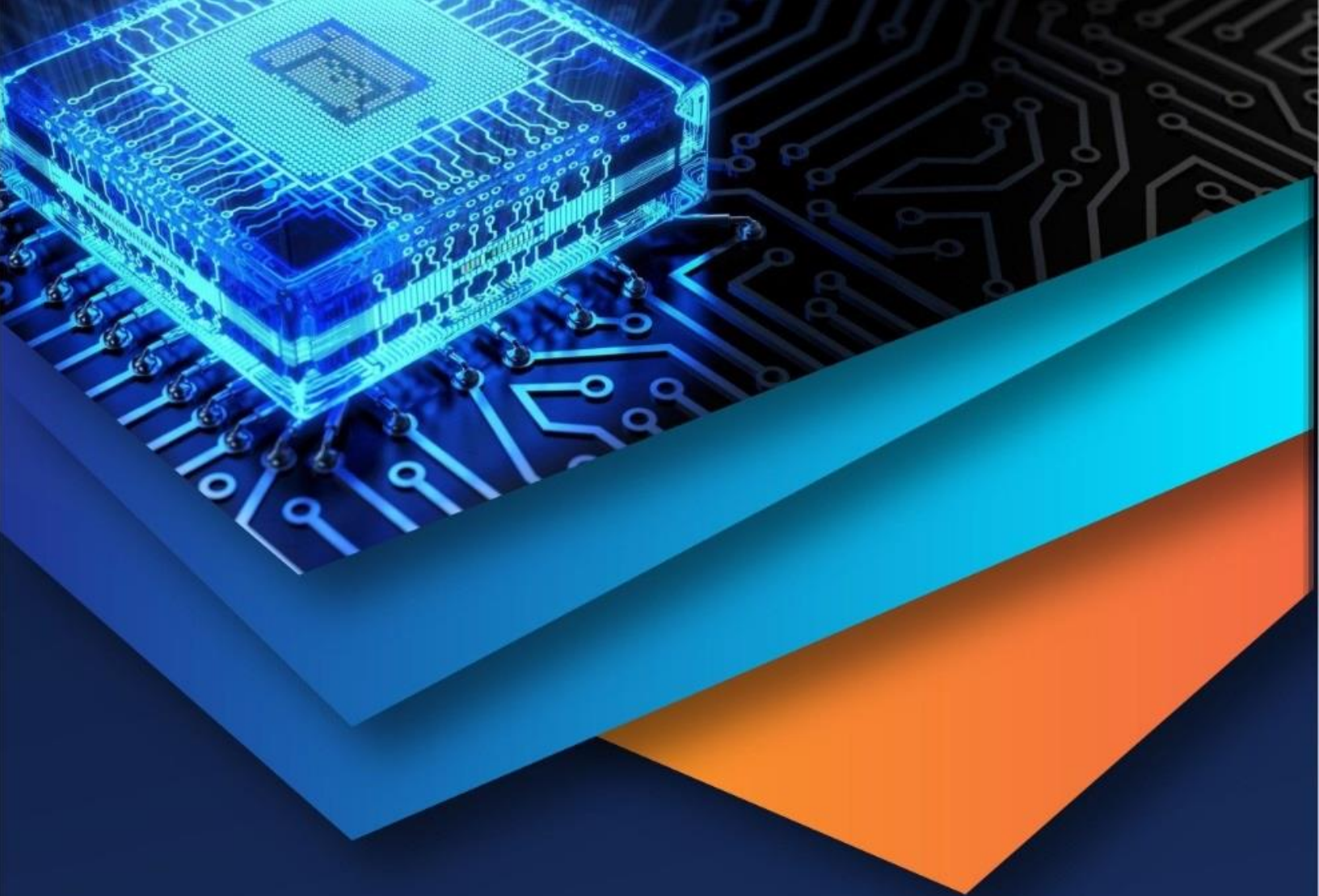
VIII. CONCLUSION

The reviewed studies indicate increasing interest in real-time and embedded approaches to intrusion detection, including machine learning, deep learning, federated learning, and explainable AI. However, the reviewed approaches largely address cyber or network-level threats. The proposed prototype extends the concept toward physical intrusion monitoring by combining ultrasonic sensing, directional scanning, camera-based observation, local processing, alerts, and controlled actuation. Existing studies have explored deep learning, machine learning, federated learning, side-channel analysis, adaptive detection, and explainable AI for improving intrusion detection in IoT environments. However, most of these approaches primarily concentrate on cyber or network-based intrusion detection, with limited integration of physical intrusion sensing and automated response. The proposed Automatic Intrusion Detection and Defense approach to automated physical intrusion detection. Its performance can be evaluated through detection accuracy, scanning capability, response time, alert reliability, camera monitoring, and safe response operation under different distances and angles. Future improvements may incorporate lightweight AI, IoT connectivity, sensor fusion, remote monitoring, and adaptive decision-making to further enhance the reliability and intelligence of the system.

REFERENCES

- [1] S. Racherla, P. Sripathi, N. Faruqui, M. A. Kabir, M. Whaiduzzaman, and S. A. Shah, "Deep-IDS: A Real-Time Intrusion Detector for IoT Nodes Using Deep Learning," *IEEE Access*, vol. 12, pp. 63584–63597, 2024, doi: 10.1109/ACCESS.2024.3396461.
- [2] A. Domínguez Campos, F. Lemus-Prieto, J.-L. González-Sánchez, and A. Caro Lindo, "Intrusion Detection for IoT Environments Through Side-Channel and Machine Learning Techniques," *IEEE Access*, vol. 12, pp. 98450–98465, 2024, doi: 10.1109/ACCESS.2024.3362670.
- [3] M. K. Nallakuruppan, S. R. K. Somayaji, S. Fuladi, F. Benedetto, S. K. Ulaganathan, and G. Yenduri, "Enhancing Security of Host-Based Intrusion Detection Systems for the Internet of Things," *IEEE Access*, vol. 12, pp. 31788–31797, 2024, doi: 10.1109/ACCESS.2024.3355794.
- [4] M. H. Bhavsar, Y. B. Bekele, K. Roy, J. C. Kelly, and D. B. Limbrick, "FL-IDS: Federated Learning-Based Intrusion Detection System Using Edge Devices for Transportation IoT," *IEEE Access*, vol. 12, pp. 52215–52226, 2024, doi: 10.1109/ACCESS.2024.3386631.

- [5] S. S. Mahadik, P. M. Pawar, and R. Muthalagu, "Edge-Federated Learning-Based Intelligent Intrusion Detection System for Heterogeneous Internet of Things," IEEE Access, vol. 12, pp. 81736–81757, 2024, doi: 10.1109/ACCESS.2024.3410046.
- [6] A. Vyas, P. C. Lin, R. H. Hwang, and M. Tripathi, "Privacy-Preserving Federated Learning for Intrusion Detection in IoT Environments: A Survey," IEEE Access, vol. 12, pp. 127018–127050, 2024, doi: 10.1109/ACCESS.2024.3454211.
- [7] P. Turaka and S. K. Panigrahy, "Dynamic Attack Detection in IoT Networks: An Ensemble Learning Approach With Q-Learning and Explainable AI," IEEE Access, vol. 12, pp. 161925–161940, 2024, doi: 10.1109/ACCESS.2024.3485989.
- [8] H. Liao, M. Z. Murah, M. K. Hasan, A. H. M. Aman, J. Fang, X. Hu, and A. U. R. Khan, "A Survey of Deep Learning Technologies for Intrusion Detection in Internet of Things," IEEE Access, vol. 12, pp. 4745–4761, 2024, doi: 10.1109/ACCESS.2023.3349287.
- [9] S. Abdulkareem, C. H. Foh, M. Shojafar, F. D. Carrez, and K. Moessner, "Network Intrusion Detection: An IoT and Non IoT-Related Survey," IEEE Access, vol. 12, pp. 147167–147191, 2024, doi: 10.1109/ACCESS.2024.3473289.
- [10] N. A. Hamad, K. A. Abu Bakar, F. Qamar, A. M. Jubair, R. R. Mohamed, and M. A. Mohamed, "Systematic Analysis of Federated Learning Approaches for Intrusion Detection in the Internet of Things Environment," IEEE Access, vol. 13, pp. 95410–95444, 2025, doi: 10.1109/ACCESS.2025.3574672.
- [11] C. Gutti, K. Thumula, and P. Balbudhe, "Federated Learning for Distributed IoT Security: A Privacy-Preserving Approach to Intrusion Detection," IEEE Access, vol. 13, pp. 135863–135875, 2025, doi: 10.1109/ACCESS.2025.3592481.
- [12] R. Manzano, M. Zaman, D. Upadhyay, N. Goel, and S. Sampalli, "Federated Learning Framework Based on Distributed Storage and Diffusion Model for Intrusion Detection on IoT Networks," IEEE Access, vol. 13, pp. 79571–79595, 2025, doi: 10.1109/ACCESS.2025.3565409.
- [13] M. Baich and N. Sael, "A Federated Learning-Based Intrusion Detection System Using Dynamic Ensemble Aggregation for IoT Networks," IEEE Access, vol. 13, pp. 205826–205839, 2025, doi: 10.1109/ACCESS.2025.3640521.
- [14] M. A. Bilal, I. U. Islam, N. Iltaf, M. J. Khan, et al., "Federated Learning With Explainable AI for Malicious Traffic Detection in IoT Networks," IEEE Access, vol. 13, pp. 173368–173383, 2025, doi: 10.1109/ACCESS.2025.3613459.
- [15] "Intrusion Detection System Framework for SDN-Based IoT Networks Using Deep Learning Approaches With XAI-Based Feature Selection Techniques and Domain-Constrained Features," IEEE Access, vol. 13, pp. 136864–136880, 2025, doi: 10.1109/ACCESS.2025.3595595



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)