SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Cyber-Physical System Security Using AI-Based Intrusion Detection And Predictive Threat Intelligence Models

Rahul Pradhan[1], Balla Satyanarayana[2], Ambika P[3], Talla Prashanthi[4], Dr. M. V. Rajesh[5], Shailesh Kulkarni[6], Tanya Singh[7]

[1]Department of Computer Engineering & Applications, GLA, University, Mathura, Email: rahul.pradhan@gla.ac.in
[2]Associate Professor, Department of Civil Engineering, Pragati Engineering College, ADB Road, Surampalem, NearPeddapuram, Kakinada District, Andhra Pradesh, India - 533437. Email: snballa1670@gmail.com
[3]Assistant Professor, Department of Commerce, Meenakshi College of Arts and Science, Meenakshi Academy of Higher Education and Research, Email: ambikap@maher.ac.in
[4]Assistant Professor, Departmentof Information Technology, Vardhaman College of Engineering, Shamshabad, Hyderabad, India - 501 218, Email: prashanthi1711@vardhaman.org
[5]Associate Professor, Department of Information Technology, Aditya University, Surampalem, Andhra Pradesh, Pin 533437, Email: assocdean_se@adityauniversity.in
[6]Professor, E&TC Engineering, Vishwakarma Institute of Technology, Pune, Maharashtra, 411037, Email: shailesh.kulkarni@vit.edu
[7]School of Engineering &Technology,Noida international University, Uttar Pradesh 203201, India,
Email: dean.academics@niu.edu.in

Abstract

A new concept of Cyber-Physical Systems (CPS) has become an essential element of the current industrial automation, intelligent healthcare, intelligent transportation, and intelligent grid systems. Nevertheless, with the growing connection of physical devices to communication networks, vulnerability to advanced cyber threats, such as distributed denial of service attacks, malware injection and data manipulation, and unauthorized access have greatly increased. Traditional intrusion detection tools have repeatedly been shown to offer few capabilities in monitoring dynamic attacks and zero-day attacks in the dynamic CPS environment. In this paper, an AIbased intrusion detection and predictive threat intelligence taskforce is suggested to boost CPS cybersecurity. The proposed framework incorporates combination of a hybrid Convolutional neural network- Long short term memory (CNN- LSTM) model and predictive threat intelligence to enhance accuracy of attack detection and proactive threat prediction. The CNN component learns spatial traffic features and LSTM network learns temporal attack behaviors based on the CPS network traffic data. The CICIDS2017 dataset with various actual attack types was used to evaluate the experiment. The proposed framework obtained an intrusion detection accuracy of 97.2, precision of 96.8, recall of 96.1, F1-score of 96.4 and ROC-AUC score of 0.982. Comparison revealed high performance in comparison to traditional machine learning and stand-alone deep learning models. The proposed framework was statistically validated using 10-fold cross-validation to verify the strength and the generalization of the proposed framework. The designed predictive threat intelligence module also enhanced the proactive prediction of attacks and cybersecurity responsiveness on CPS infrastructures. The proposed framework offers an extensible and smart security implementation to next generation Cyber-Physical Systems.

Keywords: Cyber-Physical Systems, Intrusion Detection System, Deep Learning, CNN-LSTM, Predictive Threat Intelligence, CPS Security, Artificial Intelligence, Cybersecurity

1. Introduction

Cyber-Physical Systems (CPS) are systems incorporating computational intelligence, communication networks and physical infrastructures to aid self-monitoring, control and decision making in the contemporary industrial settings. Applications of CPS technologies should include smart manufacturing, healthcare systems, intelligent transportation, smart grids, and the Industrial Internet of Things (IIoT) (Awadallah et al., 2024; Khalaf et al., 2025). Though these interconnected systems enhance operational efficiency and ability to automate, major cybersecurity vulnerabilities are also created which can be exploited by malicious attackers. The attacks include cyberattacks of CPS infrastructures that can cause the loss of operations and data, as well as financial and physical losses. Examples of common attacks are distributed denial-of-service (DDoS), malware injection,

spoofing, phishing, botnet attacks, and unauthorized access attempts (Mao et al., 2021; Al-Quayed et al., 2024). The conventional intrusion detection systems largely depend on signature-based and rule-based designs, which do not tend to be effective to address unknown and dynamic cyber threats (Ndibe, 2025). Moreover, traditional systems tend to produce a large amount of false-positives and are poorly adapted to the dynamic CPS setting. The deep learning techniques and the Artificial Intelligence (AI) have become effective solutions in undertaking smart cybersecurity systems. Convolutional neural networks (CNNs), Recurrent neural networks (RNNs), as well as Long short-term memory (LSTM) networks, are deep learning architectures capable of learning complex patterns of attack behaviour and enhancing accuracy in intrusion detection (Shaik et al., 2025; Singh and Chandra, 2024). Nevertheless, the current research remains limited with limitations such as the ineffectiveness of the learning of the temporal aspect, deficiency of the predictive threat intelligence capacity, and the lack of real-time scalability (Kim et al., 2023; Zhang and Liu, 2024). In order to overcome these problems, this research offers an AI-supported intrusion detection and future predictive threat intelligence platform of Cyber-Physical System security. The intelligent attack classification and predictive cybersecurity analytics are based on a hybrid CNN-LSTM architecture proposed. The effectiveness of the proposed framework was demonstrated with the help of the experimental testing based on the dataset CICIDS2017. The key findings of this paper can be recapped as follows:

1. Creation of the AI-based intrusion detection system of CPS security.
2. Predictive threat intelligence mechanisms that can be incorporated to enable proactive attack prediction.
3. Training a hybrid CNN-LSTM model to learn a spatial-temporal feature.
4. Experimental analysis with the CICIDS2017 cybersecurity data.
5.Comparison with traditional machine learning and deep learning models.
6. Cross-validation validation with statistics.
7. Neural complexity assessment toward feasibility of its practical deployment.

The rest of the paper is presented in the following way. The related work is discussed in Section 2. The proposed methodology is shown in Section 3. The data and experimental design are outlined in section 4. The results and discussion are provided in section 5. Lastly, Section 6 will have a conclusion and will give future research directions.

2. Related Work

The fast development of Cyber-Physical Systems (CPS) and the Industrial Internet of Things (IIoT) infrastructures has heightened cybersecurity issues in industries. There are multiple machine learning and deep learning approaches that have been suggested by researchers to enhance intrusion detection efficiency and resilience to cyber-attack in CPS environments (Kim et al, 2023; Khalaf et al, 2025). Intrusion detection systems have been performed using traditional machine learning algorithms that include Support Vector Machine (SVM), Random Forest, Decision Tree and K-Nearest Neighbor (KNN). Even though these methods have been found to have reasonable performance, they tend to be limited in scale and poor feature extraction performance with high-dimensional CPS traffic data (Zhang and Liu, 2024; Rao and Smith, 2023). Intriguing research has been conducted on the deep learning methods of smart intrusion detection. Convolutional Neural Networks (CNNs) are excellent at identifying spatial attack features, whereas Long Short-Term Memory (LSTMs) networks can identify sequential and temporal attack patterns (Singh and Chandra, 2024; Akshya et al, 2025). The architectures of hybrid CNN-LSTM have further enhanced the performance of attack classification by learning spatial and temporal features. Some of the researchers have as well examined predictive threat intelligence processes to proactive cybersecurity analytics. Nevertheless, most of the existing models have a restricted real-time performance and lack of integration with deep learning-based intrusion detection systems (Oyedotun et al, 2025; Ding et al, 2019). Moreover, some of the works continue to use old-fashioned datasets like KDDCup99, which are not representative of case scenarios of a contemporary CPS attack. New databases like CICIDS2017 and ToN-IoT have now more realistic numbers due to cybersecurity traffic that can be used in intrusion detection studies (Al-Quayed et al, 2024).

Table 1. Comparative analysis of existing intrusion detection approaches				
Author	Method	Dataset	Accuracy (%)	Limitation
Al-Quayed et al, 2024.	SVM-Based IDS	NSL-KDD	89.4	Limited scalability
Oyedotun et al, 2025	Random Forest	UNSW-NB15	91.2	High false positives
Singh and Chandra, 2024	CNN Model	CICIDS2017	94.6	Weak temporal learning
Zhang and Liu, 2024	LSTM-Based IDS	ToN-IoT	95.1	Computational overhead
Khalaf et al, 2025	CNN-LSTM Hybrid	CICIDS2017	96.3	No threat prediction
Proposed Method	CNN-LSTM + Predictive Intelligence	CICIDS2017	97.2	Improved predictive capability

Literature review shows that intrusion detection systems still have issues pertaining to predictive threat intelligence, real time deployment, and attacks prediction. Thus, the given research proposes a new hybrid AI-based method of intelligent intrusion detection and predictive threat analysis in CPS settings.

3. Proposed Methodology

In this section, the researcher introduces the suggested AI and predictive threat intelligence intrusion detection system on safe Cyber-Physical Systems (CPS). The framework combines intrusion detection based on deep learning and predictive cybersecurity analytics to enhance the accuracy of attack classification and predictive capabilities in the threat. Ancillary Convolutional Neural NetworkLong Short-Term Memory (CNN-LSTM) architecture was used to seize the spatial and temporal features of attacks on CPS network traffic data.

3.1 Overall Framework Architecture

The proposed system has five stages, including data acquisition and preprocessing, feature extraction and normalization, AI-based intrusion detection, predictive threat intelligence analysis, and threat response generation. CPS traffic data of the industrial setting was pretreated and provided to the hybrid CNN-LSTM model to classify the attack and anomaly detection. CNN element obtains the spatial attack attributes of network traffic and the LSTM element obtains the sequential and temporal attack patterns. The features that are extracted are then further examined using a predictive threat intelligence module so as to estimate future cybersecurity risks. The general sequence of operations and interaction between the key structural elements is represented in Figure 1.

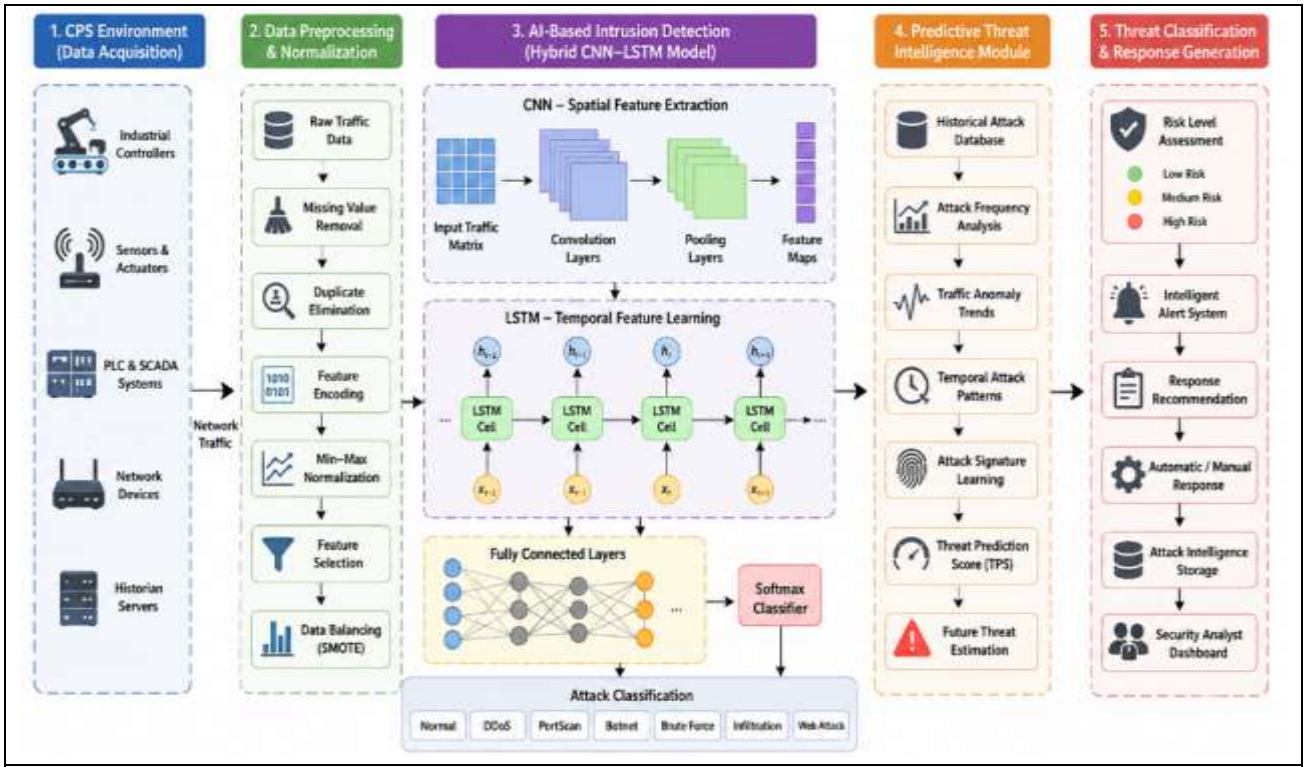

Fig. 1. Overall architecture of the proposed AI-based CPS security framework

3.2 Data Preprocessing

The CPS traffic data collected included missing values, duplicate records, noisy data and uneven distribution of attacks. Hence, before model training, preprocessing tasks such as null value removal, eliminating dups, encoding the features, normalization, feature selection, and balancing the data were carried out. Normalisation Min-Max normalization was used to scale features values between 0 and 1 using:

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

Where, Xrepresents the original feature value, X_{min}represents the minimum feature value, X_{max}represents the maximum feature value.

3.3 Hybrid CNN-LSTM Intrusion Detection Model

The proposed intrusion detection model uses a hybrid CNN-LSTM model to enhance attack classification to a greater degree. CNN module is used to generate the spatial traffic features and LSTM network generates the temporal dependencies of attacks and sequencing anomaly patterns. The figure of the workflow of the hybrid deep learning architecture is detailed in Figure 2. Convolutional operation can be represented as:

$$F(i,j) = (X * K)(i,j) \quad (2)$$

Where, Xdenotes the input feature matrix,Kdenotes the convolution kernel, $F(i,j)$represents the extracted feature map.

The LSTM network processes temporal dependencies using forget, input, and output gates.

Forget gate:

$$f_t = \sigma(W_f[h_{t-1}, x_t] + b_f) \quad (3)$$

Input gate:

$$i_t = \sigma(W_i[h_{t-1}, x_t] + b_i) \quad (4)$$

Cell state update:

$$C_t = f_t C_{t-1} + i_t \tilde{C}_t \quad (5)$$

Output gate:

$$o_t = \sigma(W_o[h_{t-1}, x_t] + b_o) \quad (6)$$

Hidden state:

$$h_t = o_t \tanh(C_t) \quad (7)$$

The extracted deep features are forwarded to fully connected layers for attack classification.

The features extracted as deep are sent to fully connected layers to do the classification of attacks. The CNN-LSTM architecture suggested comprised two convolutional layers with some max-pooling operations and LSTM based temporal learning layers. The CNN component made use of 64 and 128 convolution filters with 3×3 kernel size hierarchical spatial feature extraction of CPS traffic analysis. The 2×2 max-pooling layers were used to decrease the number of features and complexity. The LSTM model had 128 hidden units that enabled it to learn long-term temporal attack patterns and sequential aberrant patterns. Convolutional and fully connected layers included ReLU activation functions and final attack classification was done using Softmax activation. To minimize the chances of overfitting and enhance the ability to generalize the model, a dropout rate of 0.3 was used in the training process. Adam optimizer with a learning rate of 0.001 and categorical cross-entropy loss function was used to optimise the model when multiclass intrusion detection is performed.

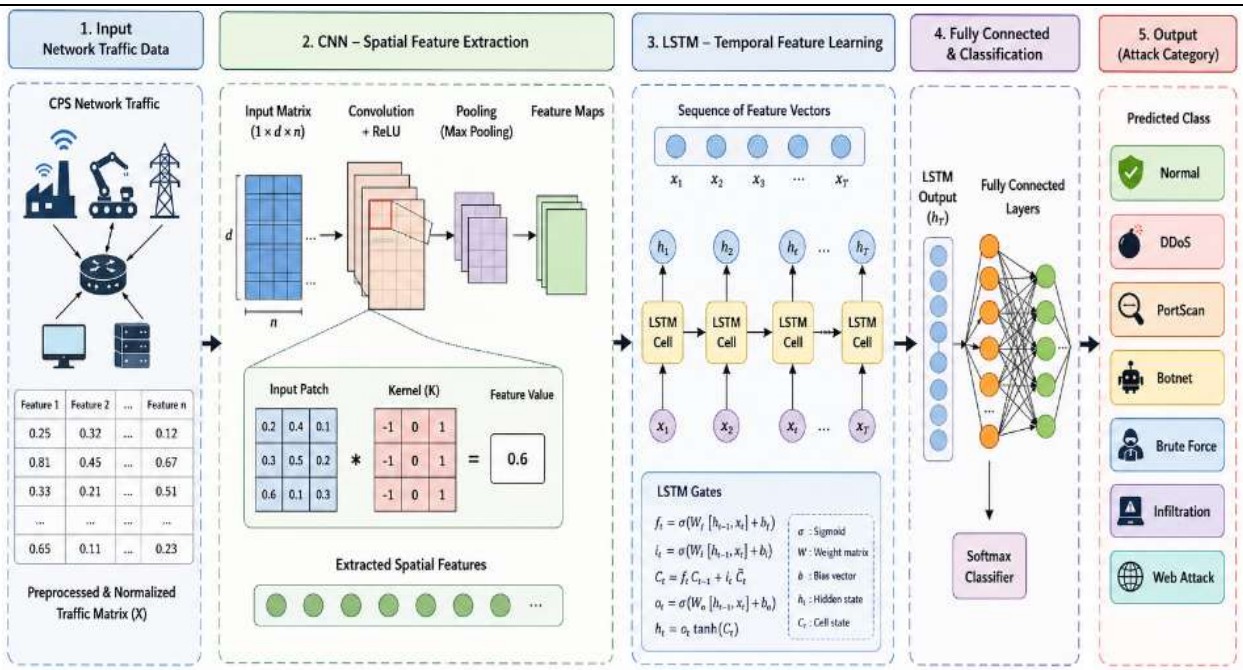

Fig. 2. CNN-LSTM intrusion detection workflow

3.4 Predictive Threat Intelligence Module

Based on the trends in anomalies and previous trends in attacks, the predictive threat intelligence module estimates the likelihood of an attack in the future and a change in cyber threats. The module examines frequency of attacks, temporal anomaly activities and network deviations to come up with foretelling threat scores. The Threat Prediction Score (TPS) would be computed as:

$$TPS = \sum_{i=1}^{n} w_i \, p_i \quad (8)$$

Where, w_i represents the feature weight, p_i represents anomaly probability.

Higher TPS values indicate elevated cybersecurity risks in CPS infrastructures.

3.5 Algorithmic Workflow

The framework suggested starts with CPS traffic acquisition and preprocessing. The processed traffic data are then provided to the CNN module where spatial features are extracted and then temporal attack learning is performed with the LSTM network. The features extracted are identified as normal and malicious traffic. This predictive threat intelligence module then estimates the likelihood of attack occurrences in the future and produces smart threat alerts to proactive CPS security management.

Algorithm 1. AI-Based Intrusion Detection and Threat Prediction

1. Input CPS traffic dataset
2. Perform preprocessing and normalization
3. Extract spatial features using CNN
4. Learn temporal attack patterns using LSTM
5. Classify network traffic into attack categories
6. Estimate predictive threat score
7. Generate intelligent threat alerts
8. Store attack intelligence for future analysis
9. End process

The suggested methodology offers a smart and scalable cybersecurity system of real-time detection of intrusion and predictive threat analysis of CPS.

4. Dataset Description and Experimental Setup

In this section, the dataset, experimental setting as well as the evaluation metrics employed to determine performance of proposed AI-based intrusion detection and predictive threat intelligence framework have been described.

4.1 Dataset Description

The suggested framework was tested on the CICIDS2017 dataset which was created by the Canadian Institute of Cybersecurity. The data sets include the simulation of realistic network traffic under normal and malicious cyberattack settings and are popular in intrusion detection and cybersecurity studies in Cyber-Physical System (CPS) systems.The CICIDS2017 data set has a number of recent attack categories including Distributed Denial-of-Service (DDoS) attacks, brute-force attacks, botnet activities, port scanning, web attacks, infiltration attacks and Heartbleed attacks. Experimentation was done with around 2.8 million records of the bidirectional network flows. This dataset has 78 features of traffic that consist of packet statistics, communication behavior, duration of flow, protocol related information, forward packet and backward packet related features, header related information, and inter-arrival time-related features. Some of the key features of network traffic include: flow duration, total forward packet, packet length statistics, average packet size, flow bytes per second, forward inter-arrival time, backward packet length, active and idle traffic duration. The distribution of the dataset was normal traffic (around 56 per cent) and malicious attack traffic (around 44 per cent). To enhance training stability and minimize non-representative samples, the preprocessing functions such as the removal of null values, removal of duplicated traffic, encoding of categorical features, feature normalization and attack-class balancing were conducted prior to the training of the models. The data was split into training and testing sets in the ratio of 80: 20. The training data included some 2.24 million traffic records, and the testing and performance evaluation data consisted of almost 0.56 million records.

Table 2. Dataset characteristics

Parameter	Value
Dataset Name	CICIDS2017
Total Records	2.8 Million
Training Samples	2.24 Million
Testing Samples	0.56 Million
Attack Categories	7
Normal Traffic	56%
Attack Traffic	44%
Features	78
Data Type	Bidirectional Network Flow Data
Feature Types	Flow, Packet, Timing, Statistical
Preprocessing Operations	Cleaning, Encoding, Normalization, Balancing

The CICIDS2017 dataset offers more realistic traffic behavior and more current attack scenarios to assess AI-based intrusion detection and predictive threat intelligence systems in CPS and Industrial IoT systems.

4.2 Experimental Environment

The deep learning frameworks were realized in Python to perform the experiments. The CNN-LSTM model suggested was run with TensorFlow and Keras in the Jupyter Notebook.

Table 3. Hardware Specifications

Parameter	Specification
Processor	Intel Core i7
RAM	16 GB

GPU	NVIDIA RTX 3060
Operating System	Ubuntu 22.04

Table 4. Software Specifications

Parameter	Specification
Python Version	Python 3.10
Framework	TensorFlow 2.13
IDE	Jupyter Notebook
Deep Learning Library	Keras

The batch size of 64 with 50 epochs was used to train the model. Learning performance was enhanced by using Adam optimizer and ReLU activation function.

Table 5. Hyperparameter Settings

Parameter	Value
Batch Size	64
Epochs	50
Optimizer	Adam
Learning Rate	0.001
Activation Function	ReLU
Loss Function	Categorical Cross-Entropy

The experimentally optimized hyperparameters of proposed CNN-LSTM framework were through iterative validation, and repeated training analysis to ensure that the hyperparameters achieve better performance in intrusion detection, and stability of model convergence. Throughout the experiment, several sets of batch size, learning rate, optimizer and training epochs were tested. The ultimate hyperparameter setup was selected due to the minimal classification loss, better validation accuracy, minimized overfitting tendency, as well as stable convergence properties upon the training cycles. The Adam optimizer, with a learning rate of 0.001 proved more efficient in convergence and stability in classification than other optimization settings.

4.3 Evaluation Metrics

The accuracy, precision, recall, F1-score, and ROC-AUC measures have been used to assess the performance of the proposed framework.

Accuracy was computed as:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (9)$$

Precision was computed as:

$$Precision = \frac{TP}{TP + FP} \quad (10)$$

Recall was computed as:

$$Recall = \frac{TP}{TP + FN} \quad (11)$$

F1-score was computed as:

$$F1 = \frac{2 \times Precision \times Recall}{Precision + Recall} \quad (12)$$

The proposed intrusion detection framework had its performance evaluated using these evaluation metrics: the capability to identify the attack and the performance in detecting the anomaly.

5. Results and Discussion

This subsection includes the performance analysis, comparative study, statistical authentication and computational complexity analysis of the suggested AI-based intrusion identification and predictive threat intelligence system.

5.1 Intrusion Detection Performance

The suggested CNN-LSTM model vividly showed excellent intrusion detection rates under various cybersecurity assessment measures. Table 6 shows the experimental results achieved by using the CICIDS2017 dataset.

Table 6. Performance evaluation results of the proposed framework

Metric	Value (%)
Accuracy	97.2
Precision	96.8
Recall	96.1
F1-Score	96.4
ROC-AUC	98.2

The findings suggest that the presented model was able to effectively extract spatial and temporal patterns of attacks based on CPS traffic data. The value of ROC-AUC is high, which indicates that it has a good performance in detecting anomalies and a good performance in classifying. The convergence behaviour of the proposed model is shown in Figure 3, the confusion matrix and ROC-AUC in Figure 4 and Figure 5 respectively. The good results of the proposed framework in terms of classification could be explained by the good spatial-temporal feature learning feature of the hybrid CNN-LSTM structure. When training the models, dropout regularization and batch normalization methods were also used to minimise the overfitting and enhance the ability of the model to generalise. Figure 3 demonstrates that the convergence curves of training and validation have reached steady training behavior with decreasing classification loss with training epochs. Also, cross-validation 10-fold and balanced dataset preprocessing facilitated better the robustness of the model and reduced the bias of the performance in experimental evaluation.

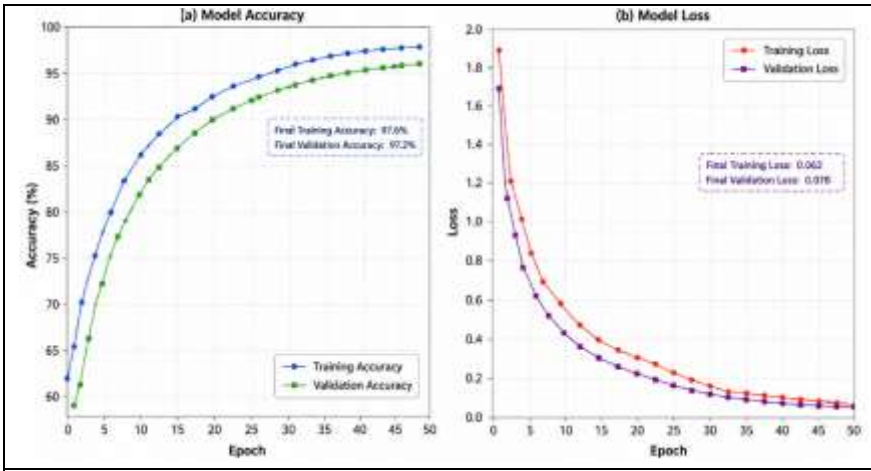

Fig. 3. Accuracy and loss convergence analysis during training

Fig. 4. Confusion matrix of the proposed intrusion detection framework

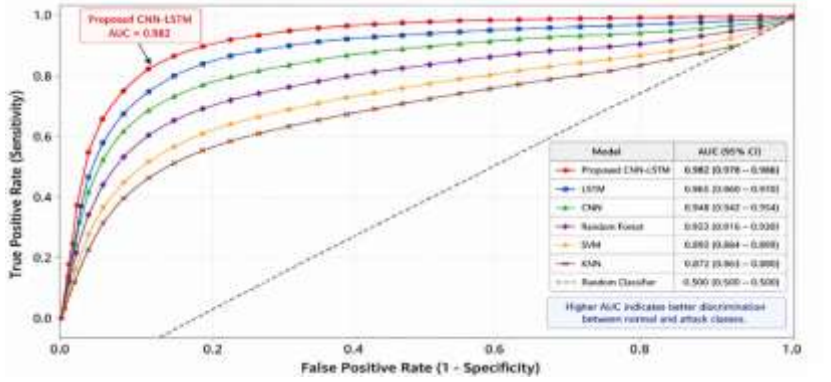

Fig. 5. ROC-AUC performance comparison

5.2 Comparative Analysis

The given framework was contrasted to traditional machine learning and single-purpose deep learning methods. The relative findings are presented in Table 7.

Table 7. Comparative analysis with existing approaches

Model	Accuracy (%)	Precision (%)	Recall (%)
SVM	89.4	88.2	87.5
Random Forest	91.6	90.9	90.1
KNN	90.3	89.8	88.7
CNN	94.8	94.1	93.7
LSTM	95.4	95.0	94.3
Proposed CNN-LSTM	97.2	96.8	96.1

The hybrid CNN-LSTM model was more effective in terms of its better spatial-temporal learning of features than the traditional machine learning and standalone deep learning models.

5.3 Ablation Study

A study was carried out to determine the value of individual components of the frameworks by an ablation study. Table 8 shows the results obtained.

Table 8. Ablation study of the proposed framework

Model	Accuracy (%)
CNN Only	94.8
LSTM Only	95.4

CNN-LSTM	97.2
CNN-LSTM + Threat Intelligence	97.9

Combination of predictive threat intelligence enhanced the performance of attacks forecasting and the performance of cyber security in general.

5.4 Statistical Validation

In order to test the ability of the model to be robust and to generalize, a 10-fold cross-validation approach was used.

Table 9. Statistical validation results

Metric	Mean ± SD	95% Confidence Interval
Accuracy	97.2 ± 0.5	96.7–97.7
Precision	96.8 ± 0.4	96.4–97.2
Recall	96.1 ± 0.5	95.6–96.6
F1-Score	96.4 ± 0.4	96.0–96.8

The small values of standard deviations attest to the fact that there are no fluctuations in performance between validation folds.

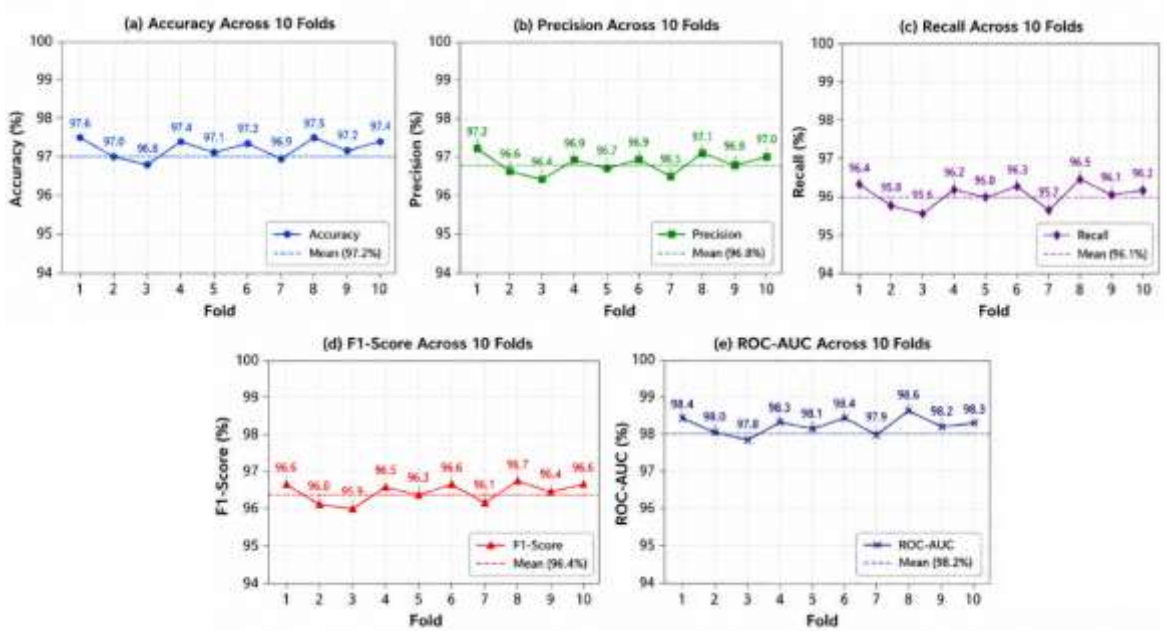

Fig. 6. Cross-validation performance stability analysis

Table 10. Inferential statistical significance analysis

Metric	p-value
Accuracy	< 0.05
Precision	< 0.05
Recall	< 0.05
F1-Score	< 0.05

This inferential statistical test proved that the performance gains obtained by the suggested CNN-LSTM framework had a statistically significant value. The p-values of the obtained values less than the 0.05 mark reveal a high degree of statistical reliability and lower the chances of the variation of performance caused by the random elements of the experiment.

5.5 Predictive Threat Intelligence Analysis

The predictive threat intelligence module was able to detect the changing patterns and upcoming cybersecurity threats. The framework showed a lower false alarm detection rate, enhanced priority of anomalies, as well as forecasting of threats proactively in dynamic CPS environments.

5.6 Computational Complexity Analysis

The calculational time of the suggested framework was examined as well. These are shown in Table 11.

Table 11. Computational complexity analysis

Parameter	Value
Training Time	138 minutes
Inference Time	21 ms
Model Parameters	2.3 Million
GPU Memory Usage	22.4 MB
Average CPU Utilization	48%

The suggested framework had a low inference latency that was accompanied by moderate memory consumption and was suitable in real-time CPS security systems and edge-enabled cybersecurity environment.

Conclusion and Future Work

The paper has introduced an AI-based intrusion detection and predictive threat intelligence system of secure Cyber-Physical Systems (CPS). The new framework combined both CNN and LSTM frameworks with predictive threat intelligence processes to enhance the accuracy of attack detection, anomaly detection, and capability of acting proactively in addressing cybersecurity. The CNN component generated spatial attack information using CPS traffic data and the LSTM network generated temporal attack information and sequential anomaly patterns. The CICIDS2017 dataset was used to evaluate the performance of the intrusion detector and it showed strong performance with an accuracy of 97.2, precision of 96.8, recall of 96.1, F1-score of 96.4 and ROC-AUC score of 98.2. Empirical studies revealed that the suggested framework performed better than the traditional machine learning and the individual deep learning methods. The strength and that of the proposed model and its generalization ability was further statistically validated. The forecasting capability of the predictive threat intelligence module was effective in enhancing proactive attacks forecasting and generation of cybersecurity responses, in dynamic CPS environments. Another finding was that computational complexity analysis showed low inference latency, moderate memory use, meaning that real-time CPS security applications can be deployed. The future research will involve federated cybersecurity learning, explainable AI-based intrusion detection, lightweight edge-AI deployment, blockchain-based CPS security, and real-time Industrial IoT threat intelligence systems. All in all, the presented framework presents a scalable and intelligent cybersecurity system in next generation infrastructures of CPS.

References

1. Akshya, J., Sundarrajan, M., Vijayakumar, R., Dhanaraj, R. K., & Nayyar, A. (2025). Explainable AI-driven intrusion detection for securing IoT-enabled autonomous transportation systems. *Cluster Computing, 28*(14), 884.
2. Al-Quayed, F., Ahmad, Z., & Humayun, M. (2024). A situation-based predictive approach for cybersecurity intrusion detection and prevention using machine learning and deep learning algorithms in wireless sensor networks of Industry 4.0. *IEEE Access, 12*, 34800–34819.
3. Awadallah, A., Eledlebi, K., Zemerly, M. J., Puthal, D., Damiani, E., Taha, K., & Yeun, C. Y. (2024). Artificial intelligence-based cybersecurity for the metaverse: Research challenges and opportunities. *IEEE Communications Surveys & Tutorials, 27*(2), 1008–1052.
4. Barbhaya, M., Dasari, P. R., Damarla, S. K., Srinivasan, R., & Huang, B. (2025). A deep learning framework for cyberattack detection and classification in industrial control systems. *Computers & Chemical Engineering*, 109278.
5. Ding, W., Jing, X., Yan, Z., & Yang, L. T. (2019). A survey on data fusion in internet of things: Towards secure and privacy-preserving fusion. *Information Fusion, 51*, 129–144.

6. Khalaf, N. Z., et al. (2025). Development of real-time threat detection systems with AI-driven cybersecurity in critical infrastructure. *Mesopotamian Journal of Cybersecurity, 5*(2), 501–513.
7. Kim, J., Park, H., & Lee, S. (2023). Enhancing IoT security with CNN-based anomaly detection using multimodal sensor data. *Journal of Cybersecurity AI, 15*(2), 120–134.
8. Li, H., & Sun, Y. (2024). Privacy-preserving machine learning methods for IoT security. *Annual Review of Machine Learning Security, 8*(1), 50–75.
9. Mao, Q., Hu, F., & Hao, Q. (2021). Deep learning for intelligent wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 20*, 2595–2621.
10. Ndibe, O. S. (2025). AI-driven forensic systems for real-time anomaly detection and threat mitigation in cybersecurity infrastructures. *International Journal of Research Publication Reviews, 6*(5), 389–411.
11. Oyedotun, S. A., Oise, G. P., &Ozobialu, C. E. (2025). Towards intelligent cybersecurity in SCADA and DCS environments: Anomaly detection using multimodal deep learning and explainable AI. *Journal of Scientific Research Reviews, 2*(3), 20–31.
12. Rao, V., & Smith, L. (2023). Federated learning for IoT security: Challenges and opportunities. *Cybersecurity Advances, 6*(1), 30–48.
13. Shaik, A. K., Mohammadi, A., & Malik, H. (2025). A systematic review of sensor vulnerabilities and cyber-physical threats in industrial robotic systems. *IET Cyber-Physical Systems: Theory & Applications, 10*(1), e70023.
14. Singh, A., & Chandra, D. (2024). Lightweight deep learning models for edge computing in IoT security. *IEEE Transactions on IoT Systems, 21*(4), 540–556.
15. Zhang, Y., & Liu, X. (2024). Temporal pattern recognition in smart devices using RNNs for cybersecurity. *International Journal of AI Security, 12*(1), 45–60.
16. Ashu Nayak. (2025). Ubiquitous DSP Processing for Edge-AI Devices Using Reconfigurable RISC-V Architectures. *National Journal of Ubiquitous Computing and Intelligent Environments*, *2*(3), 14–21.
17. Lau W. Cheng, Beh L. Wei. (2025). Fault Diagnosis and Condition Monitoring of Electric Drives Using Model-Based Analytical Techniques. *National Journal of Electric Drives and Control Systems*, 25-32.
18. Muhammad Ali, & Ahmed Bilal. (2025). Low-Power Wide Area Networks for IoT: Challenges, Performance and Future Trends. Journal of Wireless Sensor Networks and IoT, 2(2), 20-25. https://doi.org/10.31838/WSNIOT/02.02.03