Volume (2) No (1), 2026
Journal of Global Research in Multidisciplinary Studies (JGRMS)
Research Paper
Available online at https://saanvipublications.com/journals/index.php/jgrms/index

Lightweight Deep Learning Models for Intrusion Detection in Resource-Constrained Cyber-Physical Devices

Dr. Prithviraj Singh Rathore
Assistant Professor
Department of Computer Sciences and Applications
Mandsaur University
Mandsaur
prathviraj.rathore@meu.edu.in

***Abstract*—Important infrastructures like water treatment and smart grids rely heavily on cyber-physical systems (CPS), which are increasingly vulnerable to new and developing threats. The advent of Intrusion Detection Systems (IDS) tailored to CPS design has become one of the essential tactics for safeguarding them, despite the fact that traditional security measures like firewalls and encryption do not function well enough with CPS architecture. The study article presents a deep learning (DL) approach to an IDS to identify security attacks in a network of resource-constrained CPS using the CICIDS2017 database. Some preprocessing operations, such as cleaning, transformation, one-hot encoding, outliers removal using the Z-score method, and class balancing using SMOTE, were performed on the dataset. The tasks of dimensionality reduction and feature selection were performed with the help of Principal Component Analysis (PCA). The binary and multi-class intrusion detection was done with a built and tested six-layer Deep Neural Network (DNN) and a Convolutional Neural Network (CNN). The DNN could obtain 99.7% and the CNN 99.5%. The two models were good generalizers, with low overfitting, and high precision (PRE), recall (REC), and F1-Score (F1). Comparative performance analysis of the existing methods and the suggested models proved that the suggested models possess a higher detection accuracy and can be utilized much faster, hence, they may be an appropriate option when it comes to the deployment of a strong and scalable IDS in a cyber-physical environment.**

***Keywords*—Cyber Physical Systems (CPSs), Deep Learning, Intrusion Detection System (IDS), Anomaly Detection, Water Treatment Systems.**

I. INTRODUCTION

To identify and detect intrusion attacks, cybersecurity [1] systems use the Intrusion Detection System (IDS), a potent tool. There is a greater chance of intrusion attempts in different forms as data generation increases [2]. One of the biggest issues nowadays is the necessity of maintaining strong cybersecurity, since the variety of networking technologies is increasing quickly, and cyber-attacks are becoming more common [3]. In cybersecurity, one of the most crucial aspects is identifying and stopping malicious behavior and gaining access to computer networks [4]. Monitoring network activity and spotting any security breaches requires an intrusion detection system, or IDS. Traditional IDS systems primarily rely on signature-based methods, making it difficult to detect new and complex threats.

The link of a physical and cyber system where data and information are exchanged in real-time is known as a cyber-physical system (CPS) [5][6]. CPS has a lot of economic potential and is crucial in the IoT-based sector. With its foundation in the IoT, CPS takes into account how physical, network, and computer systems interact [7]. It has evolved into the Internet of Cyber-Physical Things, which offers a variety of services, including smart homes, smart cities, e-commerce, and e-health.

The resource-constrained environment in Internet of Things (IoT) security poses significant challenges, including but not limited to data encryption, privacy preservation, vulnerabilities, threats, attacks, and limits, despite the existence of several Internet security solutions. For these privacy and security concerns related to the IoT to be resolved, it is essential to develop appropriate technologies for environments with limited resources.

The AI algorithms may have their own set of vulnerabilities [8]They may also be the answer to this problem by keeping an eye on network traffic in an industrial environment. Regular updates are necessary for these systems, especially those that are connected to an IIoT infrastructure, because unknown attack signatures can greatly impact an IDS. This is how an AI-based IDS differs from a traditional IDS system [9]. It is impossible for traditional intrusion detection methods, including signature-based detection systems, to detect newly launched attacks (zero-day attacks) or to adjust to changing attack tactics. Therefore, ML and DL have become important topics in intrusion detection system network security research [10][11]. The computing power required for DL models is often considerable [12], especially when it comes to graphics processing units (GPUs) or transpose units (TPUs), which have a number of downsides, such as expensive training, subpar performance in real-time, and a heavy communication burden associated with centralized models. Such issues can jeopardize the disclosure of private data and are particularly troublesome in edge computing.

A. Motivation

The complexity of CPS and IoT networks has exposed them to increasingly advanced cyber threats. Conventional

signature-based IDS techniques are incapable of identifying new attack types or adapting to the evolving threat landscape. The research presented here aims to create smart, energy-efficient DL-driven IDS models using DNN and CNN to achieve results very close to the truth, rapid detection, and the ability to be extended to environments with limited resources in CPS. The following are the primary findings of the research:

- Designing a DL–driven IDS that uses the CICIDS2017 dataset for security in cyber-physical systems.
- Performing thorough data pre-treatment procedures, including data transformation, encoding, cleaning, and Z-score outlier detection.
- Using SMOTE, can improve the model training process and address the issue of class imbalance.
- Data dimensionality reduction and effective feature selection are accomplished by using PCA.
- Convolutional and deep neural networks (CNNs and DNNs, respectively) were used to develop IDS models.
- Model performance evaluation using REC, ACC, PRE, F1, and loss metrics to choose the best network model for intrusion detection.

B. Organization of the Research

This research is organized in the following way: Section II covers literature related to IDS in resource-constrained CPS, Section III explains the methodology, i.e., dataset, pre-processing, and model implementation, Section IV shows the comparative analysis and experimental results, and Section V conclusion the study and suggests avenues for more investigation.

II. Related Work

This study's main aim is to analyze panel study data about IDS in CPS with limited resources. The research domain and the methodological framework of this study were influenced by the findings of this analysis. A summary of the examined research is represented by Table I, which includes the aspects of the review, focus of the study, models and techniques applied, datasets, main findings, and comments.

Ravi Kumar et al. (2025) suggested a HEGSO algorithm is used to choose which features to use in the XAIID-SCPS method. The usage of an Improved Elman Neural Network (IENN) architecture for parameter standardization and the Enhanced Fruitfly Optimization (EFFO) approach for intrusion detection. To make the black-box technique simpler to comprehend and explain, the XAIID-SCPS method additionally integrates the XAI methodology with Local Interpretable Model-Agnostic explanation (LIME). This makes it possible to accurately define attacks. There is a 98.88% chance that the XAIID-SCPS technique work better than other methods, as shown by the higher simulation numbers [13].

Denis and Di Pietro (2025) they evaluated their framework with a use case focusing on authentication at the physical layer of USB devices—these latter devices being a common vector for cyber-physical attacks. Their approach achieves an average F1-score of 0.945 without requiring physical contact or activation to distinguish self from non-self-devices. The results demonstrate the feasibility of the framework for reducing the attack surface in cyber-physical environments. This work lays the foundation for broader applications of harmonic radar in intrusion detection and hardware authentication [14].

T P and Kathrine (2024) a novel IDS that makes use of GNN and RNN. The GNN+RNN architecture has been given this dataset after it has been created as a graph. With 99.13% f1, 100% of PRE, 98% of REC, and 99% detection accuracy, the suggested model has been proven to be very effective [15].

Soomro et al. (2024) Their solution was Fed Secure IDS, a cutting-edge lightweight federated deep IDS that uses federated learning (FL), CNN, LSTM, and MLP to tackle these problems. When it comes to symmetric session key exchange and mutual authentication, Fed Secure IDS provides a simple solution that tackles two major security issues: eavesdropping and man-in-the-middle attacks. Testing findings show that the suggested approach achieves a 98.68% ACC, 98.78% PRE, 98.64% REC, and 99.05% F1 by utilising a range of edge devices. In traditional centralized IDS architectures, the concept works in a similar way [16].

Latham and Bommi (2023) The suggested method is to build a trustworthy model for discovering intrusions into networks that impact Internet of Things devices. The IDS2017 dataset is used to form a regression model with Cat Boost in the system. The presented approach considers a variety of factors as critical characteristics for identifying the presence of intrusion attacks on the network. The accuracy of the system supplied was 92.5% and it was contrasted with other modern methods [17].

Abdullahi et al. (2022) proposed that the CPS is vulnerable to serious cyberattacks. To deal with this, new DL approaches that can detect, identify and respond to the change in these attacks are required. In order to identify cybersecurity risks for the CPS, this study suggested a DL model based on LSTM. Furthermore, the model has been tested using real-life datasets of gas pipeline ICSs, which include 19 attributes and 7 forms of attacks. The results obtained from the experiment showed that after being validated, the accuracy of the suggested model was 98.22%. Additionally, the report makes a suggestion for possible further research [18].

TABLE I. Summary of the Literature Review on Intrusion Detection Systems (IDS) in Limited-Resource Cyber-Physical Systems (CPS)

Author (Year)	Study Focus	Techniques / Models Used	Dataset	Key Findings	Remarks
Ravi Kumar et al. (2025)	Feature selection and explainable IDS for CPS	HEGSO, EFFO, IENN, XAI with LIME	Not specified	Achieved 98.88% accuracy, outperforming existing methods	Incorporates explainable AI for improved interpretability in IDS models
Denis and Di Pietro (2025)	Hardware authentication and intrusion detection at the physical layer	Harmonic radar-based authentication framework	USB device authentication dataset	Achieved an average F1-score of 0.945	Demonstrated feasibility for reducing attack surfaces in CPS environments

T. P. and Kathrine (2024)	Graph-based IDS for CPS	RNN + GNN	Graph-structured network traffic dataset	Achieved 99% accuracy, 100% precision, 98% recall, and 99.13% F1-score	Strong detection capability using graph-based deep learning
Soomro et al. (2024)	Federated deep IDS for edge and CPS environments	FedSecureIDS combining CNN, LSTM, and MLP within Federated Learning (FL)	Various edge device datasets	Accuracy: 98.68%, Precision: 98.78%, Recall: 98.64%, F1-score: 99.05%	Lightweight federated approach ensuring privacy and high detection accuracy
Latha and Bommi (2023)	IoT network intrusion detection	CatBoost regression model	CICIDS2017 dataset	Achieved 92.5% accuracy	Effective detection of IoT intrusions, though performance below deep learning models
Abdullahi et al. (2022)	Cyberattack detection in CPS	Long Short-Term Memory (LSTM) neural network	Industrial Control System (ICS) gas pipeline dataset	Achieved 98.22% accuracy	Demonstrated DL effectiveness in real-world CPS security applications

III. Research Methodology

The main purpose of this project is to build a security system that can recognize aberrant behaviours in cyber-physical systems via the use of) CICIDS2017 dataset and DL methods. DNN and CNN models are developed on a 70:30 split with pre-processing, SMOTE balancing, and PCA reduction. Evaluate the models' effectiveness using measures such as F1, loss, REC, ACC, and PRE to determine which model performs best in recognizing the cyber threat. The study's progression is seen in Figure 1.

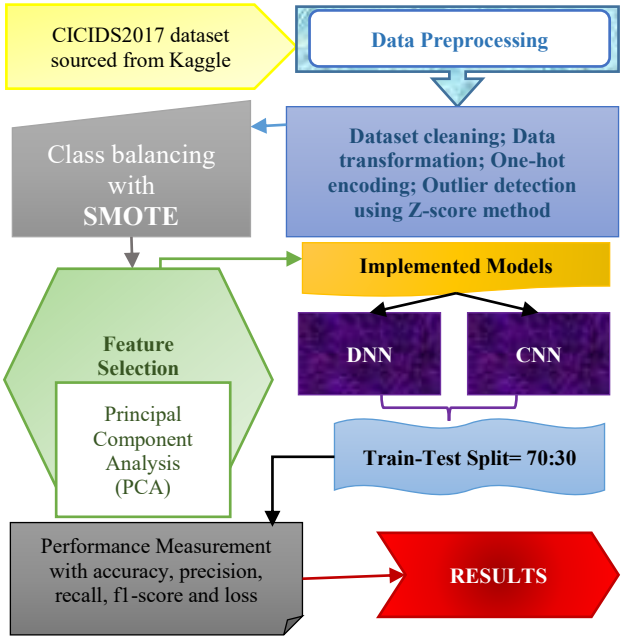


Fig. 1. Flowchart visualization for IDS in Resource-Constrained Cyber-Physical Systems

The following section thoroughly explains the methodology.

A. Data Selection and Visualization

This research employs the CICIDS2017 dataset available on Kaggle, a product of to evaluate Intrusion Detection System (IDS) efficacy in cyber-physical settings, in collaboration with the CIC. Besides normal traffic, it also contains various types of malicious traffic, including the following attacks: DoS, DDoS, Brute Force, Botnet, Infiltration, and Web Attacks. There are 78 features per network flow, and the dataset has close to 2.8 million records, thus offering an extensive and realistic resource for the creation and testing of IDS models. The data visualization of the dataset is shown below:

Fig. 2. Correlation Heatmap

The pairwise Pearson correlation coefficients of the characteristics of the dataset are presented in the Figure 2. Features are shown on the two axes and the color intensity shows the strength of correlation: strong correlations (positive) +1.0, are shown in dark red, strong correlations (negative) -1.0, are shown in dark blue, weak or no correlations (0), are shown in lighter colors. The dark diagonal line is the case of a perfect correlation between the features. This plot is useful for spotting which features are strongly correlated or even redundant and thus assist in feature selection and dimensionality reduction.

B. Data Pre-processing

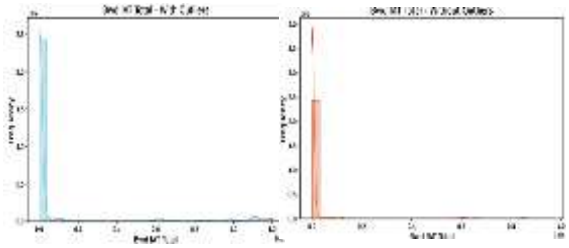
It is important to process mistakes and string data that cannot be processed numerically or not useful to train. The purpose of the processing of this study was to get rid of repetitive data, outliers, and useless data elements.

- **Dataset Cleaning:** The experiment cannot proceed without first pre-processing the data set. First, cleaned up the dataset, eliminating any unnecessary things. Missing or infinite values were eliminated from entries, since they represented such a tiny fraction of the whole dataset. To expose the models to as many different examples as possible, also removed duplicates.
- **Data Transformation:** Data transformation is an important part of getting ready for data analysis, especially in the case of heterogeneous network traffic data with both numerical and qualitative information.
- **One-Hot Encoding:** The most popular use of the one-hot encoding approach is to use 0 and 1 to transform a category data vector to a numeric feature vector.
- **Outlier Detection using the Z-score method:** In order to identify the outliers properly, took the help of Z-score technique. This statistical analysis instrument

that is good at identifying important deviations of the mean, offers an objective view to the detection of anomalies. Equation (1) gives the formula for the method:

$$Z = \frac{x-\mu}{\sigma} \quad (1)$$

where σ is the standard deviation, μ is the data mean, x is the observation value, and Z is the z-score.



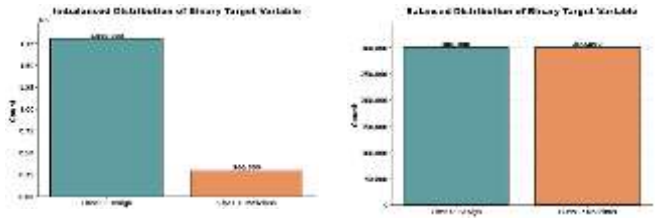
3(a) 3(b)

Fig. 3. Histograms of 'Bwd IAT Total' with and without the Outliers

Figure 3 shows the Effect of Outlier Removal — Figure 3(a), "Bwd IAT Total – With Outliers," displays a distribution that is very skewed to the right, mostly values close to zero, and extreme outliers around 1.0 × 10 8 1.0×10 8 .. Figure 3(b), "Bwd IAT Total – Without Outliers," shows the same characteristic after the high-value outliers have been removed. The distribution is still right-skewed, but the scale is compressed, so more detail and variation within the main range are visible.

C. Addressing Data Balancing with the Implementation of SMOTE

The subset's representation of attack kinds was balanced by taking additional measures. To rectify unequal distributions, these measures might include either under sampling majority groups or oversampling minority classes. During thorough examination of the dataset, a serious class imbalance problem was discovered in the study, with numerous innocuous network traffic samples and a small number of cases that are typical of specific network assaults. To lessen this issue, employed the SMOTE. And the SMOTE's concept is to use available minority samples to synthesize instances for the minority class. In order to increase the number of samples of minority classes and move them closer to equality, SMOTE strategically creates new attacks that closely mimic real attacks.



4(a) 4(b)

Fig. 4. Imbalanced and Balanced Distribution of the Target Variable in the Dataset

The comparison of the imbalanced and then balanced class distributions is shown in Figure 4. Figure 4(a) shows the original imbalance in which Class 0: Benign (1.8M) is overwhelming Class 1: Malicious (300K) significantly. Figure 4(b) shows the balanced result of both classes (300K), which means the 1:1 ratio obtained by down-sampling to balance the dataset for training the model.

D. Feature Selection by applying Principal Component Analysis (PCA)

A crucial step in the feature selection process is PCA [19]. PCA converts the initial variables into a new set of independent variables in order to discern and retain the most important aspects. By reducing data dimensionality while preserving as much variety as possible, PCA can improve model performance and reduce computational costs. Using PCA, can leverage the data's inherent patterns and structures to inform subsequent analyses and models.

E. Model Development

DL models can categorize behaviors as normal or deviant by recognizing patterns in CPS. In order to assess the efficacy of DL methodologies, created and examined many DL models, such as:

1) Deep Neural Network (DNN)

In order to identify infiltration in this experiment, a six-layer DNN has been constructed and refined. A network design with two hidden levels was the starting point. Nevertheless, the experimental findings indicate that the network's performance with two hidden layers is unsatisfactory [20]. The six-layer DNN produced the best results, so it was tested with varying numbers of hidden layers. The feature extraction module extracts features. The dataset contains the features, with eight features per row [21]. Before being sent to the suggested network, these rows are transposed using Equation (2):

$$F_{input} = [F_1, F_2, F_3, F_4, F_5, F_6]^T \quad (2)$$

The network's output vector is determined by Equation (3):

$$y^l = \sigma^l(B^l + W^l K^{l-1}) \quad (3)$$

where the output vector is denoted by y^l, the activation function by σ^l, the bias vector by B^l, and the layer before the layer l by K^{l-1}.

2) Convolutional Neural Network (CNN)

In order to perform binary and multi-class classifications, the provided model architecture incorporates a CNN. An input layer accepts a one-dimensional array of sequential data as its starting point. The first CNN block consists of a convolutional layer, max pooling, dropout, batch normalization, and ReLU activation, which is responsible for efficient feature extraction and regularization [22]. This is done iteratively using several CNN blocks with varied kernel sizes, each of which detects a unique feature or pattern in the input. In order to filter the input data and extract features, the convolution process is utilized by the CNN layers. To do this, the input feature map is used as a basis for sliding the convolution kernel across it, with each point being used to compute the dot product and ultimately produce a feature map. An equation describing the mathematical aspects of the convolution procedure is given by Equation (4) below:

$$Z_{i,j} = (X * K)_{i,j} = \sum_m \sum_n Z_{i+m,j+n} k_{m,n} \quad (4)$$

In this case, X is the input feature map, and Z is the output. The input features are transformed into output features using a convolution kernel K throughout the convolution process.

F. Dataset Splitting

The data is divided into 70:30 training and test sets, with 70% utilized for training and 30% for testing, in order to train and assess DL models.

IV. Results and Evaluation Metrics

The experiments in this research were conducted using a Core (TM) i7-1065G7 CPU operating at 1.30 GHz and 1.50 GHz. Python version 3.7.1 is also used, as it has a wide range of classification models and libraries.

A. Evaluation Measures

Important measures for evaluating cybersecurity effectiveness include F1, REC, PRE, and ACC. To achieve optimal accuracy on the IDS dataset, a DL model was trained in this investigation. The suggested DL models were evaluated for their classification performance using the CICIDS2017 dataset.

A general indicator of how well the model distinguishes between malicious and benign actions, accuracy indicates the proportion of correctly identified network activities. PRE is the proportion of intrusions found that are actual attacks, thereby minimizing false alarms. The ability of a model to capture all of the real assaults of the system is measured by its rec. A balanced measure of detection ability is the F1, the harmonic mean of acc and rec. The set has been completed by loss, which is the discrepancy between the model's projected output and the actual activity labels. It demonstrates the IDS's ability to differentiate between harmful and benign activities with minimal processing effort. The mathematical representations of these metrics are represented by Equations (5)-(8):

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} \tag{5}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \tag{6}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP+FN}} \tag{7}$$

$$F1 = \frac{2\times precision\times recall}{precision+recall} \tag{8}$$

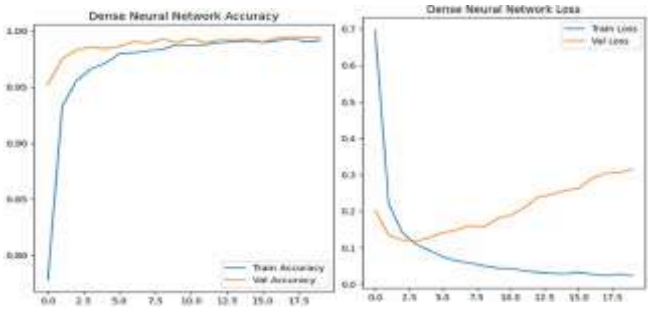
TP are the times when attacks are correctly recognized as intrusions, and TN are the normal system operations that are correctly identified as safe. FP are normal activities that have been wrongly flagged as intrusions, thus causing false alarms, and FN are those real attacks that have been wrongly taken for normal behavior, hence, they are a source of potential security risks.

B. Result Demonstrations

The effectiveness of DNN and CNN models for the Intrusion Detection task in resource-constrained Cyber-Physical Systems is compared in Table II. Both models are excellent to the point that DNN just slightly outperformed CNN. The DNN was able to achieve 99.7% accuracy, whereas the CNN was at 99.5% accuracy.

TABLE II. Model Performance for IDS in Resource-Constrained Cyber-Physical Systems

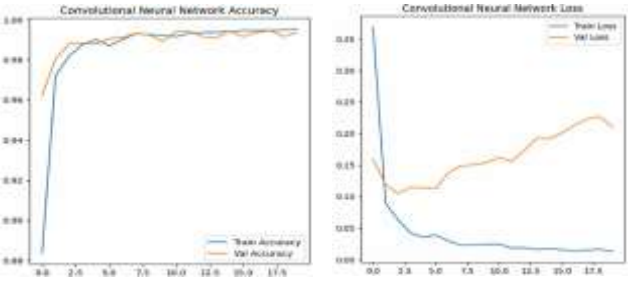
Metrics	DNN	CNN
Accuracy	99.7	99.5
Precision	99.0	98.0
Recall	99.0	99.0
F1-Score	99.0	99.0



5(a) Accuracy **5(b) Loss**

Fig. 5. Training-Validation Accuracy and Loss

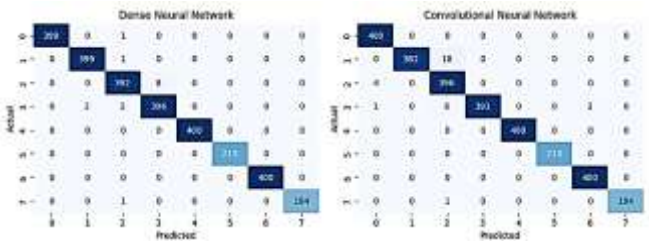
Figure 5 shows the changes of the Dense Neural Network (DNN) performance over the training epochs for Accuracy (5(a)) and Loss (5(b)). In Figure 5(a), the accuracies on both the training and validation sets reach 1.0 very quickly and remain there from about 12 epochs, indicating that the model has learned well and generalized correctly. Figure 5(b) shows the loss gradually reducing to 0 during training; however, after reaching a minimum around 5 epochs, it starts to increase slightly, indicating a slight overfitting.



6(a) Accuracy **6(b) Loss**

Fig. 6. Training-Validation Accuracy and Loss

Figure 6 illustrates the CNN model's training performance in terms of Accuracy (6(a)) and Loss (6(b)) over epochs. In Figure 6(a), the accuracies of both the training and validation sets increase rapidly from 0.96 to approximately 0.99 over 10 epochs, and they converge, indicating proper learning and generalization. In Figure 6(b), the loss of the training is continuously getting lower and reaches 0, whereas the loss of validation is a little bit higher after 5 epochs, which means that there is a small amount of overfitting, though the validation accuracy is very high.



(a) **(b)**

Fig. 7. Confusion Matrices: (a) Deep Neural Network (DNN); (b) Convolutional Neural Network (CNN)

Figure 7 shows the Confusion Matrices for a DNN (a) and a CNN (b) used for an 8-class classification task. Both models

are effective, as most of their predictions fall on the diagonal, indicating high accuracy. The DNN has a few instances of mixture between the classes '2' and '3', whereas the CNN sometimes confuses class '1' with '2'. In general, the CNN shows slightly better diagonal dominance, suggesting a marginally higher accuracy.

C. Comparative Evaluation

Table III shows the performance comparison of different intrusion detection system (IDS) models in resource-constrained cyber-physical systems based on their accuracy. The CNN-LSTM model achieved 95.21% accuracy, while the MAD-GAN and GRU models achieved 96.80% and 97.81%, respectively. The MLP model's accuracy was 94.79%. The newly designed models were beyond the reach of the old methods, with the newly designed DNN recording the highest accuracy of 99.7%, and the newly designed CNN being the second closest with 99.5% accuracy.

TABLE III. PERFORMANCE COMPARISON OF IDS IN RESOURCE-CONSTRAINED CYBER-PHYSICAL SYSTEMS

Ref.	Model	Acc.	Pre.	Rec.	F1-Sc.
[23]	CNN-LSTM	95.21	88.76	82.59	84.14
[24]	MAD-GAN	96.80	96.98	98.11	96.25
[25]	GRU	97.81	98.36	98.07	98.03
[26]	MLP	94.79	94.79	94.79	94.78
Prop.	DNN	99.7	99.0	99.0	99.0
Prop.	CNN	99.5	98.0	99.0	99.0

Table IV provides a comparison of different intrusion detection system (IDS) models that have been used on various datasets in cyber-physical systems with limited resources. The ML-CPSS model achieved 97.8% acc on the TON_IoT dataset. In contrast, the Random Forest (RF) model achieved 87.75% on the STIN dataset. The DCNN-HMACO model achieved 92.14% acc on the UNSW-NB15 and TON_IoT datasets. Also, the Decision Tree (DT) model achieved 97.85% on the HAI dataset. The proposed models have shown better results: the proposed DNN achieved 99.5% on the CIC-IDS2017 dataset, and the suggested CNN came in fairly close at 99.5%, whereas the highest accuracy was 99.7%.

TABLE IV. PERFORMANCE COMPARISON OF IDS IN RESOURCE-CONSTRAINED CYBER-PHYSICAL SYSTEMS ACROSS MULTIPLE DATASETS

Ref.	Model	Dataset	Acc.	Pre.	Rec.	F1-Sc.
[27]	ML-CPSS	ToNIoT	97.8	97.7	97.8	97.7
[28]	RF	STIN	87.75	89.98	91.02	90.50
[29]	DCNN-HMACO	UNSW-NB15 and TON_IoT	92.14 %	-	94.0	87.0
[30]	DT	HAI	97.85	-	-	99.70
Prop.	DNN	CIC-IDS2017	99.7	99.0	99.0	99.0
Prop.	CNN	CIC-IDS2017	99.5	98.0	99.0	99.0

D. Discussion

According to the study, DNN and CNN models have been very effective in detecting network intrusions in cyber-physical systems under limited resources. In essence, both models have shown fast learning, generalized well, and performed strongly in multi-class classification with very few errors. Compared with current IDS methods, the proposed models are more flexible and reliable; thus, DL architectures pave the path to increased detection efficiency and accuracy in these environments.

V. CONCLUSION AND FUTURE SCOPE

The rapid integration of CPS into key industries highlights the critical need for efficient intrusion detection. The study results show that DL-based ID may improve security in resource-restricted CPS to a greater extent by comparing several online and offline ML techniques for intrusion detection in the CPS region. It was discovered that the models tested performed very well, with the Deep Neural Network (DNN) achieving 99.7% accuracy and the Convolutional Neural Network (CNN) achieving 99.5% accuracy. Such results indicate that DL techniques are reliable, effective and adaptable in detecting and classifying network attacks, leading to the fact that the techniques are highly viable in practice in cyber-physical environments.

Future work can examine how the proposed models may be streamlined to enable real-time intrusion detection using lightweight architectures applicable to edge and IoT devices. In fact, the application of hybrid DL models, complex feature selection schemes, and continuous learning strategies can further improve the systems' ability to adapt, detection accuracy, and resistance to cyber threats in a constantly changing cyber-physical environment.

REFERENCE

[1] B. R. Cherukuri, "Advanced Multi Class Cyber Security Attack Classification in IoT Based Wireless Sensor Networks Using Context Aware Depthwise Separable Convolutional Neural Network," *J. Mach. Comput.*, vol. 5, no. 2, 2025.

[2] S. Narang and A. Gogineni, "Zero-Trust Security in Intrusion Detection Networks: An AI-Powered Threat Detection in Cloud Environment," *Int. J. Sci. Res. Mod. Technol.*, vol. 4, no. 560–70, pp. 60–70, Jun. 2025, doi: 10.38124/ijsrmt.v4i5.542.

[3] A. R. Bilipelli, "AI-Driven Intrusion Detection Systems for Large-Scale Cybersecurity Networks Data Analysis : A Comparative Study," *TIJER – Int. Res. J.*, vol. 11, no. 12, pp. 922–928, 2024.

[4] V. M. L. G. Nerella, K. K. Sharma, S. Mahavratayajula, and H. Janardhanan, "A Machine Learning Framework for Cyber Risk Assessment in Cloud-Hosted Critical Data Infrastructure," *J. Inf. Syst. Eng. Manag.*, vol. 10, no. 4, pp. 2409–2421, 2025, doi: 10.52783/jisem.v10i4.12804.

[5] G. Sarraf, "Resilient Communication Protocols for Industrial IoT : Securing Cyber- Physical-Systems at Scale," *Int. J. Curr. Eng. Technol.*, vol. 11, no. 6, pp. 694–702, 2021, doi: 10.14741/ijcet/v.11.6.14.

[6] M. R. R. Deva, "Advancing Industry 4.0 with Cloud-Integrated Cyber-Physical Systems for Optimizing Remote Additive Manufacturing Landscape," in *2025 IEEE North-East India International Energy Conversion Conference and Exhibition (NE-IECCE)*, IEEE, Jul. 2025, pp. 1–6. doi: 10.1109/NE-IECCE64154.2025.11182940.

[7] V. Shah, "Traffic Intelligence In Iot And Cloud Networks: Tools For Monitoring, Security, And Optimization," *Int. J. Recent Technol. Sci. Manag.*, vol. 9, no. 5, 2024, doi: 10.10206/IJRTSM.2025894735.

[8] K. S. BuchiReddy, B. R. Kumar, A. N. Reddy, and N. S. Kumar, "Cross-Domain Expert in Designing AI-Driven Microservices," *Int. J. Nov. Res. Dev.*, vol. 9, no. 12, pp. 820–824, 2024.

[9] P. Gupta, S. Kashiramka, and S. Barman, "A Practical Guide for Ethical AI Product Development," in *2024 IEEE 11th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)*, 2024, pp. 1–6. doi: 10.1109/UPCON62832.2024.10983504.

[10] J. R. Vummadi, H. Volikatla, and S. Dodda, "Smart HR for Smart Enterprises: A Machine Learning-Based Approach to Payroll Automation and Time Optimization," *Int. J. Artif. Intell. Data Sci. Mach. Learn.*, vol. 6, no. 3, pp. 80–89, 2025, doi: 10.63282/3050-9262.IJAIDSML-V6I3P113.

[11] A. Parupalli, "Business-Oriented Employee Performance Assessment via Machine Learning in ERP Systems," *TIJER – Int.*

Res. J., vol. 11, no. 11, 2024.

[12] B. R. Ande, "Ai-Powered Real-Time Identity Authentication And Fraud Detection Using Deep Learning Networks," 2025.

[13] M. R. Kumar, G. . Madhu, V. B. Narra, and V. K. Chidipothu, "Improved Intrusion Detection in Cyber-Physical Systems with Explainable AI and Hybrid Optimization," in *2025 IEEE International Conference on Emerging Technologies and Applications (MPSec ICETA)*, IEEE, Feb. 2025, pp. 1–6. doi: 10.1109/MPSecICETA64837.2025.11118490.

[14] N. Denis and R. Di Pietro, "Replicating Human Immune System via Harmonic Radar: A Framework and Preliminary Results in Thwarting Cyber-physical Attacks," in *2025 55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S)*, Jun. 2025, pp. 196–200. doi: 10.1109/DSN-S65789.2025.00013.

[15] D. T P and J. W. Kathrine, "Secure and Efficient Intrusion Detection System in Medical Cyber-Physical Systems," in *2024 3rd International Conference on Automation, Computing and Renewable Systems (ICACRS)*, IEEE, Dec. 2024, pp. 602–608. doi: 10.1109/ICACRS62842.2024.10841721.

[16] I. A. Soomro, H. ur Rehman Khan, S. J. Hussain, Z. Ashraf, M. M. Alnfiai, and N. N. Alotaibi, "Lightweight privacy-preserving federated deep intrusion detection for industrial cyber-physical system," *J. Commun. Networks*, vol. 26, no. 6, pp. 632–649, Dec. 2024, doi: 10.23919/JCN.2024.000054.

[17] R. Latha and R. M. Bommi, "Hybrid CatBoost Regression model based Intrusion Detection System in IoT-Enabled Networks," in *2023 9th International Conference on Electrical Energy Systems (ICEES)*, 2023, pp. 264–269. doi: 10.1109/ICEES57979.2023.10110148.

[18] M. Abdullahi, H. Alhussian, N. Aziz, S. J. Abdulkadir, and Y. Baashar, "Deep Learning Model for Cybersecurity Attack Detection in Cyber-Physical Systems," in *2022 6th International Conference On Computing, Communication, Control And Automation (ICCUBEA*, 2022, pp. 1–5. doi: 10.1109/ICCUBEA54992.2022.10010717.

[19] U. A. Korat and A. Alimohammad, "A Reconfigurable Hardware Architecture for Principal Component Analysis," *Circuits, Syst. Signal Process.*, vol. 38, no. 5, pp. 2097–2113, May 2019, doi: 10.1007/s00034-018-0953-y.

[20] K. B. Thakkar and H. P. Kapadia, "The Roadmap to Digital Transformation in Banking: Advancing Credit Card Fraud Detection with Hybrid Deep Learning Model," in *2025 2nd International Conference on Trends in Engineering Systems and Technologies (ICTEST)*, 2025, pp. 1–6. doi: 10.1109/ICTEST64710.2025.11042822.

[21] R. Patel, "Automated Threat Detection and Risk Mitigation for ICS (Industrial Control Systems) Employing Deep Learning in Cybersecurity Defence," vol. 13, no. 6, pp. 584–591, 2023.

[22] S. J. Wawge, "Evaluating Machine Learning and Deep Learning Models for Housing Price Prediction : A Review," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 11, pp. 367–377, 2025, doi: 10.48175/IJARSCT-25857.

[23] A. Balla, M. H. Habaebi, E. A. A. Elsheikh, M. R. Islam, F. E. M. Suliman, and S. Mubarak, "Enhanced CNN-LSTM Deep Learning for SCADA IDS Featuring Hurst Parameter Self-Similarity," *IEEE Access*, vol. 12, pp. 6100–6116, 2024, doi: 10.1109/ACCESS.2024.3350978.

[24] B. A. Y. Alqaralleh, F. Aldhaban, E. A. AlQarallehs, and A. H. Al-Omari, "Optimal Machine Learning Enabled Intrusion Detection in Cyber-Physical System Environment," *Comput. Mater. Contin.*, vol. 72, no. 3, pp. 4691–4707, 2022, doi: 10.32604/cmc.2022.026556.

[25] A. Al Mazroa, F. R. Albogamy, M. Khairi Ishak, and S. M. Mostafa, "Boosting Cyberattack Detection Using Binary Metaheuristics With Deep Learning on Cyber-Physical System Environment," *IEEE Access*, vol. 13, pp. 11280–11294, 2025, doi: 10.1109/ACCESS.2025.3526258.

[26] H. Babbar, S. Rani, and M. Shabaz, "Federated learning with enhanced cryptographic security for vehicular cyber-physical systems," *Sci. Rep.*, vol. 15, no. 1, pp. 1–16, 2025, doi: 10.1038/s41598-025-14341-0.

[27] F. Alserhani, "Intrusion Detection and Real-Time Adaptive Security in Medical IoT Using a Cyber-Physical System Design," *Sensors*, vol. 25, no. 15, 2025, doi: 10.3390/s25154720.

[28] I. Ashraf *et al.*, "A Deep Learning-Based Smart Framework for Cyber-Physical and Satellite System Security Threats Detection," *Electron.*, vol. 11, no. 4, pp. 1–15, 2022, doi: 10.3390/electronics11040667.

[29] M. A. Alohali, M. Elsadig, A. M. Hilal, and A. Mutwakel, "Emerging framework for attack detection in cyber-physical systems using heuristic-based optimization algorithm," *PeerJ Comput. Sci.*, vol. 9, pp. 1–22, 2023, doi: 10.7717/peerj-cs.1596.

[30] O. Tushkanova, D. Levshun, A. Branitskiy, E. Fedorchenko, E. Novikova, and I. Kotenko, "Detection of Cyberattacks and Anomalies in Cyber-Physical Systems: Approaches, Data Sources, Evaluation," *Algorithms*, vol. 16, no. 2, pp. 1–18, 2023, doi: 10.3390/a16020085.

