International Journal of Safety and Security Engineering
Vol. 15, No. 10, October, 2025, pp. 2033-2041
Journal homepage: http://iieta.org/journals/ijsse

BiGRU-Based Intrusion Detection Framework for Enhancing Security in Cyber-Physical Systems

Ponugoti Kalpana[1*], Sunitha Tappari[2], Sushma Polasi[3], L Smitha[4], Sahithi Godavarthi[5], Meeniga Vijayalakshmi[6], Gona Jagadesh[7]

[1] Department of Computer Science and Engineering, AVN Institute of Engineering and Technology, Hyderabad 501510, Telangana, India
[2] Department of Electronics and Telematics, G Narayanamma Institute of Technology and Science, Hyderabad 500104, Telangana, India
[3] Department of Computer Science and Engineering (Cyber Security), Vignana Bharathi Institute of Technology, Hyderabad 501301, Telangana, India
[4] Department of Information Technology, G Narayanamma Institute of Technology and Science, Hyderabad 500104, Telangana, India
[5] Department of Computer Science and Engineering (CS), CVR College of Engineering, Hyderabad 501510, Telangana, India
[6] Department of Electronics and Communication Engineering, G Narayanamma Institute of Technology and Science (for women), Hyderabad, 500104 Telangana, India
[7] School of Engineering, Anurag University, Hyderabad 500088, Telangana, India

Corresponding Author Email: drkalpanacse@gmail.com

https://doi.org/10.18280/ijsse.151006

Received: 22 August 2025
Revised: 9 October 2025
Accepted: 20 October 2025
Available online: 31 October 2025

Keywords:
cyber-physical system, data privacy, Bi-GRU network, sequence modeling, intrusion detection system

ABSTRACT

Cyber-physical systems (CPS) face rising sophisticated cyber attacks because they connect with digital systems through networks. Data security and privacy protection within these systems stands as the key factor for operational integrity maintenance. An effective intrusion detection method with improved security and privacy capabilities serves to enrich CPS environments. This research leverages the NSL-KDD, a well-established benchmark dataset for attack detection and the proposed model employs the BI-GRU architecture. The design of this model targets both forward and backward time sequences because it aims to analyze contextual dependencies thus enhancing threat classification accuracy. Present intrusion detection methods currently find it difficult to maintain generality between developing attack vector patterns since their sequential pattern modeling capabilities remain inadequate. In order to overcome this limitation, the proposed Bi-Gated Recurrent Units (Bi-GRU) based model presents a bidirectional representation that yields more detailed dependencies and is more resistant to various intrusion behaviors. The model attains a high accuracy of 98.47%, surpassing other models such as LSTM (94.5%), GRU (95.7%), and BiLSTM (93.9%) in generalization. While existing CPS IDS frameworks have a high false-positive rate, the suggested framework reduces false-positives rate to 3%, which makes it more reliable in real-life CPS settings. The suggested model demonstrated its effectiveness by the efficient information processing capability and its low false positive rate with its high generalization capacity. The study performs significant experimental trials to demonstrate real-time application of this approach in CPS settings that introduces a significant breakthrough in cyber-physical infrastructure security against intelligent attacks.

1. INTRODUCTION

Cyber-physical systems (CPS) act as technological transformation drivers since they integrate physical processes with computational intelligence approaches [1]. These systems have now been widely applied in multiple applications, like industrial automation, transport systems, patient care, smart cities and energy distribution networks [2-4]. Such systems have dynamic sensing and regulation based on predictive decision strategies that lead to more efficient and intellectually developed infrastructures. This extensive deployment of CPS creates higher connectivity that exposes these systems to numerous cyber risks as well as security breaches [5, 6].

Higher complexity within CPS environments results in expanded risk areas so cyber intrusions have increased rapidly. A series of cyberattacks including probing along with user-to-root exploits and remote-to-local attacks as well as Denial of Service (DoS) and Distributed Denial of Service (DDoS attacks have demonstrated high disruptiveness in their nature [7, 8]. These attacks take advantage of network communication shortcomings to stop systems by manipulating

bandwidth limits into service hindrances and corrupting data systems [9, 10]. Because CPS connect to each other, the infrastructure suffers major operational and economic damage from localized attacks which spread throughout the entire network [11].

Intrusion Detection Systems (IDS) serve as deployed tools in many CPS applications to handle these risks [12]. Network pattern analysis and malicious activity recognition and warning generation are features built into IDS tools which serve system administrators. The effectiveness of signature-based and rule-based IDS decreases when they operate in dynamic or evolving cyber systems especially when facing unknown threats [13, 14]. Zero-day attacks and new threat variants remain undetectable to IDS tools because their limited generalization capabilities make them unable to recognize unknown threats.

CPS environments create considerable flows of real-time data whose relationships depend on time, along with contextual aspects [15]. Systems require proper pattern capturing and analysis techniques to differentiate between standard activities and security threats. The complex nature of CPS exceeds the analytical capacity of shallow algorithms and current models, leading to deterioration of detection performance and more misclassifications [16-19]. The lack of data analysis precision has led to an increasing adoption of superior data-specific techniques that implement machine learning (ML) and deep learning (DL) approaches.

Effective digital protection in CPS is not only a technical specification but also a prerequisite that guarantees the security of critical infrastructure functioning. Hence, there is an essential need for a smart and scalable CPS environment defensive mechanism.

1.1 Contribution of the research

Even with this rapid progress, the existing IDS tools used in CPS settings are characterized by limited adaptability, false-positive rates, and poor temporal modeling, rendering them ineffective against zero-day and evolving attacks. These constraints become more important as CPS experience more advanced attacks like control-signal interference, sensor information corruption, and simultaneous network assaults, all of which demonstrate the incapacity of traditional IDS systems to guarantee dependable real-time security. Motivated by the above mentioned challenges, the study presents the following major findings and solutions to mitigate the growing challenges that safeguard CPS against emerging cyber threats:

1. A DL-based intrusion detection framework is introduced, which employs Bi-GRU architecture to process both forward and backward sequence temporal patterns for enhancing threat classification outcomes.
2. The study utilizes the NSL-KDD dataset with a comprehensive preprocessing pipeline that addresses the problems of data normalization and imbalance to generate high- quality training and evaluation data.
3. The system exhibits strong detection abilities for various CPS threats, as demonstrated through performance metric validation utilising accuracy, precision, recall and F1-score measures with specificity.

1.2 Paper organization

The study is organized in the following manner: Section 2 encompasses a thorough literature review on security in CPS environments. Section 3 presents the dataset characteristics, data pre-processing and the suggested Bi-GRU architecture. Section 4 includes analysis of experimental design along with evaluation outcomes and DL method comparison. At last, Section 5 wraps up the paper with valuable insights and provides the perspective of future research areas.

2. RELATED WORKS

Anusha et al. [20] presented a DL-based CNN model to identify cyber threats in IoT-based CPS. Their study discussed the limitations of the current Support Vector Machine (SVM) models, which cannot cope with the dynamic nature of cyber-attacks because they heavily depend on the historical data. The suggested CNN model exhibited better detection of cyber-attacks under different classification assessment metrics, compared to earlier models. Nevertheless, the recommended model has a comparatively high rate of false positives, which reduces its validity in real-world CPS settings where large numbers of false alerts may disrupt the normal operation of the system.

Abdullahi et al. [21] examined the application of the Extreme Gradient Boosting (XGBoost) and Long Short-Term Memory (LSTM) frameworks to detect attacks in CPS. They validated their approach on the basis of several datasets, such as the gas pipeline industrial control system dataset, NetML-2020, and the IoT-23 datasets that comprised a variety of cyberattacks. The experimental results showed that XGBoost and LSTM performed better than the classical algorithms, such as SVM and artificial neural networks (ANN), in all the performance metrics. One drawback of this work is that it fails to explain the performance of these models in the context of zero-day attacks or adversarial inputs.

Sharma et al. [22] designed a lightweight CNN-Bidirectional LSTM network to recognize DDoS attacks in smart healthcare networks. Their strategy used CNNs to classify network traffic as benign or malicious. The implemented algorithm used a batch size of 500, 20 epochs, 25 classes, with ReLU and softmax activation functions, 4 convolutional layers with maximum pooling, and a dense layer at the end. Although the architecture demonstrates potential in resource-constrained settings, the robustness of the model against advanced evasion strategies has not been extensively discussed in the study.

Alzahrani et al. [23] developed an enhanced Wireless Medical CPS based on ML techniques to address security concerns in healthcare networks. The system included three fundamental components, namely communication and monitoring, computational safety, and dynamic planning and resource administration. The patient-focused architecture retained the end-user smartphone authority on data interaction accessibility. The empirical investigation showed that the recommended system achieved an accuracy of 92%, with a minimal computation time of about 13 seconds and lower error rates against different threats. Nevertheless, the moderated accuracy of the recommended approach raises concerns about its generalization and detection.

Javed et al. [24] developed a Graph Attention Network (GAN) approach to identify persistent attacks on industrial IoT to protect CPS. The study utilised masked self-attentional layers in their approach to achieve multi-dimensional behavioral features that would be missed by conventional

methods of the DL technology. The analysis showed that the GAN could identify the malicious activities of the DAPT2020 malware dataset with 96.97% accuracy and process the Edge I-IoT dataset with 95.97% accuracy in 20.56 and 21.65 seconds, respectively. Performance analysis revealed that there were significant operational benefits relative to standard machine learning processes in I-IoT assisted CPS. Meanwhile the significant prediction times may limit the use of approach where a solution requires urgent danger recognition.

Bashar et al. [25] introduced a DL method for network threat recognition by using the multilayer LSTM network. Their architecture design focused on creating multiple levels which would optimize performance while maintaining stability during binary and multiclass classification operations. Experimental tests proved that the suggested model achieved outstanding results by delivering 95% binary classification accuracy together with 96% multiclass classification accuracy. The real-time detection of threats in high-speed networks using their method becomes complicated because stacked LSTM layers present heavy computational demands.

Mohi-ud-din et al. [26] developed an attack control framework that uses MLP to boost security levels in CPS environments. Their study focused on fixing the gaps present in traditional digital defense systems and network protocols that protect information inside CPS. The comparison showed that the recommended method delivered higher accuracy compared to Bayes Naive Gaussian and SVM and logistic regression by reaching 99.52% accuracy. Nonetheless, the research does not comprehensively explore the method's efficiency under the resource constraints typical in many CPS deployments.

Wang et al. [27] developed KD-TCNN as a Knowledge Distillation model that utilizes Triplet CNN to both enhance detection anomalies and decrease processing load for industry CPS applications. The researchers implemented a strong model loss function along with K-fold cross training as a new neural network training method to achieve stable results and accurate detection. The framework has been experimented using NSL-KDD and CIC IDS2017 benchmark datasets yielding higher performance than standard DL systems and existing state-of-the-art models. However, the dimensional reduction size-reduced the computation needs and achieved 0.4% of performance loss creating a model that is highly optimized to the IoT hardware constraints.

Akinsola et al. [28] utilised various DL algorithms to mitigate DDoS attacks on CPS environments by applying artificial intelligence methods to neutralize the attacks. They used CNN, LSTM and Gated Recurrent Units (GRU) in their method to track and identify incoming attacks. The findings showed that LSTM outperforms with 99.92% accuracy, 0.0037 loss function and a 0.026 RMSE at training, which is consistent at the testing stage (99.92% accuracy, 0.0058 loss function and 0.0278 RMSE). The comparative analysis proved the effectiveness of LSTM in comparison with other deep learning algorithms in DDoS attack mitigation. However, even though the model is highly accurate, it exhibits some overfitting, which limits its ability to be resistant to unobservable or changing patterns of DDoS attacks.

AlZubi et al. [29] presented a cognitive ML-assisted threat recognition framework to support secure medical information sharing in CPS. This patient-centric solution focused on ensuring the information was safe on trusted devices such as smartphones without losing sharing control. The system supported the aggregation and cloud storage of healthcare data, with ML models forecasting cyber-attack patterns to support healthcare experts. The Extreme Learning Machine (ELM), among others, demonstrated high performance and showed a threat recognition rate of 96.5%, a precision level of 98.2% and a delay of 21.3%, and a communication cost of 18.9% lower than the present methods. Nevertheless, the paper does not discuss the performance of the model against zero-day attacks or adversarial inputs that are intended to escape neural network detection.

Table 1 summarizes recent research on DL and ML-based intrusion detection and cyber-attack mitigation techniques for CPS and IoT environments, highlighting their advantages and limitations.

Table 1. Overview of related literatures

S. No.	Author & Year	Algorithm	Findings Obtained	Advantage	Limitation
1	Anusha et al. [20]	CNN	Improved accuracy, precision, recall, and F1-score compared to SVM models	Compared to SVM model, the recommended CNN algorithm attained good detection performance	Obtained high False Positive Rate
2	Abdullahi et al. [21]	Used XGBoost and LSTM	Outperformed SVM and ANN across various performance measures	Superior performance on multiple datasets (gas pipeline, NetML-2020, IoT-23)	Does not address performance under zero-day attack scenarios or with adversarial inputs
3	Sharma et al. [22]	Hybrid CNN-Bidirectional LSTM	Effective DDoS attack recognition	Lightweight model suitable for resource-constrained smart healthcare networks	Does not extensively address resilience against sophisticated evasion techniques
4	Alzahrani et al. [23]	ML methods	Accuracy: 92%, Computation time: 13 seconds, reduced error metrics	Patient-centric framework with user control over data exchange in wireless medical CPS	Attained moderate accuracy
5	Javed et al. [24]	Graph Attention Network (GAN)	Accuracy: 96.97% (DAPT2020 dataset), 95.97% (Edge I-IoT dataset)	Multi-dimensional behavioral feature extraction	Prediction times could restrict usage when immediate threat detection is essential
6	Bashar et al. [25]	Multilayer LSTM	Binary classification accuracy: 95%, Multiclass classification accuracy: 96%	Optimized performance with stability in classification operations	Doesn't address the recommended model's computational complexity
7	Mohi-ud-	MLP	Accuracy: 99.52%	Superior accuracy for	Does not comprehensively

	din et al. [26]		(outperformed Naive Bayes, SVM, and logistic regression)	attack control in CPS environments	explore efficiency under resource constraints typical in CPS deployments
8	Wang et al. [27]	KD-TCNN (Knowledge Distillation with Triplet CNN)	Better performance than typical DL systems	Enhanced anomaly detection with decreased processing load	Minor performance drop (0.4%) due to dimensional reduction
9	Akinsola et al. [28]	CNN, LSTM, and GRU	LSTM: 99.92% accuracy (training & testing), Loss: 0.0037 (training), 0.0058 (testing), RMSE: 0.026 (training), 0.0278 (testing)	LSTM demonstrated superior performance for DDoS attack mitigation in CPS	Suggested model overfitting concern
10	AlZubi et al. [29]	Extreme Learning Machine (ELM)	Threat recognition rate: 96.5%, Accuracy: 98.2%, Delay reduced by 21.3%, Communication cost reduced by 18.9%	Patient-centric solution with user control; facilitates healthcare data aggregation and cloud storage	Potential scalability issues

3. PROPOSED METHODOLOGY

Figure 1 illustrates the schematic representation of the recommended framework. The suggested design includes the following key stages: 1) Data Collection, in which the NSL-KDD data set is utilized as the primary source of network traffic records; 2) Data Preprocessing, where the encoding categorical features and normalization techniques are applied to ensure consistency across the input data; 3) Feature Extraction using BiGRU, where Bi-GRU network is used to extract both forward and backward relationships in the data; and 4) Classification of Attack, in which the learned features are used to accurately determine the relationship between the normal data and various types of malicious traffic, followed by 5) Result Analysis and Interpretation, which assess the model's effectiveness utilising standard measures for comprehensive evaluation.

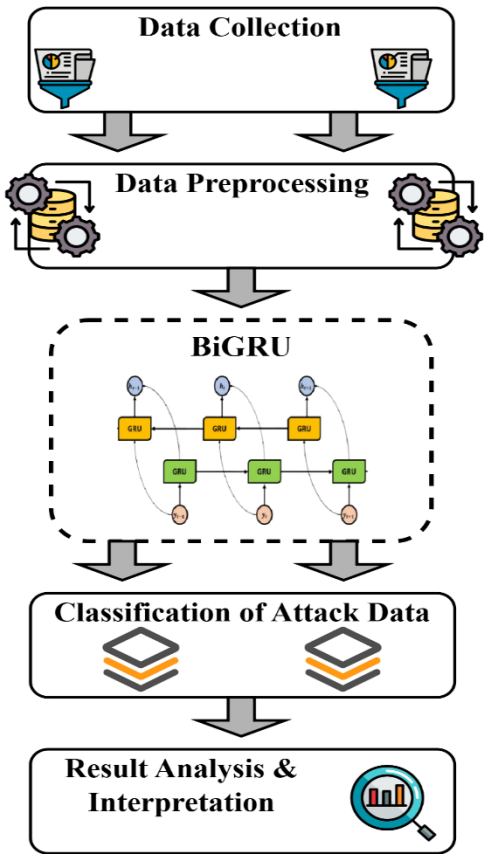

Figure 1. Architecture of the suggested framework

3.1 Materials and methods

The research uses the NSL-KDD, a proven benchmark dataset accessible on Kaggle, to assess the performance of the developed intrusion detection system [30]. The dataset accommodates 148,517 records with 41 network traffic features outlining diverse connection attributes that cover protocol type to service duration and data transfer volume. This record set consists of several detailed attributes that allow experts to conduct full network monitoring to determine normal and attacking behavior [31]. The records are divided into two types: normal traffic and threat instances, where threats are divided into DoS, Probe, Remote to Local (R2L) and User to Root (U2R) [32]. The NSL-KDD format, along with its size balance, has been found helpful in model development and comparison in intrusion detection since it provides stable experimental data.

Table 2. Overview of data categories in NSL-KDD dataset

S. No.	Dataset Description	Data Count
1	Total Number of Data Records	148,517
2	Training Dataset	125,973
3	Testing Dataset	22,544
4	Number of Features	41

Figure 2. Data distribution for training, testing, and validation in the NSL-KDD dataset

Table 2 displays a summary of the data distribution and the number of features in the dataset, whereas Figure 2 shows how data are distributed for training, testing, and validation process.

3.2 Data pre-processing technique

Several crucial preprocessing steps are applied to the data for improving consistency and data quality. The categorical features like protocol_type, service and flag are transformed into numerical format through the one-hot encoding method. Each unique category in a dataset receives binary columns through this method to let algorithms read categorical data without unintentional hierarchy structures. Min-Max normalization becomes the next step for processing the numerical dataset features. The dataset possesses measurement units of different magnitudes, particularly the duration and src_bytes and dst_bytes attributes, which normalization transforms into values ranging from 0 to 1. The normalization process helps decrease feature magnitude disparities that let every input provide a similar value during model training. The Min-Max normalization requires this calculation for its operation:

$$X' = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (1)$$

The equation includes original feature X alongside its minimum value X_{min} and maximum value X_{max} . The conversion methods generate numerically homogeneous data for the successful analytical processing.

3.3 Model design

The BiGRU model developed by this research helps detect various network threats in CPS through an efficient intrusion detection technique. The following sections describes the BiGRU model architecture and details its operational mechanisms which are employed throughout this investigation.

3.3.1 BiGRU

The Bi-GRU model belongs to recurrent neural networks (RNNs) and serves as a temporal sequence manager to learn temporal connections within and beyond current time points. BiGRUs differ from typical RNNs because they process inputs sequentially, both forward and backward, thus achieving a better understanding of temporal sequences. The model contains dual GRU processing components which scan the data forward while another unit works in the reverse direction. The model incorporates the integrated outputs as an enhancement to its potential to learn more complicated temporal patterns to recognize anomalies and intrusions. The BiGRU architecture is depicted in Figure 3.

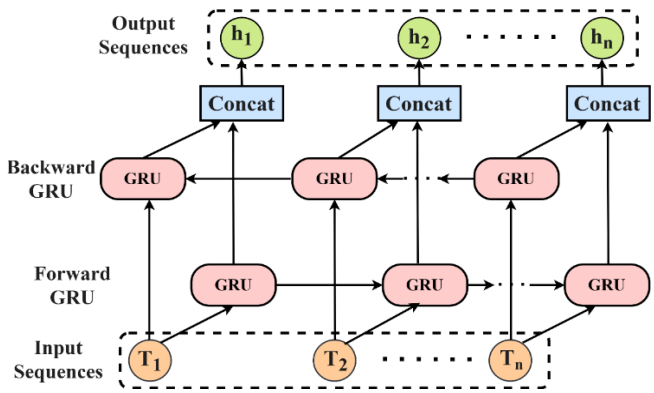

Figure 3. BI-GRU network architecture

GRU Cell Mechanics. BiGRU implements the GRU at its foundation, which represents an efficient LSTM-related unit. GRUs are more efficient in their information flow than LSTM networks in executing time steps and need fewer parameters. The GRU cell has two critical gating systems that act in a mutually exclusive way:

1. Update Gate (z_t): Decides how much of the past data needs to be retained and how much of the new information should be incorporated.
2. Reset Gate (r_t): This parameter determines how much old information should be forgotten when the current output is being computed.

These gates dynamically regulate the passage of information, allowing the model to selectively focus on relevant patterns while discarding noise and redundancy. The model solves the issue of gradient disappearance that occurs when deep neural networks process extended sequence data. The GRU cell performs its internal operations based on these subsequent expressions:

The computation for the update gate requires the following expression:

$$z_t = \sigma(W^z x_t + U^z h_{t-1} + b^z) \quad (2)$$

The reset gate is denoted using,

$$r_t = \sigma(W^r x_t + U^r h_{t-1} + b^r) \quad (3)$$

The candidate activation, representing the intermediate memory content, is expressed as:

$$\hat{h}t = \tanh(W x_t + U(r_t \odot h_{t-1}) + b) \quad (4)$$

The last activation which represents the hidden state transforms according to the following equation:

$$h_t = (1 - z_t) \odot h_{t-1} + z_t \odot \hat{h}t \quad (5)$$

The equations include x_t as input and h_{t-1} from previous step and use σ as the sigmoid function along with $\odot$ for element-wise multiplication and W, U, b for weight matrices and bias terms.

The GRU unit uses its gating mechanism to automatically maintain proper short-term and long-term dependency relationships over time as a means of dealing with unpredictable network dynamics.

Output Layer. Both the forward and backward outputs of processed input sequences are concatenated at the BiGRU before dense layers classify them. The dense layers receive learned temporal features as inputs and transform them into category assignments.

The output sequences are classified into one of several attack types or normal traffic through an application of the softmax activation function at the final stage. The dual-context approach in the model design allows it to detect complex patterns, which boosts its accuracy and defensive capabilities in detecting threats in CPS.

4. RESULTS AND DISCUSSION

4.1 Implementation details

The recommended methodology conducted operations

through Python 3.8 alongside dependencies NumPy and Pandas and libraries Matplotlib and Seaborn and Scikit-learn. The TensorFlow and Keras frameworks carried out the deep learning operations during the execution. The high-end workstation with an Intel Core i7 CPU (3.4 GHz) speed combined with 16 GB of RAM and an NVIDIA RTX 3060 GPU allowed for fast model training and validation processes that reduced computational delays. Table 3 summarizes the key hyperparameters and their values used for training the recommended BiGRU model to optimize performance.

Table 3. Hyperparameters utilized for training the suggested model

S. No.	Hyperparameter	Description / Value
1	Epochs Count	80
2	Batch Size	64
3	Optimizer	Adam
4	Learning Rate	0.001
5	Activation Function (Output)	Softmax
6	Dropout Rate	0.3
7	Loss Function	Categorical Cross-Entropy

During the training phase, the BiGRU model was configured with the listed hyperparameters to optimize learning. Early stopping technique was used to prevent overfitting and assure the algorithm generalizes effectively to unseen data.

4.2 Performance metrics

The effectiveness of the suggested approach was measured by applying accuracy, precision, recall, specificity together with F1-score evaluation indicators. A comprehensive set of performance indicators allows complete evaluation of how well the model performs in attack traffic detection. During training the model utilized early stopping to prevent overfitting, thus ensuring algorithm performance on new test data. All formulas for the evaluation measure calculations appear in Table 4.

Table 4. Mathematical representation for the evaluation measures

S. No.	Evaluation Measures	Numerical Representation
1	Accuracy	$\frac{TP+TN}{TP+TN+FP+FN}$
2	Recall	$\frac{\text{TP}}{\text{TP+FN}} \times 100$
3	Specificity	$\frac{TN}{TN+FP}$
4	Precision	$\frac{TN}{TP+FP}$
5	F1-Score	$2 * (\frac{Precison * Recall}{Precision + Recall})$

The analysis involved True Positive (TP) along with True Negative (TN) values and False Positive (FP) while False Negative (FN) cases also utilized.

4.3 Experimental findings

Table 5 presents a comparative analysis of various DL algorithms for intrusion recognition in CPS, based on key performance measures established in Table 4. The suggested model is substantially superior to the conventional DL methods, such as RNN, 1D CNN, LSTM, GRU, Bidirectional LSTM (BiLSTM). With a high classification accuracy of 98.47%, the suggested model exhibits a greater ability to detect and classify network-based attacks. From Table 5, it is evident that the excellent results in all the measures highlight its strength, effectiveness, and dependability in protecting CPS environments against the changing cyber threats.

Figure 4, on the other hand, contrasts the performance of specific DL models in cyber-attack detection in CPS settings. Each of the evaluation metrics indicates the superiority of the recommended Bi-GRU model over other models to establish its remarkable threat recognition capacity.

Table 5. Comparative performance of models in cyber threat classification

Algorithms	Accuracy (%)	Precision (%)	Recall (%)	Specificity (%)	F1-score (%)
LSTM	94.5	93.8	92.3	93.2	93.5
GRU	95.7	94.8	94.2	94.5	94.6
1D CNN	92.8	91.7	90.9	91.3	91.5
BiLSTM	93.9	92.2	91.6	92.8	93.0
Proposed Model	98.47	98.2	97.0	97.5	98.9

Table 6. Computational parameters for distinct models in both CPU and GPU

Algorithm	Computational Performance (CPU)				
	Inference Time (s)	Memory (MB)	FLOPs (×10⁶)	Computation Time (s)	No. of Parameters
LSTM	0.185	28.4	88	10.42	402,110
GRU	0.162	25.7	76	9.31	348,920
1D-CNN	0.141	23.5	65	8.12	221,640
BiLSTM	0.214	32.1	112	11.96	489,530
Proposed BiGRU	**0.118**	**21.3**	**59**	**7.84**	**274,310**
Algorithm	**Computational Performance (GPU)**				
	Inference Time (s)	**Memory (MB)**	**FLOPs (×10⁶)**	**Computation Time (s)**	**No. of Parameters**
LSTM	0.134	26.9	84	7.86	402,110
GRU	0.109	24.3	72	6.51	348,920
1D-CNN	0.087	22.7	61	5.47	221,640
BiLSTM	0.153	29.8	107	8.72	489,530
Proposed BiGRU	**0.073**	**20.8**	**54**	**4.99**	**274,310**

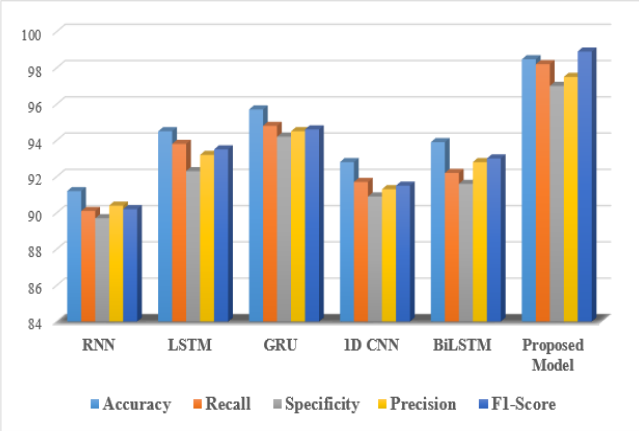

Figure 4. Comparison between different algorithms that detect attacks

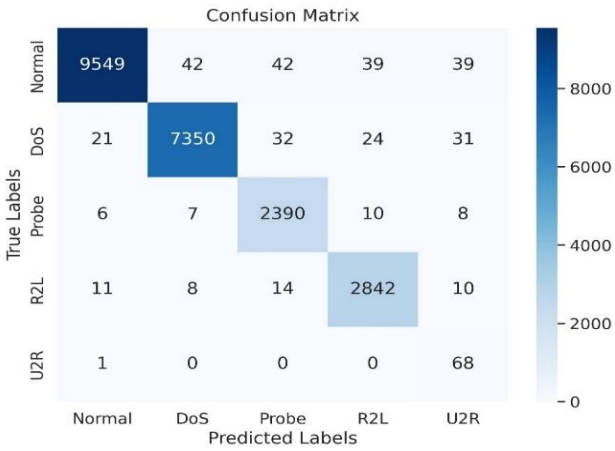

Figure 5. Confusion matrix for the suggested network

Figure 5 presents a confusion matrix of the suggested algorithm indicating high classification accuracy across all categories with particular excellence of the suggested algorithm in detecting both Normal and DoS attacks. Figure 6 demonstrates that training and testing levels of accuracy measured across epochs smoothly improve without showing any signs of overfitting in the system. Figure 7 demonstrates the ROC curve which proves that the algorithm shows exceptional capability in detecting normal and malicious traffic, thus affirming its strength in CPS intrusion detection.

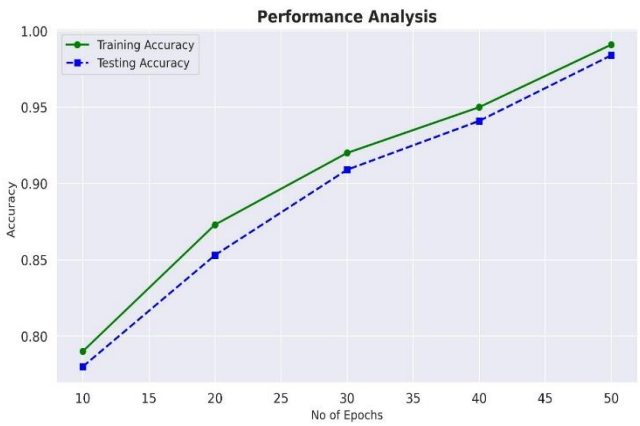

Figure 6. Training and testing accuracy over epochs for the suggested method

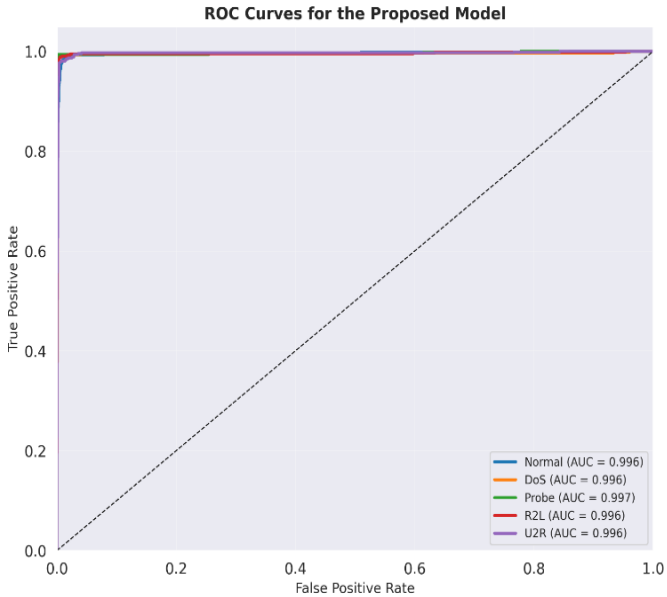

Figure 7. Receiver Operating Characteristic (ROC) curve depicting multi-class classification performance

4.4 Computational performance analysis

A computational performance study was carried out to evaluate the feasibility of implementing the recommended intrusion detection framework in real-time CPS settings. The analysis included inference speed, memory usage, overall computation time, and the count of trainable parameters in various baseline models. Tests were performed on both CPU-based and GPU-accelerated systems to obtain a complete performance comparison. Table 6 present the computational properties of different deep learning architectures utilized in intrusion detection.

The suggested architecture, as indicated in Table 6, consistently needs fewer computational resources than other deep learning-based IDS frameworks. It has the shortest inference time and memory consumption and has a much lower FLOP count. These findings support the model in real-time CPS settings, especially in edge and embedded applications where the computational efficiency is required.

4.5 Statistical validation process

A Wilcoxon signed-rank test was performed to confirm whether the performance gains achieved by the suggested BiGRU model were statistically significant. This non-parametric paired test indicates whether the differences in the observed accuracy between the recommended approach and other models are consistent and not due to random variation. The test was conducted with the accuracy scores based on five independent runs on the NSL-KDD dataset. The resulting p-values for each model comparison are presented in Figure 8.

Based on Figure 8, it is apparent that the recommended BiGRU model yields the lowest p-value among all the compared IDS models. This is a clear indication that its performance gains are statistically significant. The low p-values in all comparisons verify that BiGRU model is providing a consistent and repeatable gain and not a random variation. Altogether, the statistical test confirms the excellence of the recommended approach in comparison to the current baseline models.

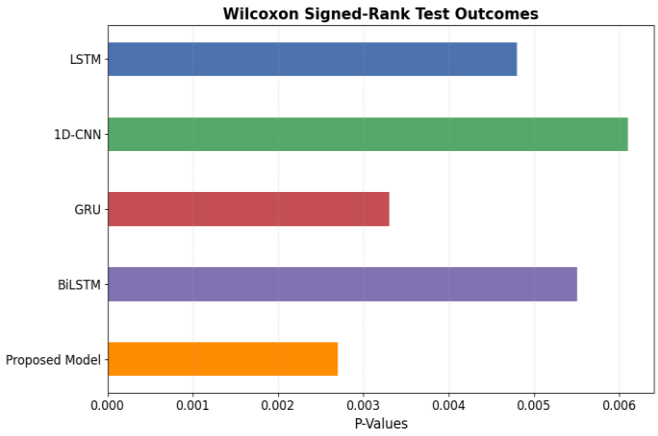

Figure 8. Wilcoxon signed-rank statistical comparison for different models

4.6 Results discussion

The overall results indicate that the Suggested BiGRU-based IDS provides a consistent enhancement compared to current DL models. The suggested framework has the advantage to include both forward and backward temporal dependencies, which adds to its high-accuracy level of 98.47%, indicating high recognition power in all types of attacks. The confusion matrix also supports the stable classification behavior, especially between the Normal and DoS classes, in which the misclassification is low. Other performance measures like precision, recall, specificity, and F1-score indicate similar results, proving that the model does not over-fit and still maintains a good level of generalization. The ROC curve substantiates the strength of the highly separable normal and malicious traffic classifier. The computational analysis also demonstrates the applicability of the model to real-time CPS functions, with low inference time and low resource usage. The statistical validation by Wilcoxon test proves that the improvement of performance is not some random increase, which indicates great reliability of the suggested framework.

5. CONCLUSION

The research establishes data security and privacy improvement in CPS as an essential matter which deep learning advances effectively address. When connected CPS infrastructures link with a regulatory framework of digital utilities they become strong security targets for sophisticated cyber attacks that lead to critical service failures and the compromising of private data. The study uses NSL-KDD data to develop a robust intrusion detection framework which implements the BI-GRU model. The BI-GRU model demonstrates ability to detect both forward and backward sequence dependencies which leads to 98.47% classification accuracy. Numerous evaluation measures with precision and recall and specificity and F1-score indicate that the model demonstrates dependable recognition for multiple cyber-attack patterns. The suggested approach proves suitable for real-time CPS deployment, as it offers excellent generalization and minimizes false positives. The developed security system further design advanced defensive systems that secure vulnerable infrastructure components. This exploration provides future directions to create adaptive system models that address new attack patterns in dynamic CPS operating environments. Nevertheless, the research is restricted by the absence of real-life validation data, that can influence the applicability to dynamic CPS settings. Future research may include the implementation of the model on real-world CPS traffic, the introduction of federated learning to train a privacy-aware model, and the use of explainable AI methods like SHAP or LIME to enhance model interpretability.

REFERENCES

[1] Hamzah, M., Islam, M.M., Hassan, S., Akhtar, M.N., Ferdous, M.J., Jasser, M.B., Mohamed, A.W. (2023). Distributed control of cyber physical system on various domains: A critical review. Systems, 11(4): 208. https://doi.org/10.3390/systems11040208

[2] Chen, F.L., Tang, Y.Q., Wang, C.L., Huang, J., Huang, C., Xie, D. (2022). Medical cyber–physical systems: A solution to smart health and the state of the art. IEEE Transactions on Computational Social Systems, 9(5): 1359-1386. https://doi.org/10.1109/TCSS.2021.3122807

[3] Mishra, A., Jha, A.V., Appasani, B., Ray, A.K., Gupta, D.K., Ghazali, A.N. (2023). Emerging technologies and design aspects of next generation cyber physical system with a smart city application perspective. International Journal of System Assurance Engineering and Management, 14(Suppl 3): 699-721. https://doi.org/10.1007/s13198-021-01523-y

[4] Ryalat, M., ElMoaqet, H., AlFaouri, M. (2023). Design of a smart factory based on cyber-physical systems and Internet of Things towards industry 4.0. Applied Sciences, 13(4): 2156. https://doi.org/10.3390/app13042156

[5] Verma, R. (2022). Smart City healthcare cyber physical system: Characteristics, technologies and challenges. Wireless Personal Communications, 122: 1413-1433. https://doi.org/10.1007/s11277-021-08955-6

[6] Wang, B.C., Zheng, P., Yin, Y., Shih, A., Wang, L.H. (2022). Toward human-centric smart manufacturing: A human-cyber-physical systems (HCPS) perspective. Journal of Manufacturing Systems, 63: 471-490. https://doi.org/10.1016/j.jmsy.2022.05.005

[7] Jbair, M., Ahmad, B., Maple, C., Harrison, R. (2022). Threat modelling for industrial cyber physical systems in the era of smart manufacturing. Computers in Industry, 137: 103611. https://doi.org/10.1016/j.compind.2022.103611

[8] El-Kady, A.H., Halim, S., El-Halwagi, M.M., Khan, F. (2023). Analysis of safety and security challenges and opportunities related to cyber-physical systems. Process Safety and Environmental Protection, 173: 384-413. https://doi.org/10.1016/j.psep.2023.03.012

[9] SaravanaKumar, G., Kalpana, P., Murthy, G.V., Gadekallu, T.R., Salhi, A., Quasim, M.T. (2025). Beetle-optimized hybrid ensemble for multi-attack classification in VANETs. Transactions on Emerging Telecommunications Technologies, 36(10): e70281. https://doi.org/10.1002/ett.70281

[10] Aruna, E., Sahayadhas, A., Kalpana, P., Khan, S.B., Quasim, M.T., Almusharrf, A. (2025). A web 3.0 integrated blockchain enabled access system augmented by meta-heuristic cognitive learning framework for mitigating threats in IoT enabled consumer electronic

devices. IEEE Transactions on Consumer Electronics, 71(1): 1201-1210. https://doi.org/10.1109/TCE.2025.3553741

[11] Sahin, M.E., Tawalbeh, L., Muheidat, F. (2022). The security concerns on cyber-physical systems and potential risks analysis using machine learning. Procedia Computer Science, 201: 527-534. https://doi.org/10.1016/j.procs.2022.03.068

[12] Alohali, M.A., Al-Wesabi, F.N., Hilal, A.M., Goel, S., Gupta, D., Khanna, A. (2022). Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment. Cognitive Neurodynamics, 16: 1045-1057. https://doi.org/10.1007/s11571-022-09780-8

[13] Kalpana, P., Tappari, S., Smitha, L., Madhavi, D., Naresh, K. Vijayalakshmi, M. (2025). A novel end-to-end privacy preserving deep Aquila feed forward networks on healthcare 4.0 environment. Discover Internet of Things, 5: 65. https://doi.org/10.1007/s43926-025-00157-x

[14] Zoppi, T., Gharib, M., Atif, M., Bondavalli, A. (2021). Meta-learning to improve unsupervised intrusion detection in cyber-physical systems. ACM Transactions on Cyber-Physical Systems (TCPS), 5(4): 1-27. https://doi.org/10.1145/3467470

[15] Thakur, S., Chakraborty, A., De, R., Kumar, N., Sarkar, R. (2021). Intrusion detection in cyber-physical systems using a generic and domain specific deep autoencoder model. Computers & Electrical Engineering, 91: 107044. https://doi.org/10.1016/j.compeleceng.2021.107044

[16] Alqaralleh, B.A.Y., Aldhaban, F., AlQarallehs, E.A., Al-Omari, A.H. (2022). Optimal machine learning enabled intrusion detection in cyber-physical system environment. Computers, Materials & Continua, 72(3): 4691-4707. https://doi.org/10.32604/cmc.2022.026556

[17] 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

[18] Hao, W.J., Yang, T., Yang, Q. (2023). Hybrid statistical-machine learning for real-time anomaly detection in industrial cyber–physical systems. IEEE Transactions on Automation Science and Engineering, 20(1): 32-46. https://doi.org/10.1109/TASE.2021.3073396

[19] Kim, S., Park, K.J., Lu, C. (2022). A survey on network security for cyber–physical systems: From threats to resilient design. IEEE Communications Surveys & Tutorials, 24(3): 1534-1573. https://doi.org/10.1109/COMST.2022.3187531

[20] Anusha, G., Baigmohammad, G. Mageswari, U. (2024). Detection of cyber attacks on IoT based cyber physical systems. MATEC Web of Conferences, 392: 01166. https://doi.org/10.1051/matecconf/202439201166

[21] Abdullahi, M., Alhussian, H., Aziz, N., Abdulkadir, S.J., Alwadain, A., Muazu, A.A. (2024). Comparison and investigation of AI-based approaches for cyberattack detection in cyber-physical systems. IEEE Access, 12: 31988-32004. https://doi.org/10.1109/ACCESS.2024.3370436

[22] Sharma, A., Rani, S., Shah, S.H., Sharma, R., Yu, F., Hassan, M.M. (2023). An efficient hybrid deep learning model for denial of service detection in cyber physical systems. IEEE Transactions on Network Science and Engineering, 10(5): 2419-2428. https://doi.org/10.1109/TNSE.2023.3273301

[23] Alzahrani, A., Alshehri, M., AlGhamdi, R., Sharma, S.K. (2023). Improved wireless medical cyber-physical system (IWMCPS) based on machine learning. Healthcare, 11(3): 384. https://doi.org/10.3390/healthcare11030384

[24] Javed, S.H., Ahmad, M.B., Asif, M., Akram, W., Mahmood, K., Das, A.K. (2023). APT adversarial defence mechanism for industrial IoT enabled cyber-physical system. IEEE Access, 11: 74000-74020. https://doi.org/10.1109/ACCESS.2023.3291599

[25] Bashar, G.M.H., Kashem, M.A., Paul, L.C. (2022). Intrusion detection for cyber-physical security system using long short-term memory model. Scientific Programming, 2022(1): 6172362. https://doi.org/10.1155/2022/6172362

[26] Mohi-ud-din, G., Liu, Z.Q., Zheng, J.B., Wang, S.F., Zeng, X.Y., Lai, Z.Z., Lin, Z.J., Asim, M. (2022). A novel learning-based attack detection system for enhancing security in cyber-physical environments. Computer Science and Technology, 1(1): 16-26. https://doi.org/10.57237/j.cst.2022.01.003

[27] Wang, Z.D., Li, Z.Y., He, D.J., Chan, S. (2022). A lightweight approach for network intrusion detection in industrial cyber-physical systems based on knowledge distillation and deep metric learning. Expert Systems with Applications, 206: 117671. https://doi.org/10.1016/j.eswa.2022.117671

[28] Akinsola, J.E.T., Abimbola, R.O., Adeagbo, M.A., Awoseyi, A.A., Onipede, F.O., Yusuf, A.A. (2022). Application of artificial intelligence for DDoS attack detection and prevention on cyber physical systems using deep learning. In Internet of Things and Cyber Physical Systems, pp. 83-126.

[29] AlZubi, A.A., Al-Maitah, M., Alarifi, A. (2021). Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques. Soft Computing, 25: 12319-12332. https://doi.org/10.1007/s00500-021-05926-8

[30] Nasir, Z.U.I., Iqbal, A., Qureshi, H.K. (2024). Securing cyber-physical systems: A decentralized framework for collaborative intrusion detection with privacy preservation. IEEE Transactions on Industrial Cyber-Physical Systems, 2: 303-311. https://doi.org/10.1109/TICPS.2024.3425794

[31] Archana, G., Goyal, R., Madan Kumar, K.M.V. (2025). Blockchain enabled light weight encryption scheme for IoT-Edge devices applied for smart medical image transmission. International Journal of Safety and Security Engineering, 15(6): 1219-1228. https://doi.org/10.18280/ijsse.150612

[32] Anjali, T., Goyal, R., Balaji, G.N. (2025). Enhanced gated sway network and hybrid Henon encryption for secured VANET communication. International Journal of Safety and Security Engineering, 15(3): 543-553. https://doi.org/10.18280/ijsse.150313