

Lightweight and Flexible Intrusion Detection System to Protect Industrial IoT Settings: Using a Mixed AI Strategy

S. Mythily^{1*}, and Dr.C. Meenakshi²

^{1*}Research Scholar, Department of Computer Science, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamil Nadu, India.
mythilysar1@gmail.com, <https://orcid.org/0009-0000-1684-5073>

²Associate Professor, Department of Computer Application, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamil Nadu, India. cmeenakshi.scs@velsuniv.ac.in,
<https://orcid.org/0000-0002-9020-6031>

Received: October 08, 2025; Revised: December 03, 2025; Accepted: January 06, 2026; Published: March 31, 2026

Abstract

The increasing exposure of the Industrial Control Systems (ICS) and Industrial Internet of Things (IIoT) environments to cyber threats is connected with the proliferation of obsolete industrial protocols, the lack of computational capabilities, and the extended integration of the Information Technology (IT) and Operational Technology (OT) environments. The conventional intrusion detection systems do not work well in such an environment because they are not protocol-aware, are not cheap in terms of computation, and are not capable of operating under the strict real-time requirements. In order to overcome these issues, this paper offers a flexible and lightweight hybrid intrusion detection system that is specially created to be used in industrial networks. The suggested system will integrate protocol-based rule-based detection with machine-based anomaly detection to detect known and unknown cyberattacks. It uses deep packet inspection and time-based statistic feature extraction to record the behavior of industrial traffic, and model optimization technology can be used to effectively deploy to edge devices that have limited resources. NSL-KDD, UNSW-NB15, and custom Modbus-TCP are used to evaluate the system with real and realistic industrial conditions created as a result of a simulated SCADA environment. Experimental results demonstrate that the proposed hybrid intrusion detection system achieves a detection accuracy of 98.6%, with a low false positive rate of 1.4%, significantly outperforming standalone rule-based and machine-learning approaches. Precision, recall, and F1-score consistently exceed 97%, confirming reliable intrusion identification. Moreover, the system has a mean detection latency of less than 8 ms, which meets the real-time performance of industrial monitoring. Finally, the suggested hybrid IDS provides a moderate balance between high detection rates and protocol sensitivity, along with low computational cost, which makes the proposed model a feasible, scalable security tool to be used in real-life ICS and IIoT implementations.

Keywords: IDS, ICS, IIoT, Cyber-security, Anomaly-Detection, Machine-Learning, Edge- Computing.

1. Introduction

The introduction of the Industrial Internet of Things (IIoT) into the current Industrial Control Systems (ICS) has created a great impact on the automation in industries by providing the ability to exchange data in real-time, conduct predictive maintenance, and provide intelligence in controlling the processes (Shrivastwa et al., 2022). Although these developments have enhanced the efficiency and productivity of operations, the acculturation of the Information Technology (IT) with the Operational Technology (OT) has similarly increased the cyber-attack area of industrial settings significantly (Akshya et al., 2025). Consequently, the manufacturing plants, power grids, water treatment plants, and oil refineries that form some of the key infrastructures have become progressively exposed to advanced and cyber threats, turning industrial cybersecurity into an urgent issue (Khraisat & Alazab, 2021).

Historically, industrial control networks used to work separately, but modern ICS implementation strongly depends on mutual interaction between components like Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), and Human-Machine Interface (HMIs) (Alohali et al., 2022). Most of them still run with outdated industrial communications standards, such as Modbus and DNP3, that have no fundamental security mechanisms, such as authentication, encryption, and integrity checking (Aleisa, 2025). This insecure nature opens up industrial processes to any attacks that would disrupt operations, undermine safety, and result in dire economic and social impacts (Kalpani & Rodrigo, 2026).

The relevance of this issue is that the operation requirements of industrial systems are high and necessitate responsiveness in real time, high availability, and a low rate of false alarms (Sinha et al., 2024). The traditional IT-based Intrusion Detection Systems (IDS) cannot usually be used in such environments because of the large computational load, protocol insensitivity, and inability to respond in real-time (Maddu & Rao, 2025). Besides, the processing power and memory of most industrial devices are limited, and this also restricts the use of complicated security solutions (Latif et al., 2021). These issues underscore the seriousness of the requirement to develop lightweight protocol-conscious intrusion detection mechanisms that would be able to deliver accurate and real-time protection without interfering with industrial operations (Mendonca et al., 2022).

Key Contribution

1. Extends protocol-aware rule-based detection and machine-learning-based anomaly analysis to identify known and unknown attacks.
2. Achieves high accuracy (98.6%) and F1-score (97.5%) with a low false positive rate (1.4%) and real-time latency.
3. Edge deployable and optimized so that it can perform efficient, scalable, and reliable intrusion detection in industrial networks.

The paper will tackle the issue of cybersecurity in the industrial IoT and SCADA systems by introducing a lightweight hybrid intrusion detection system. The second section, II, provides a review of the existing IDS approaches that have shown a limitation with regard to the cost of computation, protocol awareness, and real-time implementation. The proposed system is a combination of protocol-sensitive detection rule-based and machine-learning anomaly analysis with optimized feature extraction and edge deployment. Benchmark and custom datasets experimental evaluation shows high accuracy and low false positives, and real-time performance, whereas ablation studies show the contribution of each module. The findings highlight the reliability of the system, and the conclusion

gives the future directions, such as federated learning, adaptive thresholds, explainable AI, and large-scale industrial implementation.

2. Related Work

Industry 4.0 and the Industrial Internet of Things (IIoT) have intensively expanded, and a lot of research has been conducted on the creation of intrusion detection systems that are specific to the industrial control setting (Mallidi & Ramisetty, 2025). The popularity of deep learning-based methods has been motivated by the fact that they are able to learn complex patterns using large-scale industrial data (Schmitt, 2023). They are good at modeling non-linear correlations in network behavior, but typically demand huge computational resources and large labelled datasets, and thus are not readily applicable to run on resource-constrained industrial equipment (Awotunde et al., 2021). Further, they are black-box and thus can be limited in terms of interpretability, which is a very critical requirement for safety-critical industrial systems (Amgbara et al., 2024).

A number of studies have investigated protocol-aware and hybrid intrusion detection to overcome protocol specificity and real-time problems in Supervisory Control and Data Acquisition (SCADA) systems (Soomro et al., 2024). Hybrid IDS models are those that combine protocol-based rules with anomaly detection methods and provide lower detection latencies and high detection accuracy in known attack signatures (Villafranca et al., 2025). Although these have these benefits, such systems are usually not good at detecting zero-day attacks and can also have high false positive rates when being loaded dynamically in industrial environments (Moustafa et al., 2023). Federated learning-based IDS architectures have also been suggested more recently to improve privacy and facilitate distributed model training between distributed industrial nodes. In spite of the fact that federated learning improves privacy, it creates other issues concerning communication overhead, delays in model synchronization, and convergence, which can restrict applicability in real-time applications in industrial contexts (Latif et al., 2020). Generally, the solutions that are currently available in the market lack protocol awareness, require huge computational resources, or cannot be deployed in a real-life scenario in industries, hence the need to have a lightweight, protocol-aware, and real-time hybrid intrusion detection system (Fatima et al., 2024; Heidari & Jamali, 2023).

The current IDS solutions to industrial settings exhibit promising detection performance, though most of them have at least one significant drawback, such as excessive computation power, protocol blindness, failure to detect zero-day attacks, or failure to satisfy the real-time requirements of edge deployment. Deep learning models are resource-intensive and highly accurate, whereas rule-based systems cannot be generalized to unknown attacks. The approach of federated learning creates communication latency and synchronization burden. The constraints drive the desire for a lightweight, protocol-sensitive hybrid intrusion detection system that is able to maintain accuracy in detection, computational efficiency, and viability in real-time in an industrial control system.

3. Proposed System

Some of the issues that this paper aims to solve include the occurrence of false alarms, protocol problems, and elevated processing needs. The system emphasizes real-time surveillance, and it works effectively in edge configurations and identifies emerging risks and familiar ones in ICS and IIoT systems.

This architecture consists of four major components, which include the Data Acquisition Module, the Hybrid Detection Engine, and the Response and Alert Manager. The system is operated close to

industrial machines such as PLCs and RTUs to ensure that the process of packet inspection is speedy. The data packets are snatched by a small sniffing agent, processed, and forced through two forms of detection. The former operates by on-the-fly rule-based discovery of the known threats, whereas the latter operates with the help of an ML model to discover unusual behavior. The alert manager will relay important intrusion reports to human operators or control systems in order to respond.

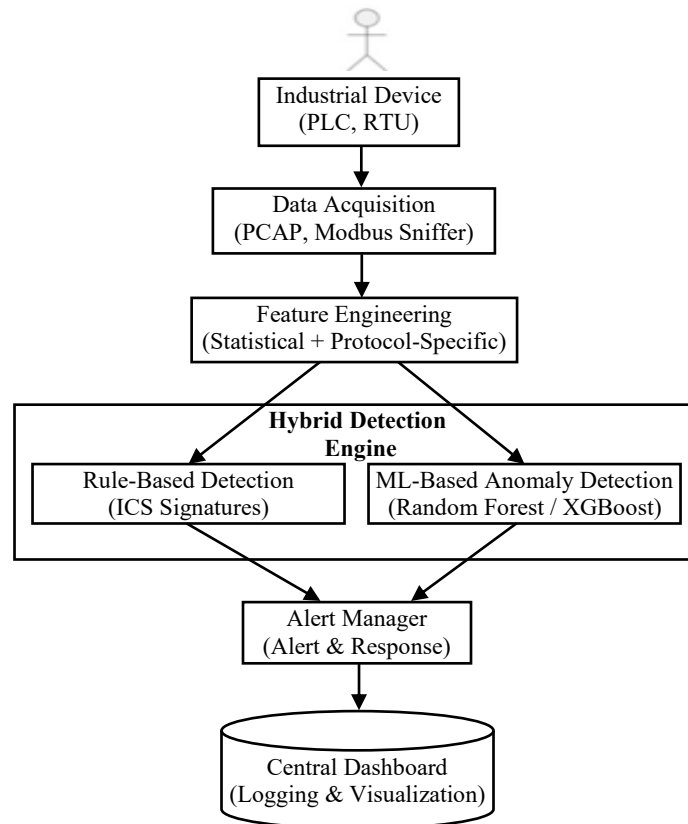


Figure 1: A hybrid IDS architecture proposed for industrial control

The proposed hybrid intrusion detection system, which is to be used in industrial settings, is set up in figure 1. It has a rule-based system and an ML model to detect known attacks. The Alert Manager handles the detected intrusions by maintaining logs, issuing alerts, and initiating automatic defense measures. All events and decisions that are logged are forwarded to a Central Dashboard in order to visualize and examine them. The entire system is configured to be deployed in real-time at the edge level in SCADA systems and in Industrial IoT systems.

3.1 Data Collection and Feature Design

The suggested intrusion detection system uses the data collected during the industrial network traffic to create a realistic and protocol-compatible analysis. The capture of network packets is done at the edge of both ICS and IIoT environments with an emphasis on industrial communication streams. Temporal and statistical characteristics such as the frequency of commands, packet rate, error response rate, time between packets, and specific protocol operation codes are also extracted to identify normal and malicious behavior. The Information Gain and Recursive Feature Elimination (RFE) are used to select the best features, minimize the computation cost, and enhance the detection performance of the resource-constrained industrial machines.

Three datasets of training, validation, and testing are used to evaluate the effectiveness of the proposed model. After the selection of features that are relevant in the industrial traffic, the NSL-KDD dataset is used in baseline training and comparative analysis. The UNSW-NB15 data set is the representation of contemporary intrusion cases concerning the variety of attack types. Also, a custom Modbus-TCP dataset is created in the SCADA testbed with Industrial Shields hardware and the Modbus Poll tool, which records real communication between HMIs and PLCs and attacks, including replay, flooding, and unauthorized write operations. This composition makes it possible to do a holistic and protocol-conscious assessment in an actual industrial setting.

Table 1: List of datasets used to evaluate models

Dataset	Year	Type	Protocols Used	Attack Types Included	Objectives
NSL-KDD	2009	Benchmark (Generic)	TCP/IP	Denial-of-Service	Model pre-training & comparison
UNSW-NB15	2015	Benchmark (Modern)	TCP/IP	Exploits, Fuzzers, Recon, Backdoors	Anomaly model training
Custom Modbus-TCP	2024	Simulated ICS Dataset	Modbus- TCP	Replay, Write Attack, Flood, Illegal Function Calls	Realistic protocol-aware testing

Table 1 provides an overview of the data that was available to test the proposed intrusion detection system. It contains benchmark and industrial traffic data of protocol-specific and generic traffic. NSL-KDD is applied in the pre-training of the initial model and comparison, and UNSW-NB15 is offered with the current intrusion settings, testing the powerful capabilities to detect anomalies. The design of the custom Modbus-TCP dataset is to mirror realistic patterns of industrial communication and protocol-level attacks, and allows evaluation of protocol-awareness under the conditions of the ICS.

3.2 Engine Detection During Hybrid Mode

The intrusion detection system is created in the form of a two-layered hybrid detection engine in order to respond to both known and unknown attacks. The former layer is a rule-based detection module, which uses protocol-sensitive rules based on industrial standards and specifications of the Modbus-TCP. This layer is effective in detecting known attack signatures, malformed packets, and protocol violations with minimum latency.

The second layer uses a machine-learning-based anomaly detector with the help of such algorithms as Random Forest and XGBoost. This element examines behavioral patterns within the extracted features to identify an anomaly that can be a zero-day attack or an attack that has not been recognized. The hybrid approach allows for tremendous improvement of detection accuracy with minimal false positives by combining rule-based accuracy and machine-learning flexibility in the detection approach. In order to have runnability on edge devices, model optimization tools like model size reduction and quantization are used, making it possible to run on a platform like Raspberry Pi and the NVIDIA Jetson Nano.

Algorithm 1: Lightweight Protocol-Aware Hybrid IDS for ICS/IIoT

Input:

Captured packet stream $\mathcal{P} = \{p_1, p_2, \dots\}$, time window size W , ruleset \mathcal{R} , trained ML model $f(\cdot)$, decision thresholds τ_r, τ_m

Output:

Final label $\hat{y} \in \{0,1\}$ where 0 = Normal, 1 = Attack; alert/log actions

Steps:

1. **Initialize** rule engine with \mathcal{R} ; load ML model $f(\cdot)$; set window W .
2. For each incoming packet p_t :
 - 2.1 Parse protocol fields (e.g., Modbus function code, unit id, address, length).
 - 2.2 Insert p_t into the sliding window buffer \mathcal{B} of length W .
3. **Feature Extraction:** When the window is full (or every Δt):
 - 3.1 Compute statistical + timing features vector \mathbf{x}_t from \mathcal{B} .
 - 3.2 Apply feature selection mask \mathbf{m} (Information Gain / RFE): $\mathbf{x}'_t = \mathbf{m} \odot \mathbf{x}_t$.
4. **Layer-1 Rule Detection:**
 - 4.1 Compute rule score $s_r = g(\mathcal{R}, \mathcal{B})$.
 - 4.2 If $s_r \geq \tau_r$, set $\hat{y} = 1$ (Attack) and go to Step 6.
5. **Layer-2 ML Anomaly Detection:**
 - 5.1 Compute ML probability $s_m = f(\mathbf{x}'_t) \in [0,1]$.
 - 5.2 If $s_m \geq \tau_m$, set $\hat{y} = 1$ else $\hat{y} = 0$.
6. **Fusion & Response:**
 - 6.1 Fuse final decision: $\hat{y} = I[(s_r \geq \tau_r) \vee (s_m \geq \tau_m)]$.
 - 6.2 If $\hat{y} = 1$: log event, send alert via MQTT/HTTP, optionally block IP / isolate device.
 - 6.3 Else: store summary statistics and continue monitoring.
7. Repeat for the next packets.

The proposed workflow of the protocol-aware lightweight intrusion detection system is described in Algorithm 1. This algorithm analyzes the traffic of industrial networks with the help of the sliding time window, derives statistically significant and timing characteristics, and implements a two-layer detection strategy. The protocol-specific rule evaluation identifies known attacks, whereas the unknown or anomalous behavior is identified with the aid of a machine-learning model. The resulting decision is a combination of the two layers, which allows for the detection of intrusions precisely and in real-time with fewer computing resources, as this is appropriate to implement in ICS and IIoT settings.

3.3 Mathematical Model of the Proposed IDS

The analysis of mathematical formulation specifies the traffic behavior, the hybrid detection decision, and the performance analysis of the proposed intrusion detection system. These equations offer formal grounds for the correct identification of intrusions and reliability in both ICS and IIoT systems.

Feature Extraction Using Packet Rate (Traffic Intensity)

In this equation, equation 1 calculates the rate at which packets are being transmitted during a fixed period, in which N represents the number of packets that are recorded, and ΔT is the time that the observation window is taking. Anomalous growth of the packet rate is a sign of flooding or denial-of-service of ICS and IIoT networks.

$$\lambda = \frac{N}{\Delta T} \tag{1}$$

Hybrid Intrusion Detection Decision Function

The decision acts as a hybrid of the results of the protocol-aware rule-based detector (s_r) and the machine-learning-based anomaly detector (s_m). Intrusion is called when one of the detection layers surpasses its threshold, which allows the discrimination of both known and unknown attacks (Equation 2).

$$\hat{y} = \mathbb{I}[(s_r \geq \tau_r) \vee (s_m \geq \tau_m)] \quad (2)$$

False Positive Rate (FPR)

False Positive Rate is the ratio of normal traffic by industrial to malicious traffic. In industries, a low FPR is essential, and a large number of false alarms may disrupt the workflow and decrease the reliability of the system (Equation 3).

$$\text{FPR} = \frac{FP}{FP+TN} \quad (3)$$

3.4 Response and Alerting Mechanism

When suspicious or malicious activity is detected, the response and alerting module is triggered. The system produces elaborate logs and broadcasts lightweight communications like MQTT or HTTP alerts to a central monitoring dashboard. In critical intrusion events, automatic response measures such as blocking the IP addresses of devices or isolating them can be activated to prevent further spread of the attack. Events are all logged and stored safely to facilitate forensic analysis, auditing, and investigation of the incident after it has taken place.

3.5 Experimental Environment

All tests are run using the Python 3.11 version, where Scikit-learn and XGBoost are used to build models. The datasets are partitioned into 70% training, 15% validation, and 15% testing subsets to ensure unbiased evaluation. Measurement of performance measures like accuracy, precision, recall, F1-score, false positive rate, and detection latency is taken. The real-time detection latency and system responsiveness are properly captured using Wireshark-based traffic logs and synchronized system clocks.

Table 2: Key parameter initialization

Parameter Name	Range / Value
Time Window Size (W)	1 – 5 seconds
Packet Rate Threshold (τ_r)	0.6 – 0.9
ML Decision Threshold (τ_m)	0.5 – 0.8
Number of Trees (Random Forest)	50 – 200
Learning Rate (XGBoost)	0.01 – 0.3
Quantization Bit Width	8 – 16 bits

Table 2 shows the most significant parameters and relevant range to set the proposed hybrid intrusion detection system to guarantee the balanced detection accuracy, real-time functionality, and effective implementation in resource-limited ICS and IIoT systems.

4. Results and Discussion

The suggested hybrid intrusion detection system will aim at detecting known and unknown cyber threats in a real-time industrial communication setup. The test system was tested on the data sets and experimental design in Section IV, especially on industrial networks that were running on the Modbus-TCP. The goal of this evaluation is to determine the detection accuracy, reliability, and viability of real-time in practice scenarios of ICS and IIoT.

4.1 Evaluation Metrics

The intrusion detection system performance is measured against popular classification and real-time performance metrics.

The accuracy is the general accuracy of the intrusion classification (Equation 4).

$$Acc = \frac{TP+TN}{TP+TN+FP+FN} \quad (4)$$

Precision is when the system minimizes the false alarms and is able to detect malicious traffic correctly (Equation 5).

$$Prec = \frac{TP}{TP+FP} \quad (5)$$

Recall (sensitivity) is used to test how the system is sensitive in identifying real intrusions (Equation 6).

$$Rec = \frac{TP}{TP+FN} \quad (6)$$

F1-score is a balanced score, which is an aggregate of precision and recall (Equation 7).

$$F1 = \frac{2 \cdot Prec \cdot Rec}{Prec + Rec} \quad (7)$$

False Positive Rate (FPR) is utilized to measure the percentage of harmless industrial traffic that has been wrongly identified as hostile and is a crucial factor when operating safety-critical industries (Equation 8).

$$FPR = \frac{FP}{FP+TN} \quad (8)$$

Moreover, detection latency is the duration to detect an intrusion following capture of traffic, which indicates how well the system can be deployed in real-time (Equation 9).

$$L = T_{capture} + T_{feature} + T_{rule} + T_{ml} + T_{alert} \quad (9)$$

Figure 2 will compare the performance of the proposed hybrid intrusion detection system with machine-learning and rule-based systems on various metrics of evaluation on the Modbus-TCP dataset. The accuracy, precision, recall, and F1-score of the proposed model are always higher, and the false positive rate is much lower, which proves its effectiveness and reliability in real-time intrusion detection in ICS and IIoT systems.

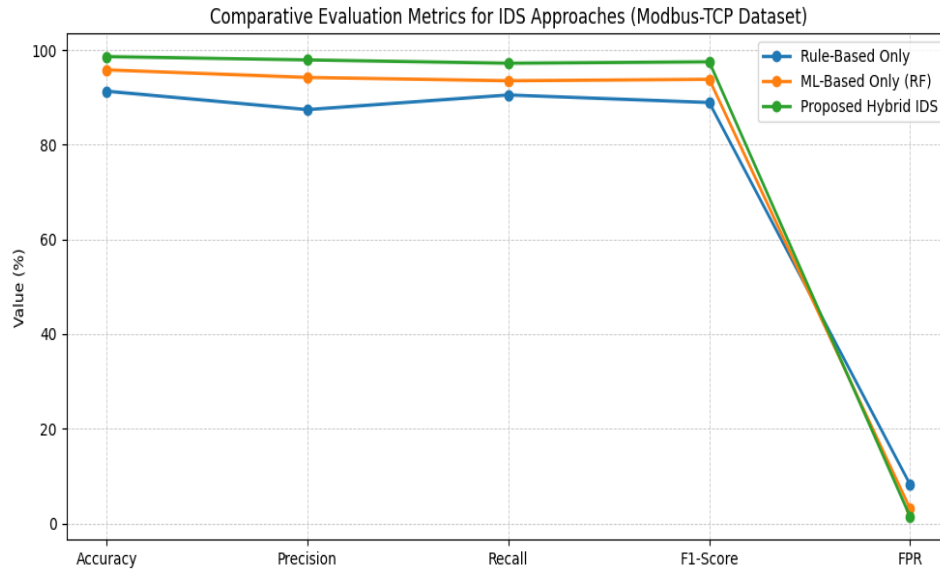


Figure 2: Comparative evaluation of intrusion detection performance across key metrics

4.2 Performance Comparison

A reasonable experimental setup and the same datasets are used to compare the performance of the new intrusion detection models with already existing models, so as to be fair and reproducible. The suggested hybrid intrusion detection system is compared to purely rule-based and machine learning based methods on the same system of the Modbus-TCP data, feature set, and data partitioning strategy. All models are trained and evaluated in the same conditions, and their results are evaluated using common evaluation measures, such as accuracy, precision, recall, F1-score, false positive rate, and detection latency. The comparative analysis allows for an objective evaluation of the detection effectiveness, reliability, and feasibility in real-time in terms of the positive and negative aspects of each method in industrial control system settings.

Table 3: Comparative performance analysis of IDS approaches on the Modbus-TCP dataset

Model Type	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)	Avg. Detection Latency (ms)
Rule-Based Only	91.3	87.4	90.5	88.9	8.2	6.5
ML-Based Only (RF)	95.8	94.2	93.5	93.8	3.1	18.7
Proposed Hybrid IDS	98.6	97.9	97.2	97.5	1.4	7.8

Table 3 presents a comparison between the suggested hybrid IDS and individual rule-based and machine-learning-based methods on the dataset of the Modbus-TCP. The hybrid IDS achieves the highest detection accuracy (98.6%), with precision, recall, and F1-score exceeding 97%, while maintaining a low false positive rate of 1.4% and average detection latency below 8 ms, demonstrating superior accuracy and real-time efficiency over existing models.

4.3 Confusion Matrix Analysis

The confusion matrix measures the accuracy of the proposed IDS in classification, i.e., depicts the correct and incorrect predictions of the normal and attack classes. The large diagonal values and low rates of misclassification attest to the reliability and the correct performance of the intrusion detection model.

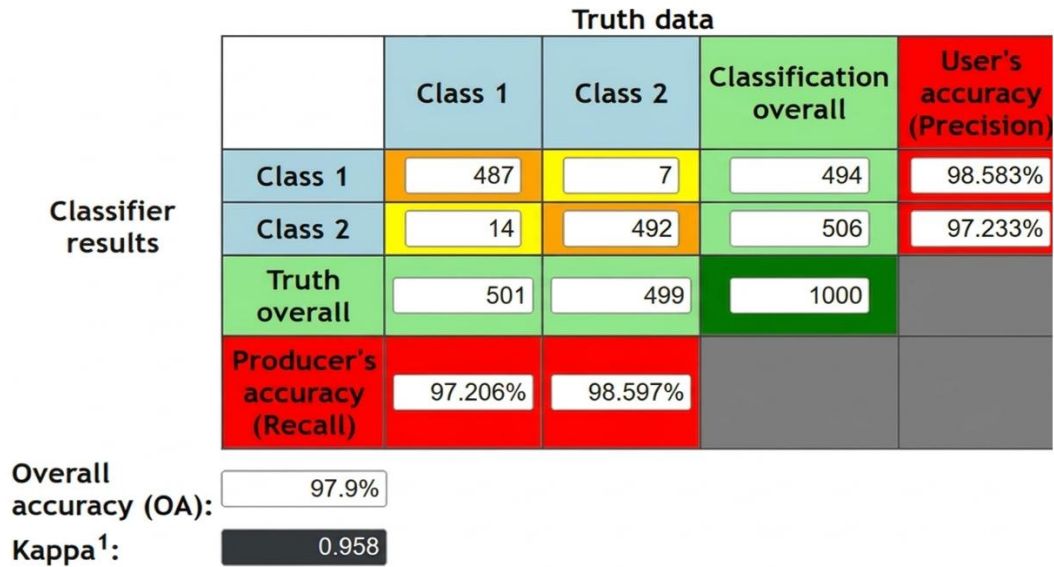


Figure 3: Confusion matrix and classification accuracy of the proposed hybrid IDS

The proposed IDS confusion matrix is presented in figure 3, which indicates its effectiveness in classifying normal and attack classes. The system achieves an overall accuracy of 97.9% with a Cohen's Kappa coefficient of 0.958, indicating a strong level of agreement beyond chance. The values of high precision (user-confidence) and recall (producer-confidence) also confirm the strength and stability of the suggested system to identify cyber threats in the industrial setting correctly.

4.4 Discussion of Results

The effectiveness of the combination of protocol-aware rule-based and machine-learning-based anomaly analysis is the main reason why the proposed hybrid intrusion detection system has better performance. The rule-based component has been shown to correctly detect known attack signatures and protocol violations using the industrial protocol specifications, and as such, to result in rapid and accurate detection at low computational costs. Simultaneously, the anomaly detection module performs an analysis of the behavioral patterns within the network traffic so that the system can identify previously unknown or zero-day attacks that cannot be identified using standard rules. This complementary design has a considerably high degree of overall detection accuracy and robustness.

The sufficiently low false positive rate makes it clear that the suggested system can be considered reliable, which is a significant demand in the industrial setting where false alarms are too many and may disrupt the entire flow and stabilize the system. The hybrid method will minimize false alarms and enhance sensitivity to real suspected attackers since it will be more efficient at filtering benign traffic. The system also has a low detection latency, which proves that the system can be used in both real-time SCADA and IIoT networks. The optimized detection process can also be deployed successfully on resource-constrained edge devices even without causing any operational delays, which means that the proposed IDS can be successfully deployed to real industrial tasks.

Ablation was carried out to determine the personal effects of the system components on the overall detection performance. In cases where a rule-based module was applied, the system was more successful at detection and had high false positive rates, but could not detect hidden attacks. Also, the detection latency and computational overhead were higher when only the machine-learning module was used,

which enhanced the detection of anomalies. The hybrid setup that incorporates rule-based and anomaly detection modules was the most suitable as it produces the highest accuracy, false positives, and real-time performance, and this proves that every element is important in improving the efficiency of the proposed intrusion detection system.

5. Conclusion

The proposed research is a lightweight and adaptable hybrid intrusion detection system (IDS) developed specifically to work in industrial IoT (IIoT) and SCADA systems. This proposed system is very effective in combining protocol-aware rule-based and machine-learning-based anomaly detection in order to combat known and novel cyber threats. Competitions with NSL-KDD, UNSW-NB15, and a knowledge-based modified Modbus-TCP database indicate that the hybrid IDS is always more effective than single rule-based and machine-learning methods. The system achieved a detection accuracy of 98.6%, precision of 97.9%, recall of 97.2%, and F1-score of 97.5%, while maintaining a low false positive rate of 1.4% and an average detection latency of 7.8 ms. These findings affirm that the hybrid solution is a quality, real-time, and computationally efficient security solution that can be deployed on resource-constrained edge devices in industrial networks. The ablation experiment also highlights the complementarity of the rule-based and machine-learning parts and demonstrates that the combination of the two guarantees the best balance between fast detection, anomaly identification, and false alarms.

The results point to the relevance of protocol-awareness integration with adaptive anomaly detection in improving the cybersecurity of critical industrial infrastructures. The statistical results not only suggest high detection but also operational reliability in the actual industrial traffic applied conditions, which is crucial in continuous monitoring of industries. Future studies could be done on how this framework can be extended to federated learning to allow collaborative threat intelligence between distributed IIoT nodes, dynamic conditions in detection thresholds, and the ability to integrate with more advanced edge-computing platforms to support large-scale industrial deployments. Also, explainable AI methods may help increase the interpretability of the industrial operators, and the long-term field testing of the different industrial fields would further confirm the scalability and resilience. All in all, the suggested hybrid IDS offers an effective and solid base for protecting the modern industrial networks against changing cyber threats.

References

- [1] Akshya, J., Sundarajan, M., Vijayakumar, R., Dhanaraj, R. K., & Nayyar, A. (2025). Explainable AI-driven intrusion detection for securing IoT-enabled autonomous transportation systems. *Cluster Computing*, 28(14), 884. <https://doi.org/10.1007/s10586-025-05617-1>
- [2] Aleisa, M. A. (2025). Enhancing security in cps industry 5.0 using lightweight mobilenetv3 with adaptive optimization technique. *Scientific Reports*, 15(1), 18677. <https://doi.org/10.1038/s41598-025-00496-3>
- [3] Alohal, M. A., Al-Wesabi, F. N., Hilal, A. M., Goel, S., Gupta, D., & Khanna, A. (2022). Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment. *Cognitive Neurodynamics*, 16(5), 1045-1057. <https://doi.org/10.1007/s11571-022-09780-8>
- [4] Amgbara, S. I., Akwiwu-Uzoma, C., & David, O. (2024). Exploring lightweight machine learning models for personal internet of things (IoT) device security. *World Journal of Advanced Research and Reviews*, 24(2), 1116–1138. <https://doi.org/10.30574/wjarr.2024.24.2.3449>

- [5] Awotunde, J. B., Chakraborty, C., & Adeniyi, A. E. (2021). Intrusion detection in industrial internet of things network-based on deep learning model with rule-based feature selection. *Wireless communications and mobile computing*, 2021(1), 7154587. <https://doi.org/10.1155/2021/7154587>
- [6] Fatima, M., Rehman, O., Rahman, I. M., 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] Heidari, A., & 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>
- [8] Kalpani, N., & Rodrigo, N. (2026). Securing industry 4.0: a systematic review of AI-driven intrusion detection approaches and emerging trends. *Journal of Reliable Intelligent Environments*, 12(1), 1. <https://doi.org/10.1007/s40860-025-00264-0>
- [9] Khraisat, A., & Alazab, A. (2021). A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity*, 4(1), 18.
- [10] Latif, S., Driss, M., Boulila, W., Huma, Z. E., Jamal, S. S., Idrees, Z., & Ahmad, J. (2021). Deep learning for the industrial internet of things (iiot): A comprehensive survey of techniques, implementation frameworks, potential applications, and future directions. *Sensors*, 21(22), 7518. <https://doi.org/10.3390/s21227518>
- [11] Latif, S., Zou, Z., Idrees, Z., & Ahmad, J. (2020). A novel attack detection scheme for the industrial internet of things using a lightweight random neural network. *IEEE access*, 8, 89337-89350. <https://doi.org/10.1109/ACCESS.2020.2994079>
- [12] Maddu, M., & Rao, Y. N. (2025). Integrated Intrusion Detection and Mitigation Framework for SDN-Based IIOT networks using lightweight and adaptive AI techniques. *Journal of Information Systems Engineering & Management*, 10(9s), 456-472.
- [13] Mallidi, S. K. R., & Ramisetty, R. R. (2025). Advancements in training and deployment strategies for AI-based intrusion detection systems in IoT: a systematic literature review. *Discover Internet of Things*, 5(1), 8.
- [14] Mendonca, R. V., Silva, J. C., Rosa, R. L., Saadi, M., Rodriguez, D. Z., & Farouk, A. (2022). A lightweight intelligent intrusion detection system for industrial internet of things using deep learning algorithms. *Expert Systems*, 39(5), e12917. <https://doi.org/10.1111/exsy.12917>
- [15] Moustafa, N., Koroniotis, N., Keshk, M., Zomaya, A. Y., & Tari, Z. (2023). Explainable intrusion detection for cyber defences in the internet of things: Opportunities and solutions. *IEEE Communications Surveys & Tutorials*, 25(3), 1775-1807. <https://doi.org/10.1109/COMST.2023.3280465>
- [16] Schmitt, M. (2023). Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection. *Journal of Industrial Information Integration*, 36, 100520. <https://doi.org/10.1016/j.jii.2023.100520>
- [17] Shrivastwa, R. R., Bouakka, Z., Perianin, T., Dislaire, F., Gaudron, T., Souissi, Y., ... & Guilley, S. (2022, October). An embedded AI-based smart intrusion detection system for edge-to-cloud systems. In *International Conference on Cryptography, Codes and Cyber Security* (pp. 20-39). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-23201-5_2
- [18] Sinha, R., Thakur, P., Gupta, S., & Shukla, A. (2024). Development of lightweight intrusion model in Industrial Internet of Things using deep learning technique. *Discover Applied Sciences*, 6(7), 346. <https://doi.org/10.1007/s42452-024-06044-4>
- [19] Soomro, I. A., Hussain, S. J., Ashraf, Z., Alnfai, M. M., & Alotaibi, N. N. (2024). Lightweight privacy-preserving federated deep intrusion detection for industrial cyber-physical system. *Journal of Communications and Networks*, 26(6), 632-649. <https://doi.org/10.23919/JCN.2024.000054>

- [20] Villafranca, A., Thant, K. M., Tasic, I., & Cano, M. D. (2025). AI-Enabled IoT Intrusion Detection: Unified Conceptual Framework and Research Roadmap. *Machine Learning and Knowledge Extraction*, 7(4), 115. <https://doi.org/10.3390/make7040115>

Authors Biography



S. Mythily holds M.Sc., M.Phil., and B.Ed. degrees and is currently a Research Scholar in the Department of Computer Science at Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai. She has over 14 years of academic experience in teaching. Her academic interests include Cloud Computing, Artificial Intelligence, and IoT applications. She has contributed to scholarly work through journal publications, a book chapter in AI and IoT Applications, and paper presentations at national and international conferences. Actively involved in curriculum development and student mentorship, she is passionate about enhancing student learning and academic excellence. She has been recognized for her contributions with the Women Icon Award 2024 in the IWR Book of Records.



Dr.C. Meenakshi is an Associate Professor in the Department of Computer Applications (PG), School of Computing Sciences at Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai. She holds MCA, M.Phil., and Ph.D. degrees and has over 18 years of academic experience in teaching and research. She has made significant contributions to the field of Computer Science, with research interests spanning Artificial Intelligence, Natural Language Processing, IoT, and emerging technologies. She has published 56 research articles in reputed journals, authored 4 books, presented papers at national and international conferences, and holds 4 patents. A dedicated academician and mentor, she has received multiple awards, guided research scholars, secured project grants, and actively participated in FDPs, workshops, and NPTEL courses. Her commitment to academic excellence and innovation continues to inspire students and researchers alike.