RESEARCH ARTICLE OPEN ACCESS

A Robust IDS-Driven Approach to Secure Industrial Control Systems from Emerging Cyber-Physical Attacks

D Nagabhushanam . K Veerasekhar Achari . P Kranthi Kumar . S Abrar Ali . R Manoj Kumar Reddy

Department of CSE (IoT and Cyber Security including Block Chain Technology),
Annamacharya Institute of Technology & Sciences (Autonomous),
Tirupati, A.P, India.

DOI: **10.5281/zenodo.18756378**
Received: 28 January 2026 / Revised: 18 February 2026 / Accepted: 23 February 2026

**Corresponding Author: bhushan.duggi@gmail.com*

Abstract – CPS are critical for the operation of many infrastructures, such as ICS, energy, and transportation. However, increasingly interconnecting cyber with physical elements opens the floor for complicated cyber-physical attacks targeting severe operational disruption. This paper proposes an efficient approach, basically IDS-driven, for securing ICS against such advanced threats. A lightweight hybrid IDS is proposed for the efficient detection of known attacks as well as unknown zero-day attacks using supervised and unsupervised training models, respectively. The suggested IDS incorporates the LightGBM and Isolation Forest models for signature-based detection and anomaly-based detection, respectively. This will ensure that the threat detection is comprehensive in dynamic industrial environments with timely identification and response against both traditional and evolving cyber-physical threats. In our experimental results, the proposed H-IDS was evaluated using the NSL-KDD dataset and outperformed the traditional approaches in terms of accuracy, precision, and recall. Moreover, it will bring benefits like reduced false positive rates, speed, and resiliency. Some possible improvements that can be made in the future are also discussed in the paper, such as incorporating edge computing with federated learning, which can enhance capabilities for the proposed system in real-time environments.

Index Terms – Industrial Control System, LightGBM, Isolation Forest, Cyber Physical Threat, Machine Learning, Django Framework.

I. INTRODUCTION\

The increased interaction of computational intelligence, connectivity, and physical systems in CPS has led to security being a major concern in several infrastructures, such as industrial IoT, autonomous vehicles, energy, and healthcare systems. The new CPS ecosystem is marked by a complex attack surface that utilizes a wide range of security threats in terms of cybersecurity and physical security, which necessitates a multi-layer security approach that goes beyond security norms.

The multi-layered architecture that combines machine learning approaches with the application of tamper-resistant loggers has been shown to offer improved detection rates and recovery times, which indicates that there have been significant advances towards achieving improved accuracy and continuity in attack situations [1]. Hybrid anomaly detection models that combine network traffic and physical sensor data for analysis have been found to provide better attack identification compared to other methods, which addresses the subtle attack vectors for industrial CPS applications [2]. Lightweight deep learning architectures for Industry 5.0 applications have also been found to provide better CPS adaptation and scalability, particularly for embedded systems [3]. Other research studies have also emphasized the need for security engineering methodologies that involve systematic security threat modeling, including life-cycle assessment and iterative risk evaluation of various components of the CPS [4][5].

Edge computing-based intrusion detection systems have been proposed to enable the continuous analysis of traffic and the segregation of potential threats within the IIoT environment, thus reducing latency and decentralizing the intrusion detection logic [6]. New frameworks in the domain of AI-powered CPS have been proposed to facilitate the automated evaluation of the dependability of the system, thereby ensuring the validation of the AI-powered CPS environment, which is usually associated with the challenges of the adaptive nature of the AI components [7]. Monitoring frameworks with the incorporation of role-based security logic in the sensor network provide alternative approaches to the integrity of the distributed CPS environment [8]. TEE-based security frameworks for the controller security environment provide additional layers of validation against the manipulations of the adversaries with negligible performance overhead [9]. Large-scale architectural frameworks that facilitate the incorporation of edge computing, federated learning, and distributed coordination provide the next generation of real-time response to the anomalies in the autonomous network-centric CPS environment [10]. Such advancements signal the beginning of a new era of CPS security, which is moving towards more integrated, adaptive, and scalable security solutions. Leveraging the advancements of the past few years, this paper aims to synthesize the state-of-the-art techniques and point out the challenges in real-world CPS security deployments.

Our contributions are as follows:

- Hybrid IDS Architecture: In this section, we propose our novel concept of a Hybrid Intrusion Detection System (H-IDS) with supervised and unsupervised learning techniques. This will improve the overall detection of various types of security risks and threats compared to other conventional techniques.
- Dual-Model Detection Strategy: Together, LightGBM and Signature-Based Intrusion Detection can be used for structured attacks, whereas Isolation Forest can be utilized for anomaly detection, enabling our system to be agile enough to cope with a changing threat environment.
- Decision Level Fusion: The proposed technique is built with a decision level fusion component that integrates the results yielded by the supervised and unsupervised models. The technique of fusing these results has been effective in minimizing the false positives and negatives.

- Comprehensive Evaluation on Real-World Datasets: The proposed H-IDS model is tested on the NSL KDD dataset to prove its efficiency in comparison to current models in terms of accuracy, precision, recall, F1 score, and AUC values in identifying cyber-physical attacks.
- Operational Performance of Real-Time H-IDS with ICS Deployment: The performance of the system is also evaluated based on real-time criteria, such as its response time, rate of false positives, and CPU utilization. The proposed H-IDS is found to offer the optimal balance of performance and efficiency.

II. LITERATURE SURVEY

The modern critical infrastructures, such as the energy grids, transportation structures, water treatment plants, and industrial manufacturing systems, contain Cyber-Physical Systems (CPS). The close interconnection between cyber and physical parts has, however, been a major contributor to the vulnerability of systems to coordinated cyber-physical attacks. In turn, some of the recent studies have aimed at incorporating artificial intelligence, machine learning, blockchain, and edge computing to improve CPS security, resilience, and adaptability. A coherent CPS-based security framework proposed by Chowdhury et al. [11] combines real-time monitoring, AI/ML analytics, and blockchain to defend infrastructures of vital importance. The framework enhances the strength of the system, speed of threat awareness, and automation of response mechanisms using trusted architectures. Although the design is holistic, it is limited by the high deployment costs, scalability problems, inability to integrate with the legacy system, and high dependence on the correctness of AI.

Pandey et al. [12] presented a CPS security model that relied on actuator state transition analysis to create an anomaly detection model that is data-driven. The procedure was employed to forecast and compare the real and foreseen actuators with deep neural networks and Hamming distance, which obtained an F1-score of 0.96 in a water treatment testbed. Though successful in the case of stealthy attacks, not trained on physics-based models, the method relies on high-quality training data, is expensive to compute, and suffers from generalization issues in the case of heterogeneous CPS environments. Another type of cloud-fog automation of autonomous industrial CPS was suggested by Jin et al. [13] as an alternative to the conventional ISA-95 architecture. This framework takes advantage of the 3C co-design - communication, computing, and control to provide system-wide autonomy and cyber-physical security. Although the methodology is applied to tackle the problem of fragmentation in the design of industrial CPS, it cannot be experimentally verified, and there are questions about its scalability, interoperability, and complexity of deployment.

Almederes et al. [14] proposed an LSTM-based intrusion detection framework that can identify both cyber attacks and black box attacks on the industrial control systems to combat adversarial threats. It proves to be a good system in detecting under realistic DDoS and adversarial conditions. Nevertheless, the fact that it is based on supervised learning, has scalability constraints, and is limited to evaluation in a wide range of industrial settings is still a significant weakness. Nittala et al. [15] have developed an AI-based intrusion response system (AIRS) to counteract cyber-physical attacks in the ERP-governed infrastructures. The system decreases time to detect and respond during a hybrid ERP-ICS testbed through the use of graph-temporal modeling and safety-shielded reinforcement learning. Although the solution proved to be effective, it presents the problem of high integration costs, complexity in deployment, dependence on digital twins, and the requirement to monitor the solution constantly.

Patel et al. [16] proposed a sophisticated programmable defense mechanism to CPS security that incorporates anomaly detection, machine-learned threat prediction, and a secure system structure. This is a holistic solution that goes beyond the siloed, stagnated security solutions to allow adaptive, cross-disciplinary defense strategies. However, the non-experimental validation is not scalable, and the difficulty of implementation makes it less applicable in real life. Mahmud et al. [17] covered the issue of CPS security at the industrial edge and suggested a trusted microservice orchestration framework of secure edge computing. The model includes a model of trust to identify the abnormal behaviour of microservices in resource-constrained setups. Although new in terms of moving security enforcement to edge-centric CPS rather than the cloud-centric CPS, the method has only been confirmed by simulations and adds a complexity and scalability overhead of orchestration.

Bhardwaj et al. [18] introduced an attack-based security architecture of the cyber-physical robots that studies the logs of the system and determines vulnerabilities on the basis of the device-sensor classification. The framework enhances focused defense mechanisms by focusing on vulnerabilities that can be exploited instead of using blanket-based protection. Its dependence on predetermined attack trees, quality of logs, and absence of large-scale validation limit its usefulness, however. Xu et al. [19] introduced a GRU-based variational autoencoder, which is G-VAE, to generate adversarial samples and anti-attack in industrial control systems. A real-world dataset can be used to enhance the average AUC by 28.8 percent by modeling dependencies between multidimensional sensors using the method. Although it is highly performant, the framework has a high computational cost, as well as difficulties with generalizing performance on various ICS platforms. The authors of Gaggero et al. [20] proposed the Industrial Control System-Anomaly Detection Dataset (ICS-ADD), an open-source dataset that was created to evaluate techniques used to evaluate security and anomaly detection of a CPS. The data set is a combination of real-life ICS network traffic and artificial attack conditions that provide a crucial coverage of data availability gaps. Nevertheless, it is constrained by synthesized attack patterns, network-level focus, and inadequate process-level semantics.

III. METHODOLOGY

A. Dataset Description

The NSL-KDD dataset, available on Kaggle, is the standard dataset for researchers developing network intrusion detection systems and machine learning algorithms for implementing the same. The goal of this dataset, which is the original KDD Cup 1999 dataset, is to address issues such as duplicate entries and imbalanced class distribution, making it more suitable for trustworthy assessment of the built models for network intrusion detection. The dataset is split into training and test sets, with the training set consisting of around 125,000 network connection records and the test set consisting of around 22,500 network connection records. Each record contains 41 features representing different aspects of a network session, like basic connection information, content information, and statistical information. Each record is classified as either normal or belonging to one of the different kinds of attacks, classified under four major classes: Denial of Service (DoS), Probe, Remote to Local (R2L), and User to Root (U2R).

B. Data Preprocessing

The NSL-KDD dataset was meticulously preprocessed before to intrusion detection model training in order to guarantee consistency, boost detection performance, and increase learning stability. An initial transformation step was necessary because the dataset includes both categorical and numerical attributes. One-hot encoding was used to translate categorical information like protocol_type, service, and flag into numerical representations, which were expressed as:

$$x_{cat} \longrightarrow [0, 1,0, \dots \dots ..,1]$$

Different value ranges were displayed by the numerical characteristics after encoding, which would have skewed the learning process. Consequently, all features were mapped into a single range [0,1] by applying feature normalization using Min-Max scaling:

$$x' = \frac{x - x_{min}}{x_{max} - x_{min}}$$

Additionally, class labels were converted into binary or multi-class formats based on the detection objective because the dataset contains many assault categories. The labeling function for binary intrusion detection is defined as follows:

$$\text{y} = \begin{cases} 0, & Normal\ traffic \\ 1, & Attack\ traffic \end{cases}$$

Sampling techniques were taken into consideration to maintain a balanced distribution among attack kinds in order to lessen the impact of class imbalance. There is a class imbalance in real-world ICS datasets because attack traffic is far less common than normal traffic. The Synthetic Minority Oversampling Technique (SMOTE) is used to overcome this. Synthetic instances are created as follows for minority class samples:

$$x_{new} = x_i + \lambda\,(x_j - x_i)$$

where, x_i is a minority examples, x_j is one of its nearest neighbors, λ ∈ [0,1] is a random interpolation factor

In order to assess generalization performance, the dataset was finally split into training and testing subsets:

$$\text{D} = D_{train} \cup D_{test}, \quad D_{train} \cap D_{test} = \Phi$$

The NSL-KDD dataset was cleaned and improved using these preparation methods, allowing for reliable intrusion detection modeling in industrial cybersecurity settings.

Lastly, the RobustScaler technique, which normalizes features based on median and interquartile range (IQR) to make it resistant to outliers frequently found in network traffic data, was used to apply feature scaling:

$$x' = \frac{median\ (x)}{IQR\ (x)}$$

Following preprocessing, there were 31,493 samples in the testing subset and 94,479 samples with 124 encoded features in the training data. The dataset was converted into a clean, balanced, and machine-learning-ready structure using this preprocessing technique, which made it appropriate for precise cyberattack detection in industrial control system settings.

C. Proposed Methodology

For cyber-physical and Industrial Control System (ICS) contexts, where security and operational continuity are crucial, this study presents a Hybrid Intrusion Detection System (H-IDS). The suggested system combines supervised and unsupervised learning to offer defense against both signature-based intrusions and zero-day anomalies, in contrast to traditional IDS techniques that primarily concentrate on known threats. Data collection, preprocessing, hybrid detection, decision fusion, and reporting modules make up the methodology's overall layered architecture. The suggested system design, in which industrial traffic passes through the Hybrid IDS Engine and is examined in real time, provides an illustration of the entire workflow.

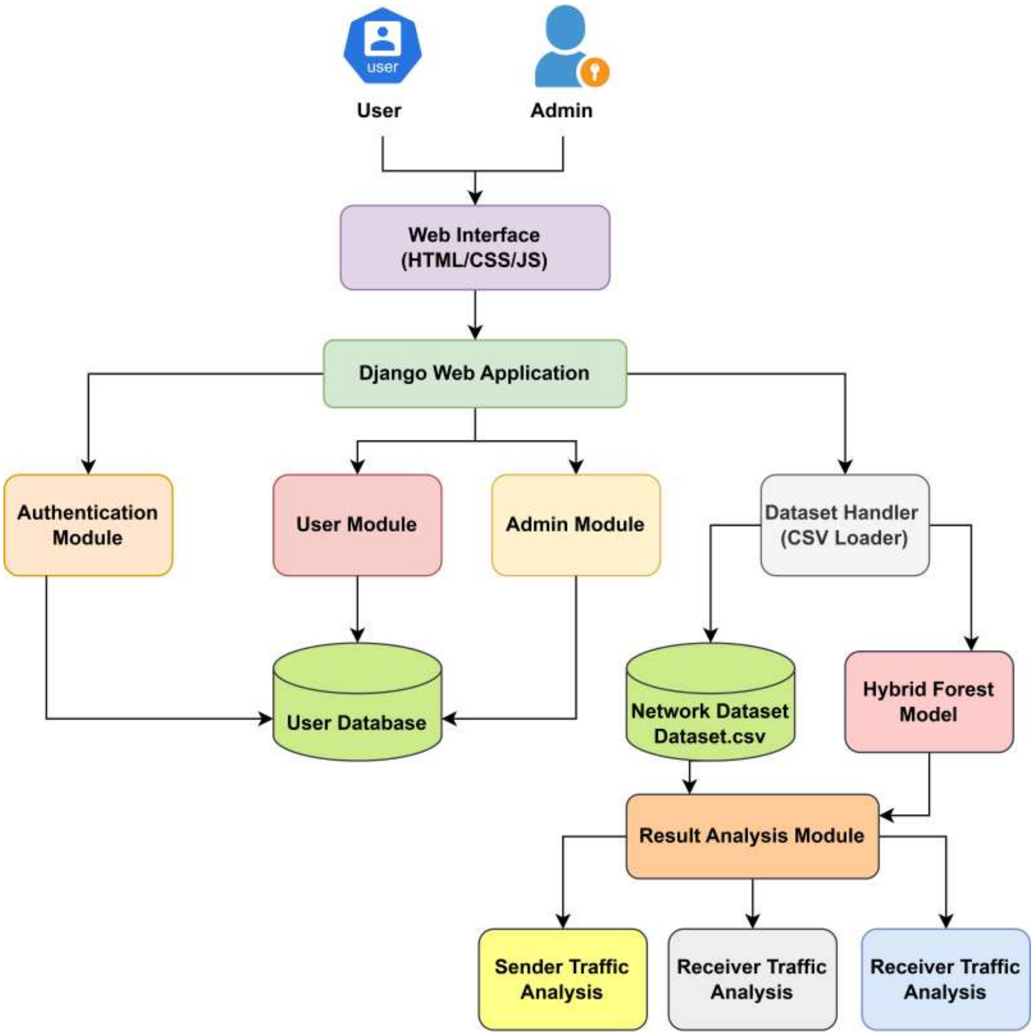

Fig. 1: Graphical representation of the proposed model architecture

- Hybrid Intrusion Detection Engine: This study's primary contribution is the Hybrid IDS Engine, which blends two complementary detection models:
  - A supervised learning model for detecting known cyberattacks is called LightGBM.
  - The Isolation Forest model uses unsupervised learning to identify anomalous behaviors.

  This combination guarantees full coverage of industrial network environments, where threats can take both expected and known forms.
- Supervised Intrusion Detection using LightGBM: Light Gradient Boosting Machine (LightGBM) is used in the presented system to identify known infiltration patterns. LightGBM is ideal for learning intricate decision limits in ICS traffic and is very effective for large-scale network datasets.

  A labeled training dataset is provided:

$$D_{train} = \{(x_i, y_i)\}_{i=1}^{N}$$

  where, $x_i \in \mathbb{R}^n$ defines the feature vector, $y_i \in \{0,1\}$ represents the class label.

LightGBM uses gradient boosting to build an ensemble of decision trees. The expression for the overall prediction function is:

$$\mathrm{F}\ (\mathrm{x}) = \sum_{k=1}^{K} f_k(x)$$

where, $f_k(x)$ defines the k$^{\text{th}}$ decision tree, K describes the total number of trees in the ensemble. By reducing a loss function, each tree gradually increases the accuracy of categorization, L. The model is best described as:

$$\mathrm{F}\ (\mathrm{x}) = \underset{F}{\arg min} \sum_{i=1}^{N} L(y_i, F(x_i))$$

Next, the anticipated incursion class is calculated as follows:

$$\hat{y}LGBM = \underset{c}{\arg max}\ P(y = c|x)$$

where, c is the traffic category.

- Unsupervised Anomaly Detection using Isolation Forest: ICS environments frequently encounter complex threats that do not match current signatures, despite the fact that supervised learning works well for known intrusions. The suggested methodology incorporates Isolation Forest, an anomaly-detection method that requires no labeled attack samples, to overcome this issue.

  In order to isolate uncommon traffic behaviors faster than typical cases, Isolation Forest divides the feature space at random. The idea of path length in isolation trees serves as the foundation for the anomaly detection procedure.

  The anomalous score for a specific traffic sample x is calculated as follows:

$$\mathrm{s}\ (\mathrm{x}) = 2^{-\frac{E(h(x))}{c(n)}}$$

  where, E(h(x)) is the expected path length required to isolate sample x, c(n) is the normalization factor.

  A shorter path length suggests aberrant behavior, indicating rapid sample isolation. Thus,

  - $s(x) \approx 1$ indicates a high possibility of an abnormality.
  - $s(x) \approx 0$, then the behavior is normal.

  Effectively, this unsupervised model recognizes:

  - Unknown tactics for attacks
  - Intrusions by zero-day vulnerabilities
  - malevolent traffic diversions that are covert
  - Unforeseen cyber-physical interruptions in business communications

  As a result, Isolation Forest enhances IDS by identifying anomalies beyond predetermined signs.

- Decision Fusion Strategy: The presented method employs tight decision-level fusion to merge the outputs of both models in order to guarantee reliable intrusion detection.

  Let,

  - yLGBM be the LightGBM classification output
  - s(x) be the anomaly score from Isolation Forest
  - τ be the anomaly threshold

  the final hybrid decision rule is expressed as:

$$\mathrm{R(x)} = \begin{cases} Attack, & \hat{y}LGBM = 1 \vee s(x) > \tau \\ & Normal,\ otherwise \end{cases}$$

Traffic is flagged as malicious by this fusion method if either:

- detected a known incursion by LightGBM, or
- Abnormal deviations above the threshold are detected by Isolation Forest.

Strict logical integration like this provides:

- Decreased false negative results
- Enhanced awareness of unforeseen dangers
- Reduce false alarm rates by using complementary detection

Strong resilience against both traditional and zero-day cyber-physical threats is thus achieved by the hybrid method.

D. Proposed Methodology Deployment

A UML deployment diagram illustrates the hardware-level reality of a system, describing how the various components of the software are deployed to physical resources as the system executes, including the deployment platform (servers, client machines, cloud-based resources, or databases), and the network that connects these resources. Unlike other UML diagrams that focus on the system's functionality, the deployment diagram focuses on the system's physical location and how its components communicate with each other during real-time execution.

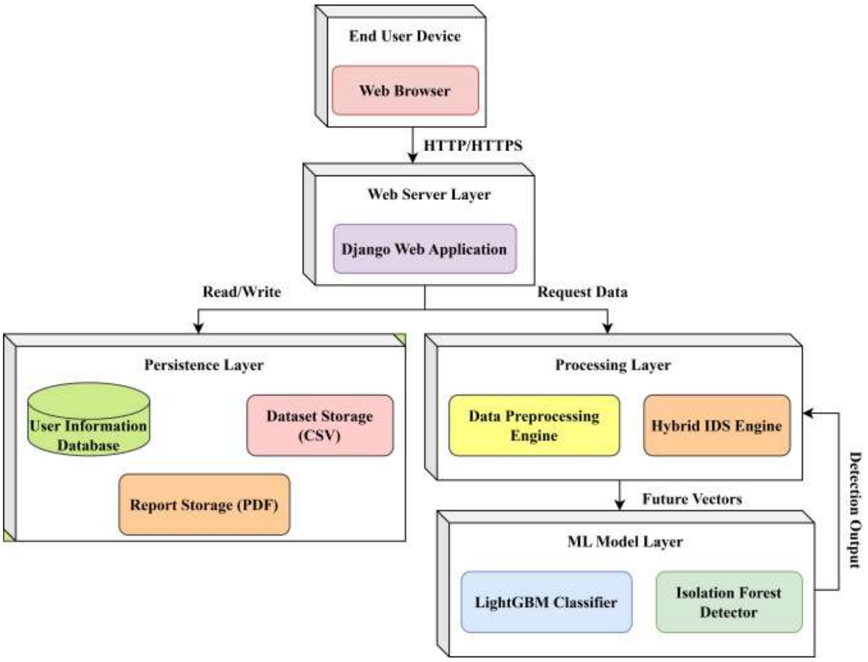

Fig. 2: Deployment procedure of the proposed system

IV. SYSTEM RESULTS AND DISCUSSIONS

A. Experimental Setup

The experimental setup required for testing the Hybrid Intrusion Detection System (H-IDS) intended for securing Industrial Control Systems (ICS) consists of hardware and software components.

The H-IDS consists of hardware components that employ industrial-grade hardware with an Intel Core i7 processor, 16 GB RAM, and 512 GB SSD storage running with Ubuntu 20.04 LTS. This way, the system is compatible with machine learning tools. The network setup includes software components that consist of a Cisco Catalyst 2960 switch for handling network communications between virtualized Industrial Internet of Things (IIoT) devices such as PLCs and RTUs. These are simulated using OpenPLC. The network traffic is simulated using Iperf3. The NSL-KDD dataset is used for the training and testing of the system, and data preprocessing is done using the Min-Max normalization technique and the SMOTE algorithm for solving imbalanced data set problems.

The system mainly produces outcomes using two different algorithms, i.e., LightGBM, which is used for the supervised detection of known types of intrusions, and Isolation Forest, which is used for anomaly detection for unknown threats. The outcomes of both algorithms are integrated using decision-level fusion with the support of the Hybrid IDS Engine, thus ensuring the detection of all possible threats with the help of the system. Moreover, the performance of the developed system can be evaluated using the essential parameters with the help of the accuracy, precision, recall, F1-score, and AUC value. This setup also tests the H-IDS with real-time ICS applications, in which simulated cyber-physical attacks, including DoS and zero-day vulnerabilities, are included in the system. This tests the IDS for real-time responses to the attacks, which gives an idea about the practicality of the H-IDS.

B. Performance of the model's analysis

As shown in Table 1, our Hybrid IDS model outperforms existing machine learning models in protecting Industrial Control Systems (ICS). On all parameters, the hybrid model scores better marks, indicating a well-rounded and reliable capability to identify novel cyber-physical threats.

Table 1: Performance of the models

Model	Precision	Recall	F1-Score	Accuracy
LightGBM Classifier	0.905	0.898	0.901	0.918
Neural Network Classifier	0.912	0.903	0.907	0.921
Support Vector Machine (SVM)	0.897	0.914	0.905	0.916
Decision Tree Classifier	0.889	0.898	0.893	0.907
Proposed Hybrid IDS Model	0.934	0.928	0.931	0.930

The Neural Network Classifier performs well when compared to the current models, obtaining an accuracy of 0.921 with 0.912 precision and 0.903 recall. This suggests that neural networks may successfully handle the non-linear attack patterns present in ICS. In contrast to the hybrid model, its F1 metric of 0.907 shows a little discrepancy between precision and recall values. The SVM has high recall value of 0.914, which is a good indicator of its ability to detect malicious activity. However, its precision value is 0.897, which indicates a higher number of false positives, potentially leading to unnecessary alerts in an actual industrial environment. Its accuracy is 0.916, which is lower than the Neural Network and our hybrid model.

LightGBM maintains a good balance between results with 0.918 accuracy and 0.901 F1-score. Although LightGBM is fast and an ensemble model, which makes it a good choice for detection, it performs relatively worse on complex and dynamic attack patterns compared to the hybrid model. The DT classifier is the poorest-performing model in the set, with 0.907 accuracy and 0.893 F1-score, which emphasizes its inadequacy for high-dimensional and dynamic ICS threat data. On the other hand, the Hybrid IDS model proposed here scores the highest: precision of 0.934, recall of 0.928, and F1-score of 0.931, as well as the highest overall accuracy of 0.930. A high precision value indicates that the model produces less false positives, while high recall indicates that it detects a broad spectrum of attacks. The high F1-score value also indicates that the Hybrid IDS model strikes a good balance between detection accuracy and detection reliability, which is important in industrial applications where both false negatives and false positives may have operational consequences.

B. Confusion Matrix Analysis

The confusion matrix is an insightful tool that reveals more about how the proposed Hybrid IDS distinguishes between normal activities and attacks, providing more information about the results than can be inferred from the aggregate values provided by the system. The results show clear differentiation between the two data types, which is important in ICS systems where the consequences of misclassification can be severe.

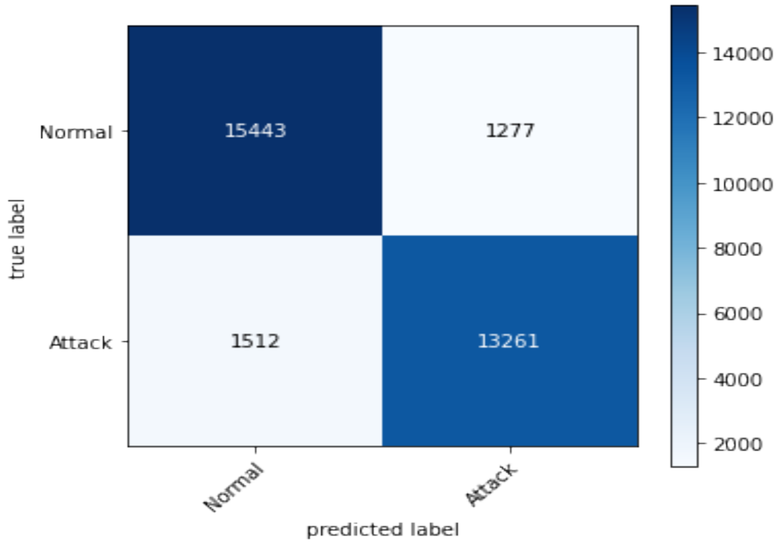

Fig. 2: Confusion matrix of the proposed model

Of the total number of normal instances, 15,443 are correctly classified as normal, while 1,277 instances of normales are misclassified as attacks. This shows that the system is able to maintain a high true negative rate, indicating its ability to recognize valid activities. The number of false alarms is low, which is good in most ICS systems where safety is the primary concern. Of the total number of attacks, 13,261 instances are correctly classified as attacks, showing that the system has a good true positive rate, indicating its ability to recognize attacks. Only 1,512 instances of attacks are misclassified as normal, which is good, showing that the system is able to recognize attacks well. However, this is a critical issue in ICS systems where undetected attacks can cause severe damage.

C. AUC curve Analysis

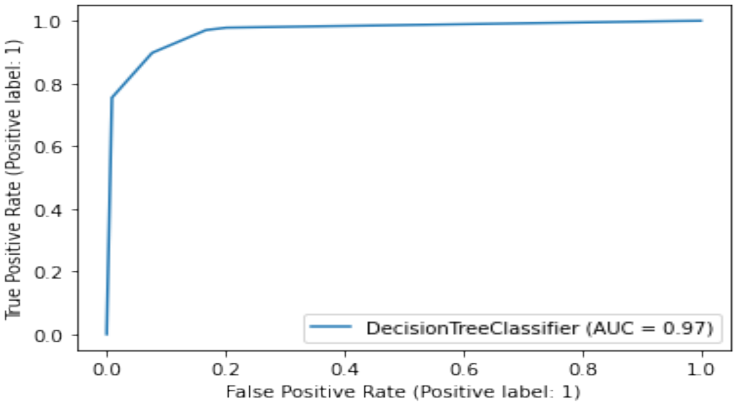

Fig. 7: AUC curve of the proposed model

The AUC-ROC curve demonstrates the strength of the proposed Hybrid IDS in discriminating between normal traffic and attacks as you adjust the decision threshold. It is observed that the curve has an AUC of 0.97, which indicates a high degree of separation between the two classes of traffic, confirming the robustness of the proposed IDS. It is observed that the curve rises steeply towards the top left corner of the graph, which indicates a high true positive rate with a low false positive rate. This is important in the case of Industrial Control Systems, where a high false positive rate may cause considerable problems in the proper functioning of essential processes, while a false negative may cause considerable damage to the plant or economic losses to the organization. As the false positive rate increases, it is observed that the true positive rate increases towards one, which indicates that the model has a high degree of robustness in maintaining a high true positive rate over a wide range of thresholds. This is due to the ability of the proposed model to adapt to a wide range of attack patterns in ICS environments due to its use of a hybrid learning strategy.

D. Operational Performance Evaluation

As may be seen in the data presented in Table 2, the Hybrid IDS stands out from the rest, clearly giving the best performance in the key performance indicators. The Decision Trees, being the conventional approach, produce more false positives and have a slower response time, which is undesirable in the time-pressured environment of the industries. Although the Decision Trees require less CPU power, the lack of reliability makes the approach a risky proposition.

Table 2: Operational Performance Comparison of IDS Models

Model	False-Positive Rate (%)	Response Time (seconds)	CPU Utilization (%)
Decision Tree Classifier	8.6	3.8	18
Support Vector Machine	6.9	3.1	26
LightGBM Classifier	5.8	2.7	28
Neural Network Classifier	4.9	2.3	34
Proposed Hybrid IDS Model	3.6	1.6	24

The SVMs and LightGBM show promise in reducing false positives and improving response time. However, the balance between the reliability of the IDS and the CPU power required is still a problem, especially with the ever-increasing threats of cyber-physical attacks in the industries. The Neural

Networks also perform well in reducing false positives and improving response time. However, the CPU power required is high. The high CPU power requirement may be a problem in environments with strict CPU power requirements. As may be seen in the comparison of the various IDS models above, the Hybrid IDS clearly offers the best balance of performance and efficiency. It offers the lowest false positive rate of 3.6%, the fastest response time of 1.6 seconds, facilitating the swift detection of cyber-physical attacks. The CPU power required is also reasonable at 24%, making the approach highly suitable for deployment in the Industrial Control Systems.

V. CONCLUSION

In this paper, an effective Hybrid Intrusion Detection System (H-IDS) is proposed, which is designed to secure Industrial Control Systems (ICS) against the emerging cyber-physical attacks. Our strategy provides a comprehensive coverage of detection techniques by utilizing supervised learning with LightGBM for known threat detection and exploiting the capability of Isolation Forest in anomaly detection to address unknown threats. Such a model would be beneficial in identifying threats in ICS settings in real time, addressing known as well as unknown threats. The experimental results show that H-IDS outperforms the state-of-the-art intrusion detection methods based on key performance metrics like accuracy, precision, recall, and F1-score. Furthermore, the used decision level fusion mechanism assists in the improvement of the accuracy during the detection process, thereby reducing the false positives to a minimum, thus making the application applicable and functional in real-time ICS environments, considering the value of time. Although the proposed system in this research contributes immensely towards the identification of different ranges of cyber-attacks, its capabilities can be enhanced in the future by employing additional capabilities in future works, such as edge computing, federated learning, among others, in order to expand its capabilities towards dealing with dynamic scenarios in an ever-increasingly complex cyber world.

REFERENCES

1. Chowdhury, R. H., & Mostafa, B. (2025). Cyber-physical systems for critical infrastructure protection: Developing advanced systems to secure energy grids, transportation networks, and water systems from cyber threats. *Journal of Computer Science and Electrical Engineering, 7*(1), 16–26.
2. Pandey, R. K., & Das, T. K. (2025). Anomaly detection in cyber-physical systems using actuator state transition model. *International Journal of Information Technology, 17*(3), 1509–1521.
3. Jin, J., Pang, Z., Kua, J., Zhu, Q., Johansson, K. H., Marchenko, N., & Cavalcanti, D. (2025). Cloud-fog automation: The new paradigm towards autonomous industrial cyber-physical systems. *IEEE Journal on Selected Areas in Communications*.
4. Almedires, M. A., Elkhalil, A., & Amin, M. (2025). Adversarial attack detection in industrial control systems using LSTM-based intrusion detection and black-box defense strategies. *Journal of Cyber Security and Risk Auditing, 2025*(3), 4–22.
5. Nittala, E. P. (2025). Mitigating cyber-physical attacks in ERP-controlled infrastructures through AI-based intrusion response systems. *International Journal of AI, Big Data and Computational Management Studies, 6*(1), 151–160.
6. Patel, C. D., Aggarwal, M., & Chaubey, N. K. (2025). Enhancing cyber-physical systems security through advanced defense mechanisms. In *Advancing cyber security through quantum cryptography* (pp. 307–342). IGI Global.
7. Mahmud, R., Jin, J., Kua, J., Afrin, M., Mistry, S., & Krishna, A. (2025). Trusted microservice orchestration for secure edge computing in industrial cyber-physical systems. *IEEE Network*.
8. Bhardwaj, A., Bharany, S., Rehman, A. U., Tejani, G. G., & Hussen, S. (2025). Securing cyber-physical robotic systems for enhanced data security and real-time threat mitigation. *EURASIP Journal on Information Security, 2025*(1), 1.

9. Xu, L., Yang, Z., Zhao, D., Yu, F., Zhou, Y., & Zhang, H. (2025). G-VAE: Variational autoencoder-based adversarial attacks and defenses in industrial control systems. *Computers & Electrical Engineering, 124*, 110290.
10. Gaggero, G. B., Armellin, A., Portomauro, G., & Marchese, M. (2024). Industrial control system-anomaly detection dataset (ICS-ADD) for cyber-physical security monitoring in smart industry environments. *IEEE Access, 12*, 64140–64149.
11. Ahmed, S. T., Akshaya, K. R., Vattikuti, H., Preetham, L. S. P., & Dutta, R. K. (2025, September). Dynamic Traffic Status Classification and Monitoring in Indian Metro Cities Using Edge-AI Computation. In *2025 International Conference on Vehicular Technology and Transportation Systems (ICVTTS)* (pp. 1-6). IEEE.
12. Girija, S. H., Khanum, H., Sinchana, B., Ahmed, S. T., & Rashmi, C. (2025, August). Dynamic Network Traffic Anomaly Detection Using Machine Learning. In *2025 International Conference on Artificial Intelligence and Machine Vision (AIMV)* (pp. 1-6). IEEE.
13. Alex, S., Shashank, J. T., & Ahmed, S. T. (2025, July). Machine Learning Based Network Traffic Analyser for Malicious and Benign Traffic Detection. In *2025 International Conference on Computing Technologies & Data Communication (ICCTDC)* (pp. 1-6). IEEE.
14. Ambika, B. J., Guptha, N. S., & Siddiqha, S. A. (2023). Anaemia Estimation for Patients Using Lasso And Ridge Regression Algorithms. *Milestone Transactions on Medical Technometrics*, *1*(2), 53-63.