International Journal on Computational Modelling Applications
Vol. 03, Iss. 01, S. No. 04, pp. 42--53, March 2026
ISSN (Online): 3048-8516

Received: 08 May 2026, Accepted: 04 August 2026, Published: 11 August 2026

Digital Object Identifier: https://doi.org/10.63503/j.ijcma.2026.258

Research Article

Deep Learning–Based Network Anomaly Detection in Cyber-Physical Systems Using Edge Hardware and Cloud Intelligence

Nguyen Gia Nhu (https://orcid.org/0000-0003-4267-3900), Dang Ngoc Cuong (https://orcid.org/0009-0007-4780-2237), Ho Duc Dung (https://orcid.org/0009-0004-0058-6686), Vo Tuan Anh (https://orcid.org/0009-0006-2823-2921)

Duy Tan University, Danang, Vietnam

nguyengianhu@duytan.edu.vn, dangngoccuong@duytan.edu.vn, hoducdung@dtu.edu.vn, votuananh4@dtu.edu.vn

*Corresponding author: Dang Ngoc Cuong, dangngoccuong@duytan.edu.vn

ABSTRACT

Modern network infrastructures have become highly vulnerable due to the rapid development of cyber-physical systems (CPS). This is because the constant creation of high-volume, high-velocity data streams requires real-time anomaly detection, which is highly computationally intensive and latency-sensitive. Although recent studies have explored deep learning and edge computing separately for anomaly detection, few studies have jointly integrated edge inference with cloud intelligence in a unified adaptive framework for CPS. Existing approaches generally suffer from one or more limitations, including high inference latency, high computational cost, insufficient scalability, or inability to continuously update deployed models. Therefore, there remains a need for an integrated architecture capable of providing accurate, scalable, and low-latency anomaly detection. In this paper, a solid anomaly detection framework is proposed that uses deep learning, integrating edge computing and cloud intelligence to enable efficient, scalable, and adaptable threat detection. The suggested system will include a structured pipeline that involves data acquisition, preprocessing, feature extraction, anomaly prediction, and adaptive feedback optimization. Low-latency inference can be achieved with edge nodes, while cloud resources can be used for computationally intensive training and model refinement. Experimental analysis shows that the suggested approach achieves 93.6% detection accuracy, 90.2% efficiency, 182 ms latency, a stability index of 0.89, and a total performance index of 0.91. The findings confirm the usefulness of the hybrid edge-cloud paradigm in enhancing the accuracy of detection, minimal response time, and high system resilience and CPS settings.

Keywords: *Deep Learning, Cyber-Physical Systems, Network Anomaly Detection, Edge Computing, Cloud Intelligence, Cybersecurity*

1 Introduction and Research Background

Cyber-physical systems (CPS) constitute an intimate level of combination of a more closely networked level. This is achieved by using computational smarts, communication systems, and bodily operations. Complicated monitoring, automation, and control of areas where sophistication is needed, such as automation in industrial use, smart grids, and electronic healthcare. Although this integration greatly contributes to the effectiveness of operations, system intelligence, and real-time responsiveness, it also increases the attack surface, making CPS infrastructures more susceptible to advanced and emerging cyberattacks [1], [2].

The inherent nature of CPS, which is real-time functionality, a distributed architecture of the system, and heterogeneous data generation, provides significant limitations to traditional mechanisms of anomaly detection. The methods traditionally used, which are mostly rule- or signature-based, are inflexible and simply unable to detect previously unknown or newly

developed attack patterns. Besides, the scalability of network traffic volume and complexity has been increasing exponentially, creating strong scalability limits with evidence of higher detection latency, higher rates of false positives, and deterioration in system reliability and resiliency in general [3], [4].

Recent progress in deep learning has proven incredibly efficient, as it enables the study of complex, nonlinear relationships implied by network traffic data. These models make it easy to automatically extract hierarchical and discriminative feature representations, hence enhancing detection performance and plasticity in dynamic settings. However, the real-world application of deep learning methods to CPS has been hampered by their high computational complexity and power consumption, and they are not always applicable to low-resource edge devices, limiting their use in real-time applications in distributed CPS systems [5], [6].

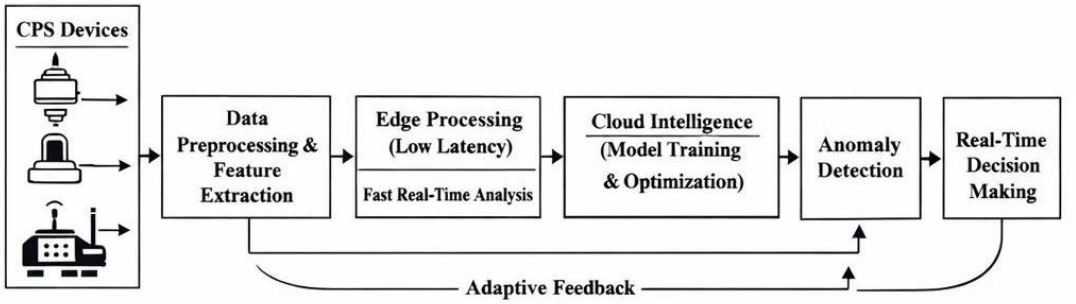

Fig.1. Graphical Abstract of the Proposed Framework**.**

Fig. 1 shows the topology of the entire proposed process of anomaly detection with deep learning based on a network of cyber-physical systems (CPS), and it represents a full picture of the end-to-end data transport of the system. It also emphasises the continuous acquisition and transformation of the network traffic data with the help of preprocessing and feature extraction, and then through deep learning analysis to detect the anomalies. The framework also illustrates that real-time decision-making can be based on an adaptive feedback mechanism, which will allow one to continually improve detection performance. An important feature of the architecture entails the combination of edge computing and cloud intelligence, where edge devices support any low-latency and real-time inference, whereas cloud platforms support high scalability of computing resources to train and optimize models. The building is a mixing combination. design that is meant to ensure a proficient process of extensive network data and coupled with a prompt response to the information of the network. In general, the system supports continuous monitoring and reaction in advance so that it is possible to adapt to the changes and emergent cyber threats in the dynamic network environment.

2 Related Research on AI Governance and Cybersecurity Compliance

Traditional anomaly-based intrusion detection systems mostly rely on rule- or signature-based approaches, which are inflexible and cannot detect new or evolving threats in dynamic cyber-physical systems (CPS) environments, thereby complicating their management [7], [8]. Moreover, these traditional methods are not suitable for receiving large and fast data streams and addressing real-time processing needs. They are also restricted to scales of constant updates to be effective in resisting new attack vectors and therefore do not scale well, which is a limitation to their usefulness.

The techniques based on machine learning have also enhanced the problem of anomaly detection as it provides the capability of detecting abnormal behavior early, which allows it to be analyzed in a predictive fashion. However, there is the risk that they might be implemented at the price of high compute cost, increased power consumption, and an overall deterioration

of the system. performance [9], [10]. Additionally, there is one more disadvantage: the issues of dependence on labels. It lacks data, has low scalability, and shows limited generalisation to real-life CPS settings, which limits their ability to handle a multiplicity of varied and variable situations.

In order to overcome the weaknesses, there have been advanced proposals of hybrid architectures. Hybridising techniques of network perceptive learning on the boundary and computational support of the cloud. Such systems have the capability to enhance the work of detection both by low-latency processing at the edge, coupled with the application of the cloud to provide large-scale model training and optimisation. Along with these benefits, these strategies come with other challenges, such as resource, complexity, and overheads of systems, which need an effective design and integration strategy to succeed in achieving a practical and scalable implementation [11–15].

Table 1 presents a comparative analysis of existing anomaly detection approaches in cyber-physical systems (CPS), highlighting their key characteristics and limitations. The comparison emphasises the need for an integrated deep learning–based edge-cloud framework to improve scalability, accuracy and real-time performance.

Table 1: Comparison of Existing Anomaly Detection Approaches

Framework Type	Core Focus	Key Limitation	Reference
Rule-based systems	Signature-based detection	Low adaptability	[7]
Cloud-based analytics	Centralized processing	High latency	[8]
ML-based detection	Pattern classification	Limited scalability	[9]
Deep learning models	Complex feature learning	High computational cost	[10]
Edge-based detection	Local real-time processing	Resource constraints	[11]
Distributed systems	Parallel anomaly detection	Network dependency	[12]
Hybrid ML-edge models	Combined efficiency and speed	System complexity	[13]
IoT-based security	Sensor-level anomaly detection	Data heterogeneity	[14]
Intelligent CPS models	Adaptive threat detection	Implementation complexity	[15]

3 Problem Statement & Research Objectives

The cyber-physical system (CPS) networks are becoming progressively more complex, and the high-volume generation of real-time traffic leads to significant load on processing requirements and response time. Large data loads reduce analysis speed and introduce delays, which can hinder timely identification of abnormal behaviour. Most of the current strategies do not suffice because they are unable to provide accuracy as they adapt to the needs of speed and scalability.

This decreases the level of system trust since it is not detected on time. Moreover, new forms of attacks are bound to arise and evolve, and the old style of dealing with threats is no longer effective at managing the dynamic, shifting threat landscape. Learning mechanisms become a must in such a situation. The systems should be in a position to adjust in a fast way and recognise irregularities in a precise way, even in circumstances that are constantly evolving.

Research Objectives:

- To develop a deep learning–based anomaly detection framework for CPS
- To efficiently analyse network traffic data in real time
- To design adaptive detection mechanisms using edge-cloud integration
- To improve detection accuracy, reduce latency, and enhance system stability

4 Proposed Methodology

It is implemented by first applying deep learning to edge devices together with cloud intelligence in identifying anomalies in the CPS networks. In the first stages, the network data is continuously gathered, and then it is preprocessed to draw meaningful features. The data are then subjected to neural network-based models in order to identify abnormalities in the network. Edge-based local processing makes processing faster and greatly shortens delays. Simultaneously, model training, optimisation, and scalability improvement workload and other computationally intensive tasks are addressed by cloud services. It functions in a dynamically changing network environment without having to reconfigure it manually. New information is added at any time, and model parameters are adjusted gradually based on observed anomalies. In case irregular patterns are identified, correction is done to enhance better detection over time. This is a constant and reactive process of learning that enables the system to adapt appropriately to changing cyber threats within the CPS environments.

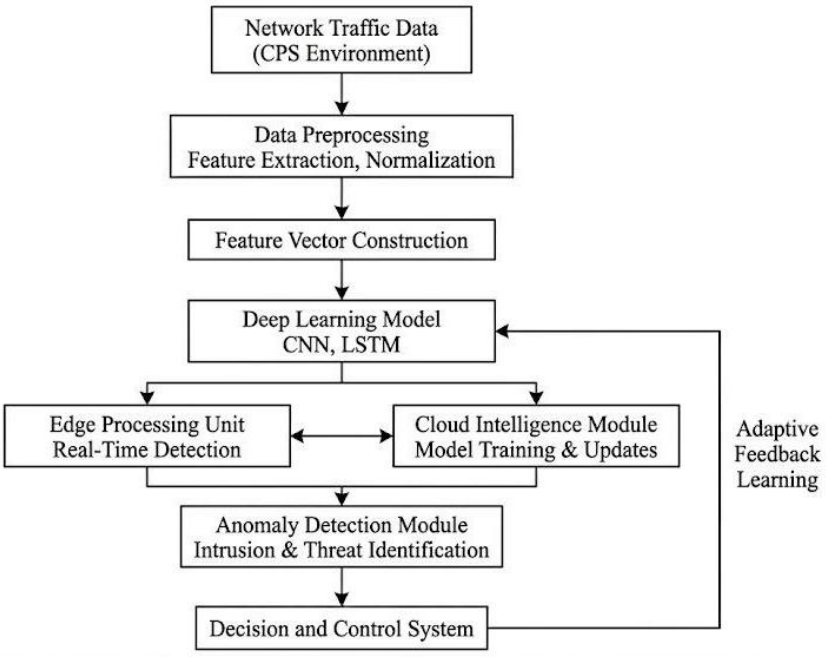

Fig.2. Architecture of the Proposed Framework

Fig. 2 shows the model of the proposed deep learning–based network anomaly detection system in cyber-physical systems. It illustrates the sequence of data preprocessing and feature

extraction, followed by deep learning–based analysis, along with edge and cloud processing for real-time detection and model optimisation. The architecture emphasises parallel processing and incorporates an adaptive feedback mechanism to ensure efficient and scalable anomaly detection.

This equation is an embodiment of the conversion of raw data from network traffic into structured features. Vectors are applied in detecting anomalies, as indicated in the equation below. (1).

$$S = f(D) \quad (1)$$

Where S is the feature vector, D is the network dataset, and $f(\cdot)$ is the feature extraction function.

This equation defines how the deep learning model generates anomaly predictions from extracted features, as shown in Eq. (2).

$$P = DL(S) \quad (2)$$

Where P is the prediction output, DL is the deep learning model, and S is the feature vector.

This equation calculates the error between actual and predicted outputs for model optimization, as shown in Eq. (3).

$$L = | y_{actual} - y_{predicted} | \quad (3)$$

Where L is the loss value, y_{actual} is the actual label, and $y_{predicted}$ is the predicted output.

This equation ensures that system constraints are satisfied during anomaly detection, as shown in Eq. (4).

$$C = \sum_{i=1}^{n} C_i \quad (4)$$

Where C is the constraint score and c_i represents individual constraint parameters.

This equation evaluates system risk based on network load and variations, as shown in Eq. (5).

$$R = f(l, v) \quad (5)$$

Where R is the risk value, l is the network load, and v is a variation in traffic conditions.

This equation measures the deviation between prediction loss and system constraints, as shown in Eq. (6).

$$D = | L - C | \quad (6)$$

Where D is the deviation, L is a loss value, and C is the constraint score.

This equation computes system efficiency based on prediction performance, as shown in Eq. (7).

$$Eff = f(P, L) \quad (7)$$

Where Eff is system efficiency, P is the prediction output, and L is a loss value.

This equation evaluates overall system performance by combining multiple factors, as shown in Eq. (8).

$$PI = w_1 C + w_2 Eff - w_3 R \quad (8)$$

Where PI is the performance index, C is the constraint score, Eff is efficiency, R is risk and w_1, w_2, w_3 are weighting coefficients.

Algorithm 1: Deep Learning-Based Anomaly Detection

Input**:** Network dataset D, system parameters
Output**:** Predictions P, performance metrics (Acc, Eff, Latency, PI)

1. Acquire network data $D \triangleleft$ Collect raw traffic data from CPS networks
2. Extract features: $S \leftarrow f(D) \triangleleft$ Eq. (1): construct feature vector
3. Generate prediction: $P \leftarrow DL(S) \triangleleft$ Eq. (2): apply deep learning model
4. Compute prediction loss: $L \leftarrow \mid y_{actual} - y_{predicted} \mid \triangleleft$ Eq. (3)
5. Evaluate system constraints: $C \leftarrow \sum c_i \triangleleft$ Eq. (4)
6. Calculate system risk: $R \leftarrow f(l, v) \triangleleft$ Eq. (5): evaluate network load and variation
7. Determine deviation: $D \leftarrow L - C \triangleleft$ Eq. (6): loss minus constraint score
8. Compute system efficiency: $Eff \leftarrow \frac{Correct\ Predictions}{Total\ Predictions} \triangleleft$ Eq. (7)
9. Calculate performance index: $PI \leftarrow w_1 C + w_2 Eff - w_3 R \triangleleft$ Eq. (8)
10. Update system parameters and optimize decisions $\triangleleft$ adaptive feedback loop

5 Experimental Setup

Performance is measured by the effectiveness of the proposed system in live cyber-physical networks, where the system's ability to detect anomalous events, response speed, and stability are key factors. Variable traffic loads are used to recreate realistic conditions rather than by using fixed settings, and varying attack scenarios are also used in combination with the traffic loads. They utilise a dataset of about 10,000 traffic records, including data packet size, session time, communication protocols, and link conditions. The data is first normalised, useful features are obtained, and noise is eliminated, and the data is then divided into training and validation. The results of the training process in terms of accuracy, cost of processing, latency, and behaviour patterns are realised and monitored in a changing environment. Moreover, abnormal events such as intrusion attempts or sudden changes, such as spikes in network traffic, are included in the tests to assess how effectively the system detects abnormalities in a realistic, dynamic environment.

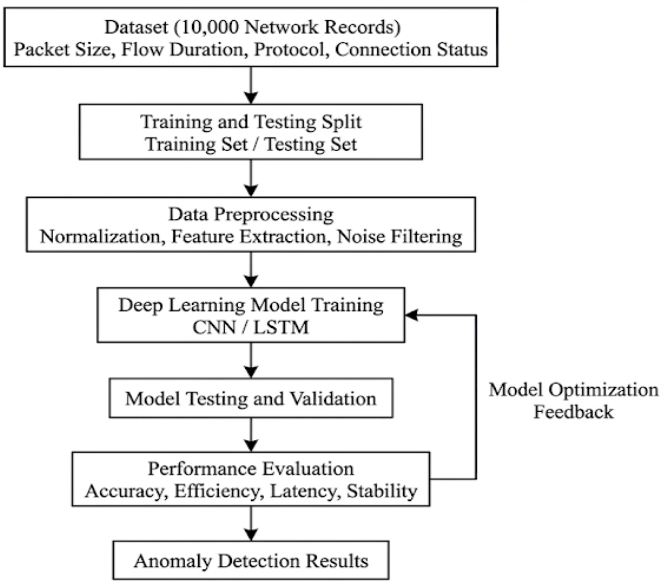

Fig.3. Experimental Setup of the Proposed Framework

Fig. 3 illustrates the experimental setup used to evaluate the proposed deep learning–based anomaly detection system. It presents the process from dataset preparation and preprocessing to model training, testing, and performance evaluation, along with a feedback mechanism for optimization. The setup ensures proper validation through distinct training and testing phases and evaluates system performance under varying network conditions.

6 Dataset

The dataset used to analyse the suggested deep learning-based anomaly detection system is a standard benchmark intrusion detection dataset, comprising both normal and malicious network traffic [16], [17]. These datasets provide a wide variety of features, including packet sizes, flow durations, protocol types, and connection states, and enable detailed study of network activity. Such benchmark datasets are used to ensure that performance is properly assessed and can be compared with existing practices in a realistic cyber-physical system (CPS) environment.

Table 2 presents the experimental tasks and corresponding modules used to evaluate the proposed deep learning–based anomaly detection framework. It outlines the functional components, expected outputs, and dataset size considered for performance analysis in cyber-physical systems.

Table 2: Experimental Tasks and Evaluation Metrics

Experimental Task	Module Used	Output Result	Dataset Size
Network Monitoring	Data acquisition module	Real-time traffic data	10,000
Data Preprocessing	Preprocessing unit	Cleaned feature dataset	10,000
DL Processing	Deep learning engine	Detection accuracy (%)	10,000
Anomaly Detection	DL model	Intrusion and anomaly alerts	10,000
Performance Evaluation	Evaluation module	Efficiency, latency, stability	10,000

7 Results and Performance Evaluation

The proposed system is compared with existing traditional and machine-learning-based hybrid systems, beginning with an introduction to the project, with the major metrics being accuracy, speed, response time, reliability, and overall system performance. The findings indicate a significant increase in the results of the integration of deep learning and edge-to-cloud processing. Detection of anomalies is improved with lower consumption of computational resources and processing delay. The system can be adaptive in real-time cyberspace and physical environments, as it can operate under a range of network conditions in a stable manner.

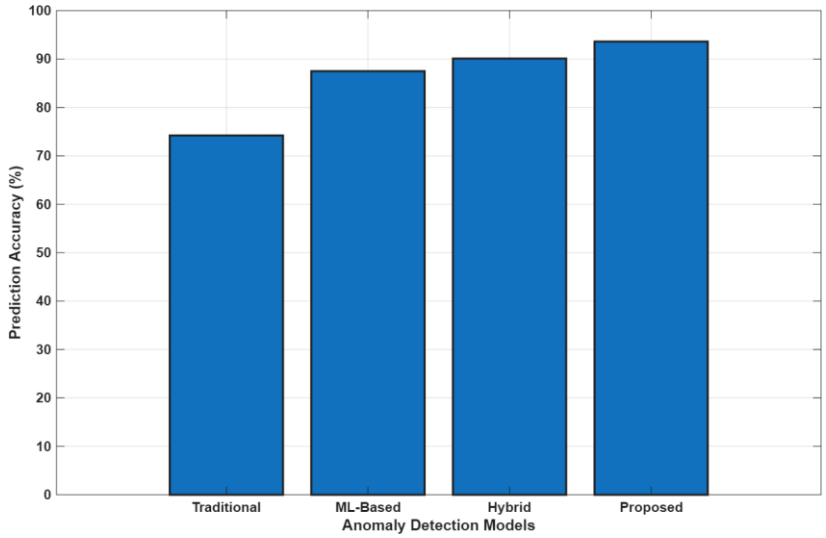

Fig.4. Accuracy Comparison of Different Models

Fig. 4 presents the comparison of prediction accuracy among different models. The proposed deep learning-based architecture achieves the highest accuracy, 93.6%, compared with other approaches. The performance of traditional (74.2%), ML-based (87.5%), and hybrid (90.1%) models is also indicated for comparison. This improvement highlights the effectiveness of deep learning in capturing complex network patterns for anomaly detection.

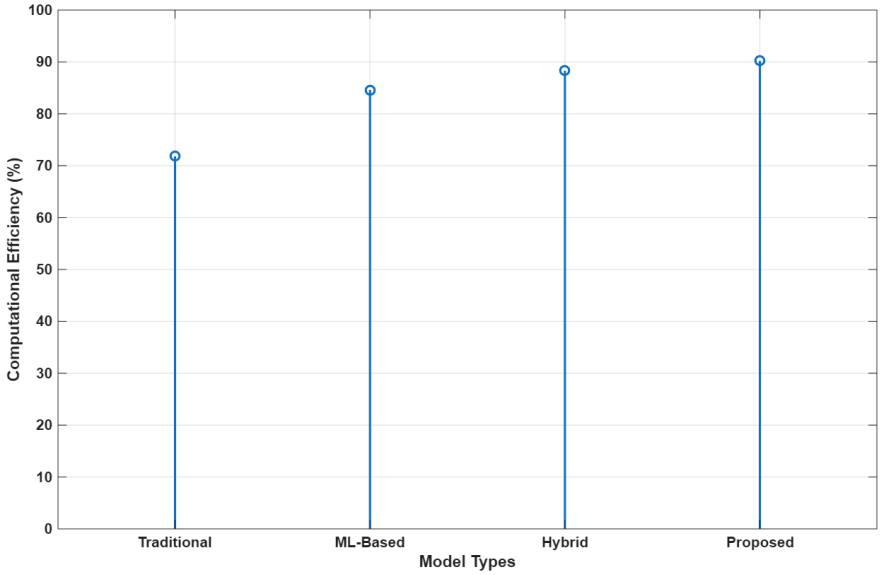

Fig.5. Efficiency Comparison of Different Models

Fig. 5 presents the efficiency comparison of different models. The proposed system is able to attain an efficiency of 90.2%, which is higher than traditional (71.8%), ML-based (84.6%), and hybrid (88.3%) models. This enhancement means there is more optimised processing, which has reduced the computational cost of the proposed form.

Table 3 presents a comparative study of traditional, ML-based, hybrid and proposed models using key performance metrics such as accuracy, efficiency, latency, stability and performance index. The results indicate the effectiveness of the proposed deep learning system in enhancing overall system performance.

Table 3: Performance Comparison of Different Models

Model	Accuracy (%)	Efficiency (%)	Latency (ms)	Stability	Performance Index
Traditional	74.2	71.8	330	0.66	0.70
ML-Based	87.5	84.6	250	0.80	0.81
Hybrid	90.1	88.3	215	0.84	0.86
Proposed	93.6	90.2	182	0.89	0.91

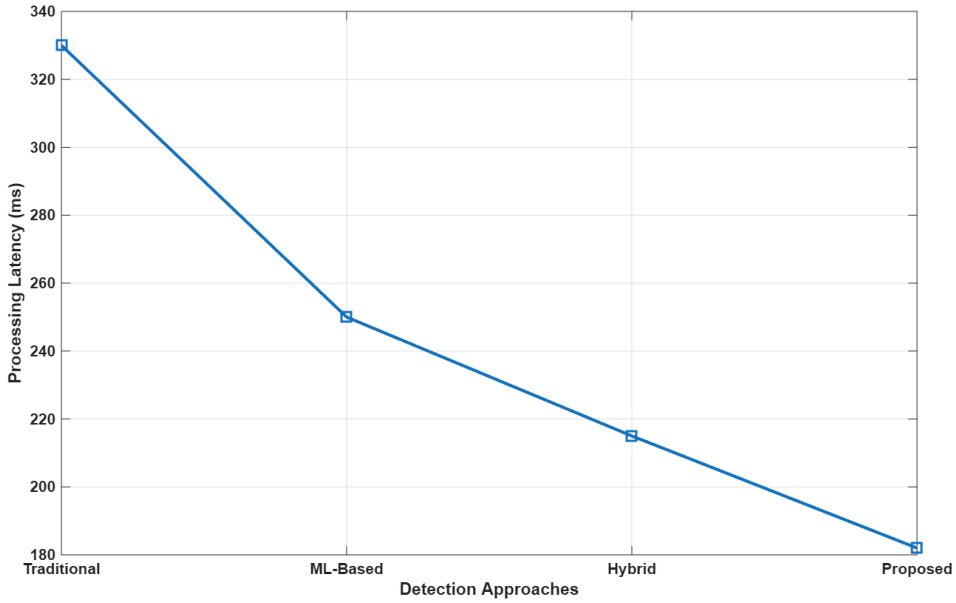

Fig.6. Latency Analysis of Different Models

Fig. 6 shows the latency comparison of various models. The designed framework will be minimised. Latency of 182ms versus 330ms of traditional models, ML and hybrid models, which log the latter. The time of 250ms and 215ms, respectively, which allows detection in real-time. This cut is such that there is a guarantee that CPS contains network anomalies that are spotted and resolved speedily.

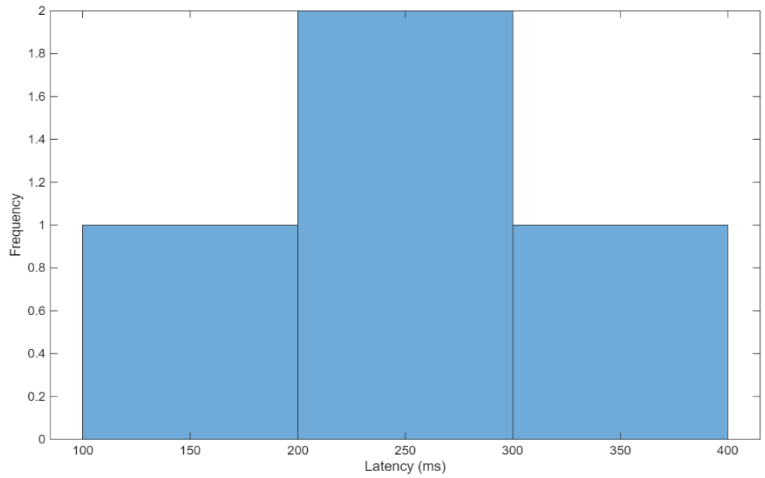

Fig.7. Stability Analysis of Different Models

Fig. 7 presents the stability comparison under varying conditions. The proposed model achieves a stability value of 0.89, which is higher than traditional (0.66), ML-based (0.80), and hybrid (0.84) models, ensuring consistent system performance. This improvement reflects enhanced robustness under dynamic and uncertain network conditions.

Table 4 gives a comparative study between the stability of the systems, the latency at which the system can compute, and the data processing capability between the various models. It shows how effective the proposal can be designed in ensuring that latency is reduced and processing efficiency is enhanced.

Table 4: Efficiency and Latency Comparison

Model	Stability	Latency (ms)	Data Processing Level
Traditional	0.66	330	Low
ML-Based	0.80	250	Medium
Hybrid	0.84	215	Medium
Proposed	0.89	182	High

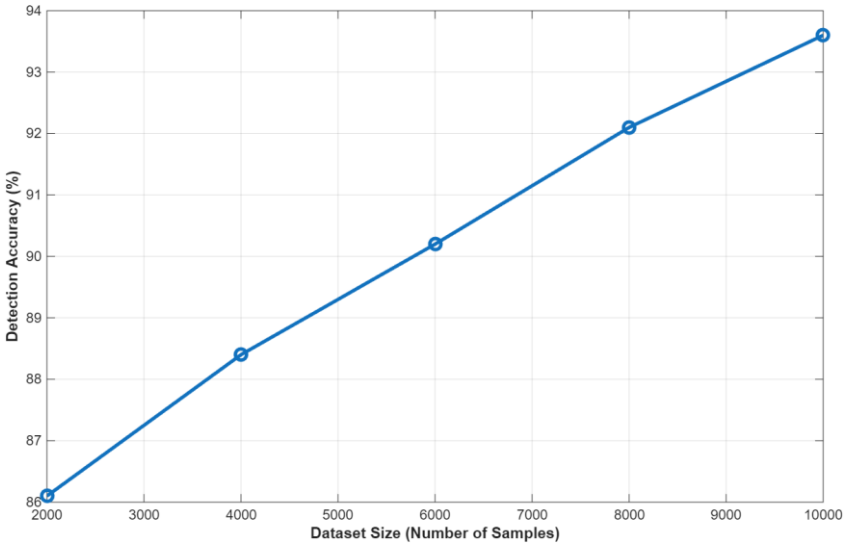

Fig.8. Scalability Analysis of Proposed Framework

Fig. 8 shows how the proposed system scales with increasing dataset size. As the dataset grows from 2,000 to 10,000 samples, the accuracy improves from 86.1% to 93.6%, being of high adaptability and strength. This legitimizes the capacity of the framework to have large scale network data.

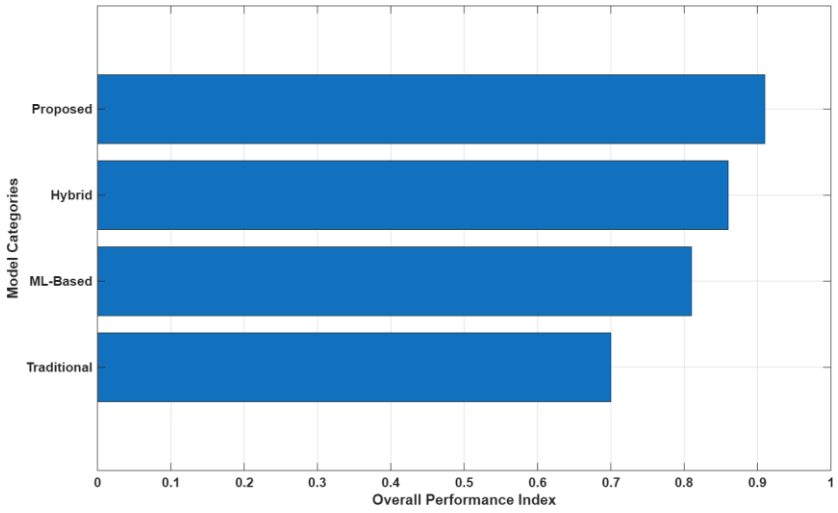

Fig.9. Performance Index Comparison of Different Models

Fig. 9 shows the comparison of the overall performance index. The proposed framework achieves the highest value of 0.91 compared to traditional (0.70), ML-based (0.81), and hybrid (0.86) models, demonstrating balanced improvement across all metrics. This justifies the effectiveness of the integrated deep learning and edge-cloud solution.

8 Conclusion and Future Work

The developed anomaly detection model for the cyber-physical system achieves 93.6% accuracy, 90.2% efficiency, 182ms latency, a stability rating of 0.89, and a performance index of 0.91. Using edge devices that can be integrated with cloud resources reduces response time, provides scalability, and enables the system to manage different workloads with higher capacity. The system is efficient at adapting to other evolving network standards without any loss of performance. Future development involves conducting large-scale real-world testing, developing further architectural enhancements, and improving system resilience across large-scale networks. Also, the focus will be on making AI-based decisions more interpretable to build greater trust in anomaly detection. Distributed learning methods can also be extended to enable model training across multiple locations without transferring raw data. Lightweight model ports may also be developed and deployed on resource-constrained edge devices. The system will be successful in combating new cyber threats because continuous updates and changes will be made over time.

References

[1] Elrawy, M. F., Awad, A. I., & Hamed, H. F. (2018). Intrusion detection systems for IoT-based smart environments: a survey. Journal of Cloud Computing, 7(1), 21. https://doi.org/10.1186/s13677-018-0123-6

[2] Pal, R., & Prasanna, V. (2016). The STREAM mechanism for CPS security the case of the smart grid. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 36(4), 537-550. doi: 10.1109/TCAD.2016.2565201

[3] Kholidy, H. A. (2021). Autonomous mitigation of cyber risks in the Cyber–Physical Systems. Future Generation Computer Systems, 115, 171-187. https://doi.org/10.1016/j.future.2020.09.002

[4] Vinayasree, P., & Reddy, A. M. (2025). A reliable and secure permissioned blockchain-assisted data transfer mechanism in healthcare-based cyber-physical systems. Concurrency and Computation: Practice and Experience, 37(3), e8378. https://doi.org/10.1002/cpe.8378

[5] Yang, J., & Mohajer, A. (2025). Multi-objective constellation optimization and dynamic link utilization for sustainable information delivery using PD-NOMA deep reinforcement learning. Wireless Networks, 31(2), 1839-1859. https://doi.org/10.1007/s11276-024-03834-x

[6] Alanezi, K., Annapareddy, T., Khan, S., & Mishra, S. (2026). An edge-based IDS for the IoT using combined ML and generative AI models. Peer-to-Peer Networking and Applications, 19(1), 24. https://doi.org/10.1007/s12083-025-02174-7

[7] Kumar, A., & Das, T. K. (2025). Orads: One class rule-based anomaly detection system in autonomous vehicles. IEEE Sensors Journal, 25(5), 8988-8997. doi: 10.1109/JSEN.2024.3523345.

[8] Kamble, A., & Dhotre, P. (2025, December). Centralized Security Monitoring for Effective Threat Detection and Analysis. In 2025 IEEE 5th International Conference on ICT in Business Industry & Government (ICTBIG) (pp. 1-6). IEEE. doi: 10.1109/ICTBIG68706.2025.11323853.

[9] Umar, H. G. A., Yasmeen, I., Aoun, M., Mazhar, T., Khan, M. A., Jaghdam, I. H., & Hamam, H. (2025). Energy-efficient deep learning-based intrusion detection system for edge computing: a novel DNN-KDQ model. Journal of Cloud Computing, 14(1), 32. https://doi.org/10.1186/s13677-025-00762-9

[10] Dong, W., Yu, J., Lin, X., Gou, G., & Xiong, G. (2025). Deep learning and pre-training technology for encrypted traffic classification: A comprehensive review. Neurocomputing, 617, 128444. https://doi.org/10.1016/j.neucom.2024.128444

[11] Kayan, H., Heartfield, R., Rana, O., Burnap, P., & Perera, C. (2025). Real-time anomaly detection for industrial robotic arms using edge computing. IEEE Internet of Things Journal. doi: 10.1109/TIA.2025.3556663.

[12] Chen, Y., Qian, C., Hussaini, A., & Yu, W. (2025). CPS foundation and principles. In Edge Intelligence in Cyber-Physical Systems (pp. 9-34). Academic Press. https://doi.org/10.1016/B978-0-44-326572-3.00008-5

[13] Al-Bahri, M., Muthanna, M. S. A., Zakarya, M., Alkanhel, R. I., Khan, A. A., & Alshahrani, A. (2026). A hybrid deep learning based intrusion detection framework to identify cyber attacks in edge-based IIoT. Telecommunication Systems, 89(2), 53. https://doi.org/10.1007/s11235-026-01421-3

[14] Nazir, A., He, J., Zhu, N., Wajahat, A., Ullah, F., Qureshi, S., & Pathan, M. S. (2025). Empirical evaluation of ensemble learning and hybrid CNN-LSTM for IoT threat detection on heterogeneous datasets: A. Nazir et al. The Journal of Supercomputing, 81(6), 775. https://doi.org/10.1007/s11227-025-07255-1

[15] Rahim, K., Nasir, Z. U. I., Ikram, N., & Qureshi, H. K. (2025). Integrating contextual intelligence with mixture of experts for signature and anomaly-based intrusion detection in CPS security. Neural Computing and Applications, 37(8), 5991-6007. https://doi.org/10.1007/s00521-024-10967-9

[16] http://research.unsw.edu.au/projects/unsw-nb15-dataset

[17] http://www.unb.ca/cic/datasets/ids-2017.html