iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VII **Month of publication:** July 2026

DOI: https://doi.org/10.22214/ijraset.2026.84396

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VII July 2026- Available at www.ijraset.com

Deep Learning based Framework for Intelligent Threat Detection in IoT-Driven Cyber-Physical Systems

Sowjanya Samineni[1], Dr. P Chiranjeevi[2]
Dept. of CSE, Amrita Sai Institute of Science & Technology Vijayawada, Andhra Pradesh, India

Abstract: ***The Internet of Things (IoT) technologies have been rapidly adopted in the field of Cyber-Physical Systems (CPS) and have greatly enhanced the automation, connectivity and operational efficiency of industrial and critical infrastructure (ICI) environments. The advent of greater device connectivity, however, has also grown the attack surface, leaving CPS environments open to many different cyber threats. The traditional methods of intrusion detection are not effective in detecting more complex and advanced attacks because the features are manually designed and cannot be easily adapted. In this publication, a Deep Learning (DL)framework for security monitoring is presented in this study, which uses CNN to improve the intrusion detection capability of the cyber-attack system in the IoT-enabled CPS environment. The intended framework accepts the network traffic data out of the UNSW-NB15 dataset to learn complicated cyber security threats and identify attacks from normal data traffic. We compared the proposed CNN model against a conventional Support Vector Machine (SVM) classifier. The experimental results demonstrate that the CNN model surpasses the others across key metrics, including precision, accuracy, F1 score and recall. The proposed approach has proved to be efficient in capturing hidden traffic characteristics and improves the reliability of cyber threat detection framework in dynamic IoT-based CPS systems. The evaluation results confirm that deep learning methods can be a scalable and efficient way to enhance the cybersecurity of next-generation cyber-physical infrastructures.***

Keywords: Cyber-Physical Systems, Internet of Things, Cyber Threat Detection Framework, Deep Learning, Convolutional Neural Networks, Cyber Security, UNSW-NB15 Dataset.

I. INTRODUCTION

The IoT is responsible for transforming the existing world of computing through interconnections of the very things which form it. Thanks to the advances achieved, there appeared what we call Cyber Physical Systems (CPS). CPS is associated with the tight integration of physical processes along with computing and communication aspects. In terms of the applications of CPS as well as IoT, they are increasingly employed in such crucial domains as smart manufacturing, healthcare, transportation, smart grid and industrial automation. The benefits of using these systems lie in their ability to increase efficiency and productivity thanks to real-time monitoring, intelligent decision-making, and automation. However, widespread interconnection and data exchange become a serious challenge when speaking about cyber security.

With the frequency and complexity of cyber-attacks, security in CPS has now emerged as an issue of major importance. The CPS system has a greater vulnerability of being attacked and these attacks may result in problems of operational disruption, monetary loss, and even safety concerns, as compared to normal information systems that directly interface with physical infrastructure. There are numerous types of attacks that can be carried out on IoT-enabled systems. These include denial-of-service attack, reconnaissance attack, malware attack, and access/network penetration attack. Besides, the fact remains that IoT-enabled systems have very limited resources, making them vulnerable to any kind of attacks.

IDS technology is widely applied to improve the security of networks by detecting malicious activities and suspicious traffic. Almost all IDS techniques utilize the signature-based and rule-based approaches that prove to be efficient in dealing with previously known attacks. The downside of these techniques is that they can fail to recognize emerging or developing threats. To overcome this problem, machine learning has been incorporated into IDS applications. In addition, some classification approaches such as SVM, Random Forests and Decision Trees have proven to be efficient in classifying traffic into two groups – normal and malicious. Still, they have several limitations including inefficiency in handling complex and high-dimensional data and the necessity of manual feature engineering.

Thanks to the recent advances in deep learning, there are new opportunities for enhancing intrusion detection performance. Deep learning models can automatically learn meaningful feature representations from raw data, which reduces the need for manually crafted features.

The CNNs are amongst the effective DL models that are employed in solving the problems of pattern recognition and classification and also perform exceptionally well in analyzing the intricate relationships within the data. This feature renders CNNs well suited to detect complex attack patterns in IoT-based Cyber-Physical Systems.

The CNN-based intrusion detection system for detecting the security attacks in CPS using IoT technology is introduced in this study. The proposed framework uses a UNSW-NB15 dataset consisting for variety of network traffic samples that span normal and malicious traffic. The performance of the CNN model has been evaluated and compared with the performance of a benchmarking process through the SVM model by analyzing the results based on accuracy, precision, recall, and f1-score measures. The experimental results demonstrate that the designed CNN model outperforms in both detection and classification processes and hence can be considered as an appropriate solution for Cyber Security. The structure of this paper is presented as follows. The second section will be on the related literature while the third one discusses the methodology used. The fourth section presents the results of experiments conducted while the fifth section concludes the paper.

II. LITERATURE SURVEY

Nowadays, CPS that is associated with Internet of Things (IoT) is a crucial element in contemporary ICI applications. As these systems grow increasingly connected, however, they have been vulnerable to many cyber threats. Cárdenas et al. [2] talked about the significant security issues of CPS environments and pointed out the importance of using sophisticated protection mechanisms that can detect malicious activities before they impact physical operations. Their project demonstrated the significance of cyber security for systems where cyber and physical parts are strongly coupled.

There are a few benchmark data sets for supporting research on intrusion detection. The UNSW-NB15 data set developed by Moustafa and Slay [7] is an extremely popular data set that represents real-world scenarios of network traffic and attacks. The researchers have also examined this data set and proved its appropriateness for testing intrusion detection systems under different network environments [8]. With the access of these datasets, researchers have been able to develop and test intelligent security systems by applying ML and DL algorithms. The majority of the IDSs in past literature have made use of the signature-based technique and ML algorithms. In a study conducted by Apruzzese et al. [3] on the suitability of ML techniques in cybersecurity problems, the authors claim that data-based models will prove to be more efficient than rule-based models for attack detection purposes Similarly, Shaukat et al. [4] conducted a comparative analysis among various ML techniques and pinpointed some issues related to feature engineering, scalability, and adaptability of models in an evolving cyber environment.

Intrusion Detection has seen tremendous improvements in the past few years by the implementation of DL. In this context, S. LeCun et al. [5] demonstrated the potentiality of DL systems in extracting features hierarchically from complicated datasets. Based on these innovations, Javaid et al. [9] developed a deep learning IDS that automatically extracted attack features from network traffic datasets. The results made them want to investigate more deeply into deep learning approaches in cyber-security.

CNN, which is one of the DL models, has been found effective for network security. Wang et al. [10] suggested the utilization of CNN models for detecting malicious network traffic and achieved higher detection rate compared to traditional ML models. In the same manner, Roopak et al. [11] examined the use of DL models for IoT security and found out that the CNN-based models detect hidden patterns of the trafficked data with respect to cyber-attack. Moreover, Potluri and Diedrich [12] showed that deep neural network architectures can improve intrusion detection performance and minimize the reliance on manual feature engineering.

DL is also widely researched to be applied in the industry-based IoT domain. Al-Hawawreh et al. [13] suggested a security model using DL which was capable of identifying malicious behaviors in the industrial network with high accuracy. Furthermore, Hodo et al. [15] provided an IDS using an artificial neural network in IoT and demonstrated the efficiency of the system in identifying network attacks. Bennett et al. [17] also investigated the possibilities for using deep learning models on resource-constrained sensor networks, and found that intelligent learning-based strategies can greatly enhance network security.

Otoum et al. [16] explored the potential for using deep learning models on sensor networks with limited resources, and concluded that intelligent learning-based approaches can significantly improve network security. Inspite of the significant advancements that have been made in research pertaining to intrusion detection, it is challenging to identify any form of attacks in CPSs enabled by IoT. Current ML techniques rely on manually designed features and can be difficult to apply to high-dimensional data to identify complex attack patterns. In this regard, this study presents an intrusion detection approach, which uses CNNs to benefit from deep learning techniques for improving the security of cyber-attack detection in the IoT scenario and IPCPS security.

III. SYSTEM ARCHITECTURE

The proposed architecture is the identification of cyber-attacks in the Internet of Things (IoT) based Cyber Physical System (CPS) through Convolutional Neural Networks (CNN). The main aim of the architecture is to accurately distinguish normal and malicious traffic based on learning hidden patterns from network data. The entire process will be comprised of data collection, data pre-processing, feature extraction, model building, classification of attacks, and performance measurement.

UNSW-NB15 is used as the primary dataset in this research for model development and validation. This dataset comprises both legitimate and illegitimate instances of network traffic and attacks on the network. Various data processing methods are utilized to improve the quality of the data set to make the learning process easy before training the machine learning model. Such processes include imputation, feature reduction, categorical feature transformation, and normalization of features.

Moreover, after completion of the process of pre-processing the data, the selected features would be fed into the architecture of CNN model. The convolution layer in the model would help in capturing the pattern of the dataset, while the pooling layer would help in reducing the dimensions of the dataset.

For comparing the efficiency of the proposed CNN model, a standard SVM classifier would be used. Some of the main performance criteria such as accuracy, precision, recall, and F1-score would be used to evaluate the efficiency of the models.

A. System Architecture

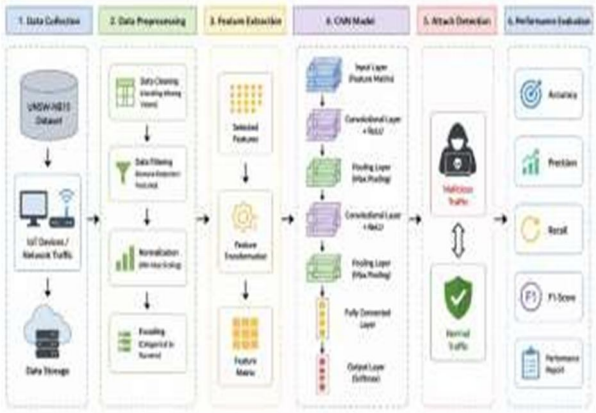


Fig. 1. Proposed CNN-Based Cyber Attack Detection Framework

B. Comparative Analysis of Existing and Proposed Methods

Parameter	SVM Model	CNN Model
Learning Method	ML	DL
Features Extraction	Manually done	Automation
Training Complexity	Medium	High
Detection Ability	Moderate	High
Scalability	Limited	Better
Accuracy	83.29%	99.52%
Precision	Low	High
Recall	Low	High
F1-Score	Low	High

Table I. Comparison between the SVM and CNN models

CNN model surpasses the traditional SVM-based one due to its ability to automatically derive the hierarchy of features from the data on network traffic. It enables the model to detect complex attacks and improve the accuracy of detection in general in Cyber-Physical Systems.

IV. METHODOLOGY

Proposed methodology is designed to detect the cyber-attacks in CPS that are fitted with IoT using CNN. These stages include the data collection stage, data preprocessing stage, feature extraction stage, training the model, and classifying attacks. The purpose of all of these stages is to let the system learn the traffic characteristics and classify normal and abnormal traffic.

A. Dataset Description

UNSW-NB15 dataset is employed to train and test the proposed ID system. Records of modern network traffic generated with realistic network conditions and both normal activities and multiple attack categories. The dataset offers a complete set of network characteristics to assist with the effective analysis and classification of cyber-attacks.

B. Data Preprocessing

The process of data preprocessing is done prior to model training with the intention of enhancing the quality of the data. Firstly, the missing data and duplicates are eliminated. Secondly, encoding of the data is done to make sure that the categorical data is encoded with numerical values. Thirdly, the raw data is normalized using feature normalization to map the data onto a common scale to enhance CNN model learning efficiency. The data after preprocessing is divided into training and testing data.

C. CNN-Based Feature Learning

The processed data is provided as the input to the Convolutional Neural Network. Convolutional Neural Networks consist of convolutional layers, pooling layers, and fully connected layers. Convolutional layers can automatically extract the features and traffic patterns from the input data. Pooling layers can compress the dimensionality of the feature space without discarding any vital information. The hierarchical way of learning allows the neural network to learn more complex features without performing any feature engineering.

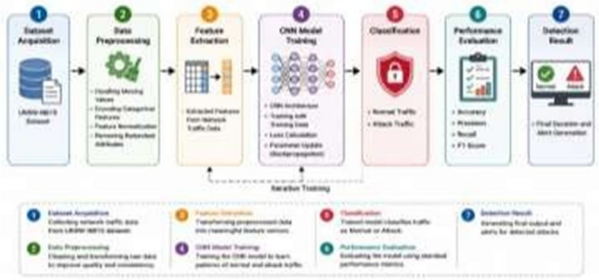


Fig. 2. CNN Architecture for Cyber Attack Detection

D. Detection Workflow

The entire detection procedure begins with the acquisition of data sets, followed by preprocessing and feature extraction. These features are used as input to train and classify the CNN model. Once the CNN model is trained, it generates predictions for the network traffic that can be either normal or malicious. The predictions generated are measured using standard metrics.

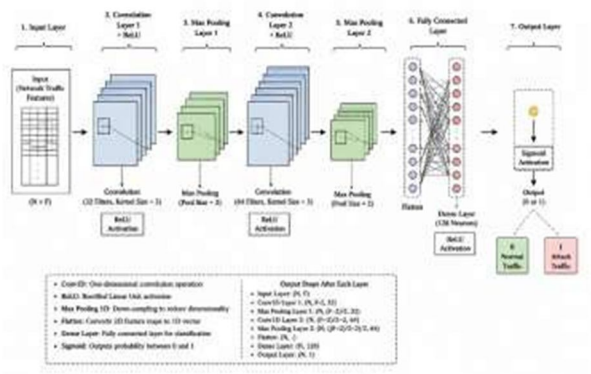


Fig. 3. Proposed Detection Process Workflow

E. Algorithm

Algorithm 1: CNN-Based Cyber Attack Detection to load the UNSW-NB15 dataset, click on

1. Load the UNSW-NB15 dataset.
2. Do data cleaning and data pre-processing step.
3. Transform categorical variables into numbers.
4. Normalize the data features.
5. Separate the dataset to training set and testing set.
6. Build CNN Architecture.
7. Train CNN model with training data.
8. Classify in test data.
9. Accuracy, Precision and Recall and F1-Score will be computed
10. Comparison of results for SVM algorithm will be done.

The methodology presented is capable of efficient learning of network traffic behavior and improves the detection capability of cyber-attacks on CPS using IoT.

The framework, with its deep learning based feature extraction, also achieves better classification performance and robust intrusion detection.

V. RESULTS AND DISCUSSION

The suggested model is the Convolutional Neural Network (CNN) and it was evaluated using UNSW-NB15 dataset by comparing it with the SVM classifier. For the evaluation process, some common evaluation measures, such as Accuracy, Precision, Recall, and F1-Score, have been used. They could be employed for analyzing the effectiveness of the intrusion detection system in detecting attacks on the IoT enabled CPS.

A. Performance Evaluation

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
SVM	83.29	87.66	81.05	82.44
CNN	99.52	99.35	99.39	99.37

Table II. SVM and CNN Model Performance Measures

It is evident from the results provided in Table II that the proposed CNN model outperforms the conventional SVM model in terms of cyber-attack detection. It can be seen that the accuracy rate of CNN is 99.52%, while that of SVM is 83.29%. In addition, there have been improvements in other performance measures like precision, recall, and F1- score.

B. Confusion Matrix Analysis

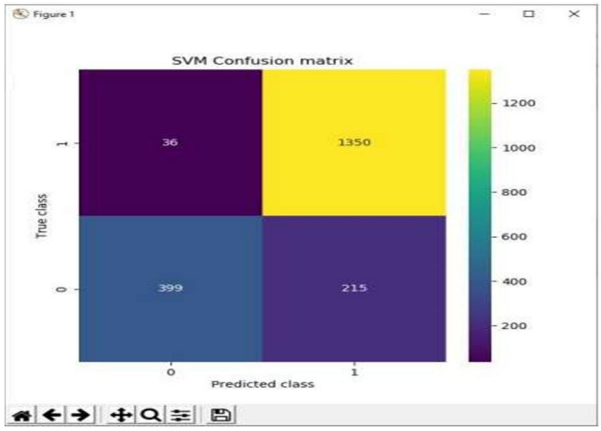


Fig. 4. SVM-Based Intrusion Detection Model is formulated in the form of a Confusion Matrix.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VII July 2026- Available at www.ijraset.com

Confusion matrix for the classifier using SVM describes the classification results for the network traffic data samples both true and false classifications. SVM model detects quite many attacks; however, there are problems related to false positives and negatives, which influence accuracy of intrusion detection. False classification makes the system untrustworthy if used within a Cyber-Physical System based on IoT environment.

The confusion matrix for the proposed CNN model is illustrated in Fig. 5. It can be observed that classification errors have been greatly reduced compared to the SVM classifier. It indicates that the CNN model has achieved accurate classification of attack and normal traffic flows and thereby reducing the false alarms and increasing detection accuracy. This improved performance shows how deep learning models learn from complex network traffic data.

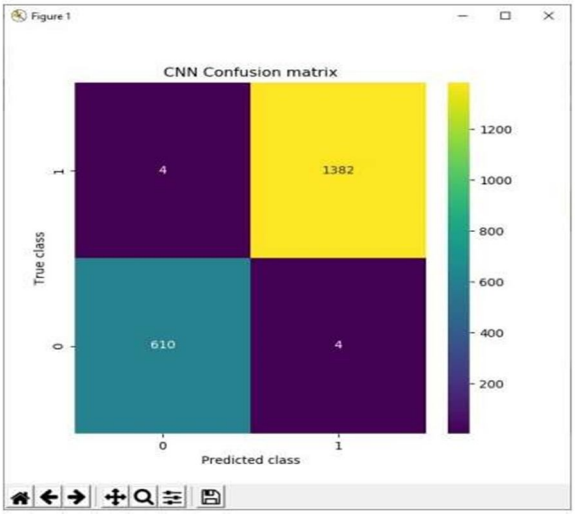


Fig. 5. Confusion matrix for the proposed CNN-based intrusion detection approach is illustrated below.

C. Comparative Performance Analysis

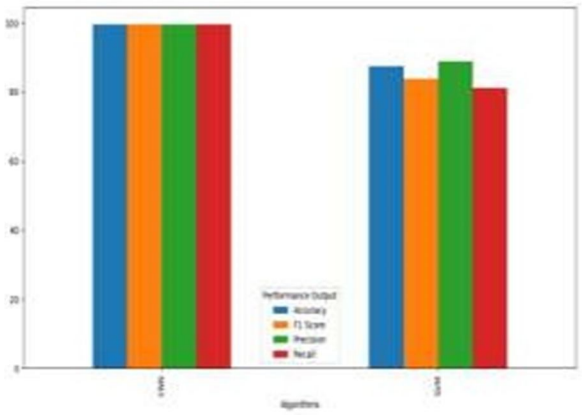


Fig. 6. The performance of SVM and CNN models was compared. The performance comparison between SVM and CNN models was conducted.

The performance comparison between the SVM and CNN model according to the evaluation criteria is presented in Figure 6. As it can be seen from the graphic illustration, the CNN model has outperformed the SVM classifier in terms of all the performance metrics. The CNN model's accuracy, precision, recall, and F1-score values have turned out to be significantly higher, which is evidence of the superior intrusion detection ability of the CNN model.

Specifically, the CNN model's precision is equal to 99.35%. This fact suggests that the number of false positives is very low because there are just a few network traffics that have been wrongly recognized as malicious. Similarly, the recall value of 99.39% implies that the CNN model has demonstrated high performance in detecting almost all attacks in the data set.

D. Discussion

The main benefit of the CNN model could be seen in the fact that the CNN can learn the features of the image automatically. The architecture of the CNN is capable of learning the hierarchical features of the data without using manual feature engineering techniques, which are used in traditional machine learning approaches. It allows detecting the complex and hidden attack patterns, which could not be detected by traditional classifiers.

Furthermore, the developed framework is quite flexible in terms of addressing the new cyber threats in the context of IoT-based Cyber-Physical Systems. As a result of the training on a big amount of data, the CNN learns discriminative features, which helps in increasing the effectiveness of the classifier. The obtained results demonstrate that the developed deep learning approach to intrusion detection is a reliable method for the protection of the Cyber-Physical System.

VI. CONCLUSION AND FUTURE WORK:

Since the Internet of Things (IoT) is gaining popularity in the field of Cyber Physical System (CPS), there is a need to take into consideration the degree of connectivity and the type of cyber-attack. In this paper, an intrusion detection system using deep learning, with Convolutional Neural Network (CNN) method, has been proposed to detect the cyber-attack in the CPS environment using the IoT device. The proposed scheme has been designed to address the limitations of the conventional machine learning schemes.

The proposed CNN model was evaluated on the basis of UNSW-NB15 data set and its performance was compared with that of a typical Support Vector Machine (SVM) classification algorithm. For the verification of CNN model, it was tested against experimental data, and it was found that the proposed CNN model outperformed in terms of all evaluation metrics. The accuracy rate of the proposed CNN model was 99.52%, whereas the precision, recall and F1-score were 99.35%, 99.39% and 99.37% respectively which is far superior as compared to SVM model. The results demonstrate the learning of complex network traffic patterns and correct classification of normal and malicious network activities using the CNN architecture.

From the findings obtained from this study, it can be concluded that deep learning algorithms can be used effectively as a feasible and scalable solution for the intrusion detection problem in CPS.

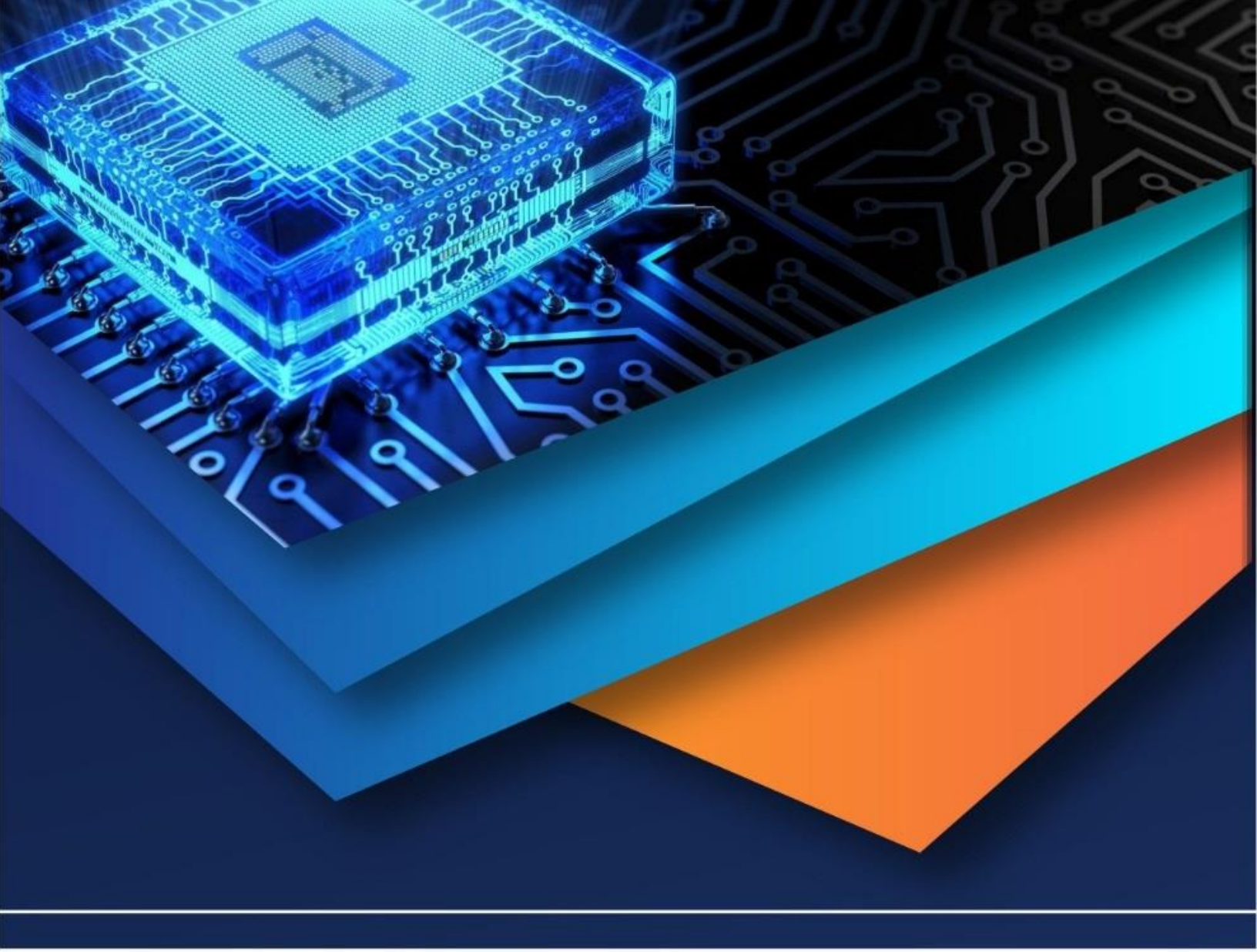
The ability of the CNNs to perform automatic feature extraction minimizes the requirement of manually extracting the features and increases the ability to detect complicated cyber-attacks. Thus, the suggested framework will improve the security of the IoT-based CPS.

The presented framework may be employed for real-time intrusion detection in large IoT systems in the future as an extension to it. Future possible enhancements in the intrusion detection performance can be obtained through use of state-of-the-art deep learning architecture including LSTM, GRU, and the combination of CNN with LSTM models. In addition, application of the framework alongside edge computing techniques and federated learning will allow increasing its scalability, privacy preservation capability, and resistance to future cyber threats. Moreover, the proposed solution may be applied in future research using recently developed intrusion datasets that include more than one class of attack.

REFERENCES

[1] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, “Internet of Things security and forensics: Challenges and opportunities,” Future Generation Computer Systems, vol. 78, pp. 544–546, 2018.
[2] D. Evans, “The Internet of Things: How the next evolution of the Internet is changing everything,” Cisco Internet Business Solutions Group, pp. 1–11, 2011.
[3] A. A. Cárdenas, S. Amin, and S. Sastry, “Research challenges for the security of cyber physical systems,” in Proc. 3rd USENIX Workshop on Hot Topics in Security, 2008, pp. 1–6.
[4] E. Hodo, X. Bellekens, A. Hamilton, P. Dubouilh, and E. Iorkyase, “Threat analysis of IoT networks using artificial neural network intrusion detection system,” in Proc. IEEE Int. Symposium on Networks, Computers and Communications, 2016, pp. 1–6.
[5] N. Moustafa and J. Slay, “UNSW-NB15: A comprehensive data set for network intrusion detection systems,” in Proc. Military Communications and Information Systems Conference, 2015, pp. 1–6.
[6] N. Moustafa and J. Slay, “The evaluation of network anomaly detection systems: Statistical analysis of the UNSW-NB15 dataset,” Information Security Journal, vol. 25, no. 1–3, pp. 18–31, 2016.
[7] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, “Toward generating a new intrusion detection dataset and intrusion traffic characterization,” in Proc. ICISSP, 2018, pp. 108–116.
[8] W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, “Malware traffic classification using convolutional neural network for representation learning,” in Proc. International Conference on Information Networking,2017, pp. 712–717.
[9] Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,” Nature, vol. 521, no. 7553, pp. 436–444, 2015.
[10] A. Krizhevsky, I. Sutskever, and G. E. Hinton, “ImageNet classification with deep convolutional neural networks,” Communications of the ACM, vol. 60, no. 6, pp. 84–90, 2017.

[11] M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, "A detailed analysis of the KDD CUP 99 dataset," in Proc. IEEE Symposium on Computational Intelligence for Security and Defense Applications, 2009, pp. 1–6.
[12] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, "On the effectiveness of machine and deep learning for cyber security," in Proc. IEEE International Conference on Cyber Conflict, 2018, pp. 371–390.
[13] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "Long short term memory recurrent neural network classifier for intrusion detection," in Proc. International Conference on Platform Technology and Service, 2016, pp. 1–5.
[14] S. Potluri and C. Diedrich, "Accelerated deep neural networks for enhanced intrusion detection system," IEEE Access, vol. 8, pp. 21928–21938, 2020.
[15] M. Al-Hawawreh, N. Moustafa, and E. Sitnikova, "Identification of malicious activities in industrial internet of things using deep learning models," Journal of Information Security and Applications, vol. 47, pp. 241–254, 2019.
[16] H. Hindy, D. Brosset, E. Bayne, A. Seeam, C. Tachtatzis, R. Atkinson, and X. Bellekens, "A taxonomy and survey of intrusion detection system design techniques, network threats and datasets," ACM Computing Surveys, vol. 54, no. 5, pp. 1–36, 2021.
[17] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, "Performance comparison and current challenges of using machine learning techniques in cyber security," Energies, vol. 13, no. 10, pp. 2509–2525, 2020.
[18] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in Proc. EAI International Conference on Bio-inspired Information and Communications Technologies, 2016, pp. 21–26.
[19] M. Roopak, G. Y. Tian, and J. Chambers, "Deep learning models for cyber security in IoT networks," in Proc. IEEE International Instrumentation and Measurement Technology Conference, 2019, pp. 1–6.
[20] S. Otoum, B. Kantarci, and H. Mouftah, "On the feasibility of deep learning in sensor network intrusion detection," IEEE Networking Letters, vol. 1, no. 2, pp. 68–71, 2019.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY