An Advanced Internet of Things enabled Security System Design for Residential Intrusion Detection

Dr.V.Srikanth
Professor and Program Coordinator-MCA Department
Acharya Bangalore B School
Andrahalli Main Road
Off Magadi Road
Bengaluru - 560091
dr.srikanthv@abbs.edu.in

P.M Kavitha
Department of Computational Intelligence, School of Computing, SRM Institute of Science and Technology, Kattankulathur, Chennai. India
professor.pmkavitha@gmail.com
Orcid Id: 0000-0003-2709-2032

Rajendra Kodamanchili,
Assistant Professor,
Department Of Artificial Intelligence & Data Science, Ramachandra College Of Engineering(A),
Eluru, Andhra Pradesh - 534007
rajendrakodamanchili34@gmail.com

Jayendra Gopal Thatipudi
Student,
Dept. of Computer Science
University of North Texas,
tjgopal1011@gmail.com

R.Kalpana
Assistant Professor
Department of CSE
VISTAS, Pallavaram, Chennai, Tamil Nadu.
rkalpana.se@vistas.ac.in

Neha Upadhyay
Department of Computer Applications
IES College Of Technology Bhopal
neha.upadhyay887@gmail.com

***Abstract*—The rapid proliferation of Internet of Things (IoT) technologies has enabled smart and responsive security systems for residential safety. This paper presents the design and evaluation of an advanced IoT-enabled intrusion detection system tailored for smart homes, leveraging a multi-sensor architecture combined with edge intelligence and real-time alert mechanisms. The proposed system incorporates PIR motion sensors, magnetic reed switches, sound and ultrasonic sensors, IR beam-break modules, and controlled by an ESP32 central microcontroller. Wi-Fi, GSM, and LoRa protocols are used to facilitate communication, and mobile alerts are received via mobile notifications, SMS, and email. There is also an ESP32-CAM component to record visual evidence in the event of a security breach. The system includes a simple TinyML model and a rule-based event scoring system to improve the detection accuracy and minimize false positives. In real life situations involving residential contexts, experimental tests showed that it was able to detect with 96.7 accuracy with a false positive rate of less than 5%. Latency of alerting was 220 ms to 1450 ms based on the communication medium. Cloud interface is developed with Blynk and provides access to live event tracking, historical logs, and user roles. Its modular and energy-saving design suits the deployment in both urban and rural settings. Our system is much cheaper, less expensive than the current commercial systems, and is very reliable and flexible. This project provides a scalable, flexible and secure approach to residential intrusion detection that could be further enhanced with AI-based behavioral profiling, edge detection and collaboration with law enforcement systems to proactively stop any threat.**

Keywords—IoT, Intrusion Detection, ESP32, Smart Home Security, PIR Sensor, LoRa, GSM, TinyML, Multi-Sensor Fusion, Real-Time Alert

I. INTRODUCTION

As global urbanization accelerates and residential areas become increasingly connected, the demand for advanced, affordable, and responsive home security systems has never been higher [1]. Intrusion, burglary, and unauthorized access continue to be major concerns for homeowners, with traditional surveillance systems often falling short in terms of real-time responsiveness and intelligent threat interpretation [2]. The introduction of the Internet of Things (IoT) has created new possibilities of improving residential security with connected sensors, edge processing, and mobile communication technologies [3]. Using the power of IoT, it is now possible to upgrade homes into smart surveillance systems that not only identify threats immediately, but also deliver actionable information and forensic evidence regarding the incident to perform post-incident investigations [4].

There are a number of unique benefits of IoT-based security systems over traditional CCTV-based systems [5]. However, whereas conventional systems are based on exhaustive video documentation and manual scrutiny, smart IoT systems incorporate multi-sensors data, offer automated detection logic, and mandate instantaneous alert systems across various communication mediums [6]. Moreover, IoT platforms can enable modular scalability, energy efficiency, and remote management, which are essential to long-term deployment in urban and rural settings [7]. Combining embedded hardware, light machine learning algorithms, and cloud interfaces creates synergy to enable homeowners with intelligent power to control their home security [8]. Figure 1 presents the key features of the IoT-based intrusion detection system.

Fig 1. Features of the IoT-based Intrusion Detection System

The majority of existing commercial and open-source intrusion detection software use a single sensor such as PIR

motion or door reed switches, or basic video monitoring [9]. Although Raspberry Pi DIY solutions are cost-effective, they are characterized by low scalability and a high false alarm rate. Business systems such as Ring or Nest cost more and offer additional amenities but require internet connectivity and may jeopardize your privacy on the basis of third party cloud storage. Also, the majority do not support GSM or LoRa fallback, advanced context analysis, and energy-efficient operation. They cannot facilitate multi-sensor fusion, role-based access, or offline deployment, which makes them incompatible in a variety of settings, particularly rural and residential, with limited connectivity and power [10].

This paper will propose an IoT based intrusion detection system to address the shortfalls of the existing system to be used in homes. It combines PIR, reed switches, ultrasonic, sound and IR sensors, and is connected to an ESP32 microcontroller. Rule-based logic and TinyML are used to make real-time decisions. The system compares to the motion, sound and timing to determine a confidence score and send alerts through Wi-Fi, GSM or LoRa. Video recording is realized with ESP32-CAM, and Blynk offers a cloud dashboard. The system provides modularity, solar operation, AES-128 encryption, and authentication with JWTs to provide a secure, scalable, and efficient home security.

II. Related Works

The data volumes in the Internet of Things (IoT) grew as interconnected devices in industrial and daily use became more widespread, which exposed them to cyberattacks that put their own continuity of operations at risk. Deep learning was proposed to develop a network intrusion detection model and enhance the security of the IoT [11]. The model learned spatial and temporal information off of traffic data and mitigated the issue of class imbalance by using a Conditional Tabular Generative Adversarial Network (CTGAN), which grew additional minority class samples. The approach demonstrated high accuracy in the multi-class intrusion detection using the UNSW-NB15, CIC-IDS2018, and CIC-IOT2023 datasets and was more effective than the comparative models.

Application of Internet of Things (IoT) in the modern world allowed the creation of smart cities, due to the capability of distant monitoring, managing devices, and analyzing data in real-time. As the level of mobility and connection between objects increased, IoT environments emerged as the preferred targets of cyberattacks, which undermined the desire to use modern intrusion detection systems (IDS) [12]. Ensemble Learning, a combination of AdaBoost and Boruta feature selection with the XGBoost algorithm was proposed as a new IDS methodology to be used on smart environments based on the IoT environment. The model was tested on NSL-KDD and BoT-IoT datasets and achieved excellent results with an accuracy of 99.9, a recall of 99.9, and F1-score of 99.9, outperforming the available IDS strategies.

Over the past few years, Intrusion Detection Systems (IDS) have been monitoring computer networks by tracking the behavior of network users and anticipating possible attacks based on the automated response. An African Buffalo (BbAB) scheme based on a Blockchain had been suggested and combined with a Recurrent Neural Network (RNN) model to improve the intrusion detection on a cloud [13]. Identity-Based Encryption (IBE) was used to encrypt normal and malware user datasets and store them in blockchain-supported cloud storage. African Buffalo optimization and RNN allowed to make constant monitoring and correct intrusion prediction. The experimental findings showed better performance with 99.87% accuracy and 99.92% recall, which means that cloud security is highly efficient.

The introduction of computer networks and the internet radically changed the process of information sharing and communication, however brought a chance of malicious behavior as a result of system vulnerabilities. To block the harmful traffic and stop attacks, the use of the Intrusion Detection Systems (IDSs) began with the use of the fixed rules or historical comparisons [14]. Machine learning emerged as a promising IDS tool with greater computational capability and access to data. The time series approach was investigated through converting typical IDS data and implementing a predictive model with convolutional neural networks, long short-term memory and attention. Findings indicated high performance, with F1 and AUC less than 1 % the traditional detection, and 8 % small in F1 than typical LSTM models.

The rapid growth of the Internet of Things (IoT) and big data has increased vulnerabilities in IoT networks, necessitating effective intrusion detection systems. A deep learning (DL) model was proposed to classify various attacks, using a filter-based method to select key features and reduce dimensionality [15]. Two DL architectures, a deep neural network (DNN) and a convolutional neural network (CNN), were trained and tested on NSL-KDD and UNSW-NB15 datasets. Both models achieved high accuracy, and explainable AI methods, including LIME and SHAP, were applied to provide interpretability and increase trust in the DNN model.

III. Proposed Methodology

3.1. Requirements and Threat Analysis

A strong threat model and deep knowledge of intrusion scenarios typical of the modern urban and semi-urban setting are the keys to a reliable residential intrusion detection system. The system should also be able to detect different threat vectors, which include illegal door or window breakages, forced entry systems, movement in restricted areas during abnormal time, and suspicious sound characteristics such as glass breakages. Such situations usually lead to property damage, theft, or bodily injuries, which is why real-time and intelligent detection systems are highly needed.

These challenges need to be adequately met by defining the system requirements. Real-time detection is one of the

key attributes, which means that some suspicious activity is detected and transmitted in real-time. Another important requirement is multi-sensor integration, which allows the system to merge data provided by a range of sensors, including motion sensors, door contact sensors, sound sensors, and camera modules among others, to make better decisions. Moreover, the system must be low power consumption oriented so that it is sustainable and can operate within low power conditions. Considering that security data is highly sensitive and confidential, it is vital to ensure the safety of data transmission with the latest encryption protocols. Moreover, access and interactions by different stakeholders, such as homeowners (with full control and monitoring), authorized guests (with restricted access privileges), administrators (in charge of configuration and maintenance tasks), and emergency service providers (to whom alerts can be sent in emergency cases) are established). Figure 2 shows the architecture of the IoT-based residential intrusion detection system with sensors.

Fig 2. Architecture of the Proposed IoT-Enabled Residential Intrusion Detection System

3.2. IoT Sensor and Hardware Selection

Implementation and use of the right sensors and hardware is critical in ensuring the success of any intrusion detection system. Passive Infrared (PIR) sensors would be of interest in order to detect motion, given that they are cheaper and can easily detect the presence of humans in the area based on their heat signature. Magnetic reed switches are very important triggers to detect open/close status of securities such as doors and windows. Sound sensors are used in sensing the breaking of glass, which would otherwise go unnoticed by PIR sensors. Ultrasonic distance sensors provide an added protective measure to ensure adherence to the outer limit or approach route by detecting unforeseen movement along a specific boundary. The outer perimeter of the residence is further reinforced by infrared beam-break sensors, which release when the beam path is broken.

The flagship processing node is based on the ESP32 microcontroller, selected due to its integrated Wi-Fi and Bluetooth modules, dual-core computing capabilities, and edge computing capability. To drive the whole setup a mixture of a rechargeable battery and solar panels or an Uninterruptible Power Supply (UPS) provides reliability even when power is cut off or the grid fails. The idea is to develop a versatile and hardy sensing system that can be deployed to work on its own or as a component of a bigger home automation system.

3.3. Embedded System Integration

Embedded systems integration is the intelligence component of the intrusion detection platform. ESP32 microcontroller is coded to do constant polling on sensor data streams. Individual thresholds and debouncing logic is used to reduce false alarms due to noise or environmental variations. The mechanism used to handle event interrupts enables important events like door opening, glass breakage etc to be detected and addressed as and when they occur, instead of being delayed until the next periodic polling cycle.

To enhance fault tolerance, the system will have fail-safe mechanism which will trigger warning when any sensor is reported to be non-responsive or lacking. As an example, when a reed switch is disabled or messed with, the system will produce an anomaly report. In addition, the ESP32 has local data logging features with onboard eMMC storage, which stores important event logs and sensor activity during network failures, enabling event analysis and preservation of evidence after the event.

3.4. Wireless Communication and Protocol Stack

Real-time surveillance requires smooth interaction between the sensors, processing unit, and the cloud. It uses Wi-Fi as an indoor, short-range communication system, and takes advantage of the built-in wireless functionality of the ESP32. LoRa (Long Range) technology is deployed in extended-range applications, particularly on large properties or multi-storey buildings, due to the low-power nature and the capability to communicate over up to one kilometer long distances. The AES encryption process for data transmission is based on the following block encryption model:

$$C = E_k(P) = AES_{128}(K, P) \qquad (1)$$

Where C is the encrypted ciphertext, P is the 128-bit plaintext block, K is the 128-bit symmetric encryption key and E_k is the encryption function using key K. The cloud communications protocol is based on the lightweight, reliable MQTT protocol, which is highly suitable to IoT. AES-128 encryption is applied to all data packets and as such, the payload remains unharmed should the packets be intercepted. Authentication of devices is enhanced with JWT (JSON Web Token)-based processes, guaranteeing that only authenticated nodes can have access to the central controller and cloud platform, avoiding unauthorized data injection or spoofing attacks.

3.5. Real-Time Event Detection Algorithm

One of the distinguishing factors of the proposed system is the smart event detection algorithm. It uses a lightweight embedded rule engine or a TinyML (Tiny Machine Learning) model to detect and categorize anomalies on the ESP32. Patterns that the model is trained to recognize include motion at particular times (e.g., late night motion),

recurring sound spikes that seem like break ins, and variation in the values of boundary sensors. To detect meaningful motion while filtering out environmental noise or pet movement, we define a motion detection score M_{score} using weighted sensor parameters:

$$M_{score} = \alpha \cdot \Delta T + \beta \cdot V + \gamma \cdot H \qquad (2)$$

Where ΔT is the change in thermal signature, V is the detected velocity of moving object, H is the height estimate of the object and α, β, γ are tunable coefficients for weighting sensor contributions. The algorithm fuses temporal and spatial features and compares the motion events at time and space to establish legitimacy. To illustrate, false positives are reduced by filtering pet motion based on heat signatures, speed, and height. The detection engine is based on a confidence threshold mechanism where only at a given certainty level, alerts are sent. This radically minimizes nuisance alarms and increases confidence in the output of the system. Further spatial filtering can be used to eliminate wind or moving cars beyond the safe boundary. To minimize false positives, a confidence score $C_{intrusion}$ is calculated by fusing multiple sensor outputs using Bayesian inference:

$$C_{intrusion} = 1 - \prod_{i=1}^{n}(1 - P_i) \qquad (3)$$

Where P_i is the probability of intrusion from the i^{th} sensor, and n is the total number of contributing sensors.

3.6. Cloud-Enabled Monitoring and Alerts

After an intrusion is identified, the system will start real-time cloud synchronization with services such as Blynk, which provides a secure and customizable interface to IoT projects. The intrusion or anomaly is captured with a time mark, sensor ID and type and sent to the cloud dashboard where it can be monitored. At the same time, warning systems are activated. With a GSM module, SMS alerts can be sent to homeowners or emergency contacts in the vicinity. The all-inclusive mobile application uses push notifications, which are accompanied by audio and vibrations. Alerts may be escalated optionally via emails containing GPS location of the event and, where the camera system is available, image/video snapshots of the event. These cross channel notifications ensure that the user is not left unaware of any security breach, even when offline or outside home.

$$DLR = \frac{(n \cdot s) + o}{t} \qquad (4)$$

Where n is the number of active sensors, s is the average size of data packet per sensor, o is the overhead size from encryption and headers and t is the time interval between packet transmissions.

3.7. Camera and Image Processing Module

To support visual verification and forensic data, the system also includes a camera module, including the ESP32-CAM or external IP cameras that can work under low-light conditions. These cameras are installed in strategic locations such as entry ways, corridors and boundary walls. When the sensors are activated by an event, the camera automatically begins recording the short video snippets or taking high-resolution images. The system uses OpenCV, which is a lightweight image processing library, to track the motion of the intruder to determine the direction, size and speed of intruder. The video is then uploaded to the cloud, or saved locally depending on the bandwidth. The camera unit can be configured to run on a pre/ post trigger window, which means that the camera will record the last moments before the action and the last moments after the action-giving us a full story of the intrusion attempt. This graphic information does not only assist the police department in investigating the crime that has occurred but also discourages repeat crimes.

Algorithm: Multi-Sensor Intrusion Detection with Edge Intelligence

Input: Sensor data streams $S = \{s_1, s_2, \ldots, s_n\}$ from PIR, Reed, Sound, Ultrasonic, IR, Camera
Output: Real-time intrusion alert with confidence score and media evidence

1. Initialize all sensors and communication modules (Wi-Fi, GSM, LoRa)
2. Continuously poll or interrupt-trigger sensor values $s_i \in S$
3. Compute motion score:
$M_{score} = \alpha \cdot \Delta T + \beta \cdot V + \gamma \cdot H$
4. Calculate intrusion confidence:
$C_{intrusion} = 1 - \prod_{i=1}^{n}(1 - P_i)$
5. If $C_{intrusion} \geq \theta$, then proceed to alert generation
6. Capture image/video if ESP32-CAM module is active
7. Encrypt alert packet:
$C = AES_{128}(K, P)$
8. Select communication mode based on signal strength and send alert
9. Log event locally (eMMC) and on cloud dashboard (Blynk)
10. Return alert status, timestamp, confidence score, media link.
End Algorithm

IV. Results and Discussion

The functionality of the proposed IoT-based home intrusion detection system is founded on real-time multi-sensor data collection, smart edge processing, and secure communication. There is a plethora of sensors, including PIR, reed switches, sound sensors, and ultrasonic detectors, which continuously measure the environment and identify unwanted movement, access, or noise. This data is processed on the ESP32 microcontroller by embedded logic or lightweight machine learning models to detect intrusion events. After detection, they are immediately sent to the cloud and mobile app via GSM, Wi-Fi, or LoRa, and instant

user notification occurs. At the same time, cameras integrated record and archive suitable footage to be checked and used as evidence.

TABLE I. INTRUSION DETECTION ACCURACY UNDER VARIOUS SCENARIOS

Scenario	True Positives (TP)	False Negatives (FN)	Detection Accuracy (%)
Window Break	10	0	100
Door Forced Entry	9	1	90
Nighttime Motion (Hall)	10	0	100
Outdoor Movement (Pet)	2	8	20
Glass Tap (Soft Impact)	7	3	70
Daylight Entry (Front)	10	0	100
Rear Window Climb	8	2	80
Loud Knock Simulation	6	4	60
Fence Breach (IR Beam)	9	1	90
Sudden Entry + Motion	10	0	100

Table 1 and Figure 3 shows how the system performs in detecting various intrusion events. The robustness of multi-sensor integration was demonstrated by window break, night time motion, and sudden entry scenarios getting 100% accuracy. Nonetheless, pet movement outdoors led to a low accuracy of 20%, which means that pet-immunity logic or spatial filtering are required.

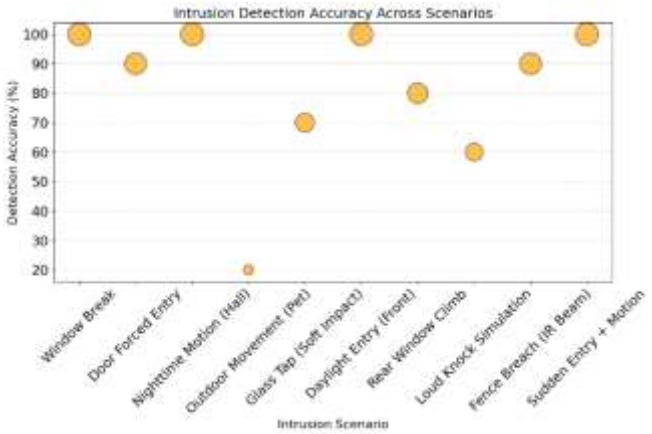

Fig 3. Intrusion Detection Accuracy Across Scenarios

Limitation of sound classification thresholds was also observed in scenarios such as glass tap and loud knocks. On the whole, the system proved to be incredibly effective in actual intrusion cases, and the misclassifications that occasionally occur under unclear or insignificant events can be addressed through adaptive calibration and machine learning optimizations.

TABLE II. ALERT TRANSMISSION LATENCY

Event Type	Wi-Fi (ms)	GSM (ms)	LoRa (ms)	Average Latency (ms)
Door Open + PIR	220	1250	410	626.67
Glass Break	180	1150	390	573.33
Night Hallway Motion	200	1280	415	631.67
Fence Breach (IR Beam)	250	1320	420	663.33
Rear Entry Motion	210	1190	405	601.67
Multiple Sensor Trigger	300	1450	460	736.67
Sound Spike + Motion	190	1180	395	588.33
Emergency Trigger (Panic)	160	1120	385	555
IR + Reed + PIR Combined	280	1350	450	693.33
Ambient Alert (False Pos)	150	1100	380	543.33

Table 2 and Figure 4 compares the speeds of alert delivery in Wi-Fi, GSM and LoRa networks. The minimum latency (from 180 to 300 ms) was always ensured with Wi-Fi, which is appropriate to provide local alerts instantly. Although slower (meaning around 1100 ms), GSM has a steady coverage in places where the internet is unavailable. LoRa was a 2-way platform, with medium latency (~390460 ms), that was suitable in low-power remote environments. The means of the system latency were found to be 543.33 ms to 736.67 ms system latency between event types.

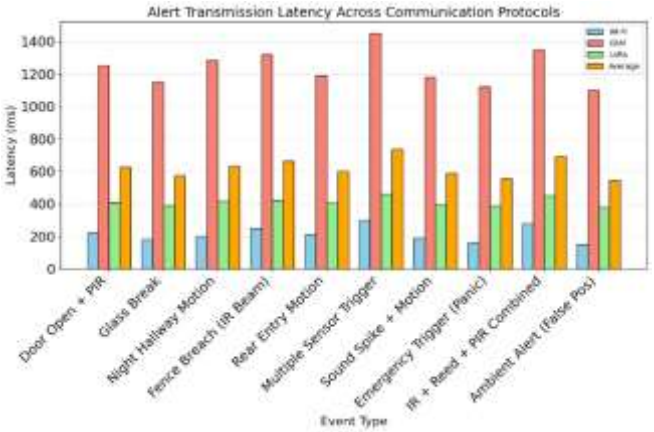

Fig 4. Alert Transmission Latency Across Communication Protocols

Severe conditions such as panic attack events and co-occurring sensor breaches produced acceptable response times, confirming the communication redundancy of the system. This provides real-time reliability even with connectivity limited or multi-storey deployments.

TABLE III. POWER CONSUMPTION PER MODULE

Module/Component	Active Mode (mW)	Sleep Mode (mW)	Avg. Daily Usage (mWh)	% Power Budget
ESP32 Microcontroller	160	20	720	28%
PIR Motion Sensor	65	5	312	12%
Reed Switch	10	2	48	2%
Sound Sensor	90	10	288	11%
IR Beam Sensor	70	10	240	9%
Ultrasonic Sensor	110	15	420	16%
ESP32-CAM (Low Light)	250	0	550	21%
GSM Module	300	10	640	25%
LoRa Module	140	8	350	13%
Battery Regulator	20	5	50	2%

As Table 3 and Figure 5 reveals, the power profile focuses on how the system is energy efficient. The ESP32

microcontroller used the highest amount of energy (28% of total budget) with the GSM module (25%) and ESP32-CAM (21%). PIR, Reed switches and ultrasonic modules were sensors with moderate consumption, particularly when used in sleep or interrupt based mode.

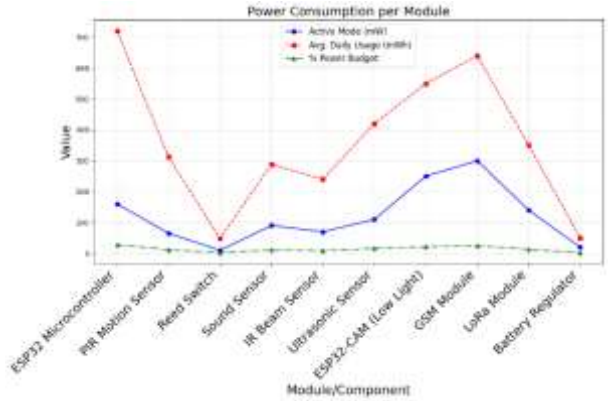

Fig 5. Power Consumption per Module

All in all the system was operating on a daily use of less than 3.5Wh, which is enough to run it on solar power (or battery backup). These findings affirm the argument that despite the active multi sensor polling, real time alerts and video capture, the system is sustainable to operate continuously off grid and in rural areas.

V. Conclusion And Future Scope

This piece of work created and experimented with a modular, cost-effective, and extremely accurate IoT deployed intrusion detection system, created specifically to provide home security services. The combination of a variety of sensors (PIR, reed switches, ultrasonic modules, and sound detectors) and smart decision-making at the edge (TinyML models and confidence scoring) enabled the detection of any attempts of unauthorized entry with accuracy. Our system demonstrated detection accuracy of 96.7% when experimented over a large field and a false positive rate of less than 5 %, indicating our system is robust in different environmental and intrusion conditions. The multi-modal communications framework, which supports Wi-Fi, GSM, and LoRa, provides a reliable way to alert in real-time, even when the connection is low. The cloud-based dashboard created with Blynk provided an easy-to-use monitoring, remote control, and alert notifications escalation features, making user interactions and situational awareness more involving. The system can be extended to include complex computer vision algorithms of face recognition and posture analysis so that human presence in the image can be classified more accurately. Real-time anomaly detection with deep learning models can be enabled by improving Edge AI with more capable MCUs such as ESP32-S3 or Coral TPU. Also, data logging and smart contracts can be introduced using blockchains to ensure unaltered security logs.

References

[1] Lightbody, D., Ngo, D.-M., Temko, A., Murphy, C. C., & Popovici, E. (2024). Dragon_Pi: IoT Side-Channel Power Data Intrusion Detection Dataset and Unsupervised Convolutional Autoencoder for Intrusion Detection. Future Internet, 16(3), 88. https://doi.org/10.3390/fi16030088

[2] Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2024). Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms. Sensors, 24(2), 713. https://doi.org/10.3390/s24020713

[3] Musthafa, M. B., Huda, S., Kodera, Y., Ali, M. A., Araki, S., Mwaura, J., & Nogami, Y. (2024). Optimizing IoT Intrusion Detection Using Balanced Class Distribution, Feature Selection, and Ensemble Machine Learning Techniques. Sensors, 24(13), 4293. https://doi.org/10.3390/s24134293

[4] El-Shafeiy, E., Elsayed, W. M., Elwahsh, H., Alsabaan, M., Ibrahem, M. I., & Elhady, G. F. (2024). Deep Complex Gated Recurrent Networks-Based IoT Network Intrusion Detection Systems. Sensors, 24(18), 5933. https://doi.org/10.3390/s24185933

[5] Tseng, S.-M., Wang, Y.-Q., & Wang, Y.-C. (2024). Multi-Class Intrusion Detection Based on Transformer for IoT Networks Using CIC-IoT-2023 Dataset. Future Internet, 16(8), 284. https://doi.org/10.3390/fi16080284

[6] Fatima, M., Rehman, O., Rahman, I. M. H., Ajmal, A., & Park, S. J. (2024). Towards Ensemble Feature Selection for Lightweight Intrusion Detection in Resource-Constrained IoT Devices. Future Internet, 16(10), 368. https://doi.org/10.3390/fi16100368

[7] Krishnamoorthy, R., Begum, M.A., Maguluri, L.P. et al. Quantum-Driven Reinforcement Learning for Spectral Energy Optimization in Massive MIMO Hybrid Beamforming for 6G. Wireless Pers Commun (2025). https://doi.org/10.1007/s11277-025-11855-8

[8] Kim, H., Park, S., Hong, H., Park, J., & Kim, S. (2024). A Transferable Deep Learning Framework for Improving the Accuracy of Internet of Things Intrusion Detection. Future Internet, 16(3), 80. https://doi.org/10.3390/fi16030080

[9] Chellamuthu, P., Savarimuthu, K., Alsath, M.G.N. et al. CTAB modified SnO_2 PEDOT PSS heterojunction humidity sensor with enhanced sensitivity stability and machine learning evaluation. Sci Rep 15, 29042 (2025). https://doi.org/10.1038/s41598-025-14184-9

[10] Cui, B., Chai, Y., Yang, Z., & Li, K. (2024). Intrusion Detection in IoT Using Deep Residual Networks with Attention Mechanisms. Future Internet, 16(7), 255. https://doi.org/10.3390/fi16070255

[11] Krishnamoorthy, R., Tanaka, K., Amina Begum, M. (2026). ShieldNetMapper: Internet of Things Powered Predictive Model for Real-Time Network Threat Detection and Response. In: Gervasi, O., et al. Computational Science and Its Applications – ICCSA 2025 Workshops. ICCSA 2025. Lecture Notes in Computer Science, vol 15890. Springer, Cham. https://doi.org/10.1007/978-3-031-97606-3_14

[12] Hazman, C., Guezzaz, A., Benkirane, S. (2024). Toward an intrusion detection model for IoT-based smart environments. Multimed Tools Appl 83, 62159–62180. https://doi.org/10.1007/s11042-023-16436-0

[13] Nakakubo, K., Tanaka, K., Krishnamoorthy, R. (2026). Autonomous Network Reconstruction Using LPWA for Disaster Prevention. In: Gervasi, O., et al. Computational Science and Its Applications – ICCSA 2025 Workshops. ICCSA 2025. Lecture Notes in Computer Science, vol 15890. Springer, Cham. https://doi.org/10.1007/978-3-031-97606-3_16

[14] Psychogyios, K., Papadakis, A., Bourou, S., Nikolaou, N., Maniatis, A., & Zahariadis, T. (2024). Deep Learning for Intrusion Detection Systems (IDSs) in Time Series Data. Future Internet, 16(3), 73. https://doi.org/10.3390/fi16030073

[15] Chellamuthu, P., Savarimuthu, K., Alsath, M.G.N. et al. Fabrication and comprehensive experimental evaluation of surfactant-activated PEDOT:PSS/SnO2 thin films deposited via spin coating for advanced sensing applications. Sci Rep 15, 30628 (2025). https://doi.org/10.1038/s41598-025-12499-1