Design and Implementation of Secured Deep Learning Model for Prediction of Cyber Attacks in Computer Networks

M Dharani[1], P Murugesan[2], B Vinothkumar[1], Kiruthika B[1], Kavya R[1] and Sharmila Devi M[1]
[1]*Department of Electronics and Communication Engineering, K.S.R. College of Engineering, Tiruchengode, Tamil Nadu, India*
[2]*Department of Mechanical Engineering, K.S.R. College of Engineering, Tiruchengode, Tamil Nadu, India*

Keywords: Cyber Security, Cyber Attacks, D-Dos Attacks, Network Traffic, Deep Learning Model, Convolutional Neural Networks-CNN, Long Short Term Memory-LSTM, Computer Networks.

Abstract: This research develops a CNN-based deep learning model to predict cyberattacks in computer networks and compares it with an LSTM model. Materials and Methods: It considered two groups: (LSTM) and (CNN) of 26 samples each with a G Power of 80%, a threshold of 0.05, and a 95% confidence interval. Result: The CNN model outperformed the LSTM model in accuracy, 92.56% to 96.74%, while the LSTM model ranged between 85.42% to 91.87%. In addition, CNN had lower false positive rates ranging from 2.87% to 4.14% compared to LSTM, which had 4.32% to 6.89%. CNN also had a better stability, with a standard deviation of 1.6743, whereas LSTM had 2.8567. These results confirm the effectiveness of CNN in cyberattack detection, consistent with studies on cybersecurity and AI-based threat detection.

1 INTRODUCTION

The increase in cyberattacks on the Internet of Things (IoT) leads to the increasing need for developed sophisticated predictive methodology for better cyber security. CNN-based deep learning has been utilized as a method to identify potential threats and eradicate them (C. Zhong et al., 2023). Using CNN, network traffic analysis may be done as an anomaly for detection, ensuring that the algorithm achieves more than 95% prediction accuracy in its predictions (C. Chen et al., 2023). Further development focuses on the need for real-time monitoring, with reports showing detection rates over 90% while keeping false positive rates under 5%. The different techniques of machine learning have also been talked about. Some deep learning models can detect patterns of an attack in as little as 0.5 seconds (P. Yadav et al., 2022) New specialized architectures for the detection of DDoS attacks have been designed with a reported accuracy of up to 98% and below 1-second response times (P. Yadav et al.,2022) In summary, the use of deep learning with CNN algorithms may offer a great hope for cyber-attack prediction and mitigation within IoT networks to enable more solid and effective solutions to cybersecurity as more devices continue to connect into a single network in the ever-expanding digital landscape (M. N. Al Jarrah et al., 2022).

2 RELATED WORKS

In the last five years alone, more than 250 articles on this topic have been published through IEEE Xplore, 80 papers through Google Scholar, and 108 papers through academia.edu. This growing literature highlights the imperative need for practical solutions in the specific domain of cyber threat detection and prediction (AD Jasim et al., 2023) Various deep learning techniques, especially convolutional neural networks (CNNs), have recently been explored for the improvement of accuracy and efficiency in cyberattack predictions.

For example, a comprehensive review of the effectiveness of AI & ML approaches on cybersecurity solutions shows that deep learning models can be used to improve threat detection (T Van Dao et al., 2022). The idea of using deep learning for cyberattack prediction has become popular, and researchers have shown that CNNs can also be used to analyze network traffic and detect anomalies which

Dharani, M., Murugesan, P., Vinothkumar, B., B., K., R., K. and M., S. D.
Design and Implementation of Secured Deep Learning Model for Prediction of Cyber Attacks in Computer Networks.
DOI: 10.5220/0013920800004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 4*, pages 789-795
ISBN: 978-989-758-777-1

may indicate a threat. Deep learning in cybersecurity attack prediction has recently demonstrated very good performance in accuracy levels in identifying many types of attacks (B Yadav et al., 2021). In addition, the survey of deep learning algorithms mainly for cyber security applications showed that these models can drastically enhance the detection rate while reducing false positives to the barest minimum (UH Tayyab et al., 2022) Deep learning techniques-based methods for network attacks have also been reviewed in depth to demonstrate the flexibility and ability of such approaches in real-time monitoring scenarios (S Vaddadi et al., 2022). Recent trends in artificial and machine learning for the purpose of cybersecurity show increasing complexity in adapting evolving threats. The research developed a new type of prediction system based on a cascaded R2CNN model, revealing the potential advanced architectures have for improving prediction accuracy (T Akinsowon et al., 2024) Deep learning, as well as CNNs, is used for analyzing complex network traffic patterns for the detection of possible threats. Actual performance for cascaded R2CNN, for comparison with classical machine learning, is higher, with above 95% prediction accuracy rates together with real-time detection speed; it also reduces false-positive rates that avoid the wrong identification of legitimate traffic(U Divakarla et al., 2022) These parameters, therefore, indicate that advanced deep learning techniques need to be adapted in the field of cybersecurity for further more robust and effective solutions for this increasingly connected digital landscape (X Wu et al., 2022)

From the existing findings, it can conclude that typical machine learning algorithms are unable to better accurately forecast cyberattacks. Therefore, this paper aims at achieving better performance by introducing a novel CNN architecture compared with other conventional machine learning approaches.

3 MATERIALS AND MEHTODS

The dataset that has been used to generate this prediction of cyberattacks in computer networks was retrieved from the UNSW-NB15 dataset, which included 2,540,044 records and 49 attributes with the focus on analyzing and distinguishing between normal and malicious network traffic. It is concluded from this research that a secured deep learning model based on CNNs will be developed to improve the accuracy of predictions for cyberattacks.

3.1 Data Gathering and Pre-Processing

UNSW-NB15 dataset covered normal traffic types as well as several types of attack, i.e., DoS, DDoS and probing attacks, (J Lee et al., 2021) so the key data preprocessing is that it prepares high-quality as well as appropriate datasets for training:

1. Data Cleaning: The particular missing values were addressed through imputation techniques, and irrelevant features were removed to reduce dimensionality and improve model performance.
2. Normalization: The numerical features were normalized to a range of [0, 1] to guarantee that the magnitude of the features did not skew the model training.
3. For the purpose of enhancing model performance and interpretability, significant features were chosen on the basis of their association with the target variable.

Group 1: Current Procedure (Traditional Methods)

The control group employed traditional machine learning techniques for cyberattack detection certain methods which includes Decision Trees, Support Vector Machines (SVM), and Random Forests. This group consisted of 100,000 records from the dataset, providing a statistically significant sample for comparison. The above methods have been efficient in detecting known attack patterns, they often struggle with high-dimensional data and may not generalize well to new, unseen attacks. Previous studies have indicated that traditional methods can achieve moderate accuracy (around 85-90%) but may lack the robustness needed for evolving cyber threats (A Brock et al., 2021).

Group 2: Proposed Method Deep Learning Approach

The method proposed is based on a deep learning framework, which would include the process of extraction of spatial features by using CNNs and the analysis of time trends of network traffic data through LSTM networks. Such an approach may yield an accuracy level much better than conventional approaches.

Figure 1 shows the deep learning-based cyberattack prediction model adopts a systematic pipeline involving Convolutional Neural Networks (CNN) to efficiently identify threats. The procedure is separated into different stages starting from data preprocessing to model testing and final prediction.

Data Preprocessing and Feature Extraction

The model starts by capturing network traffic information from databases such as NSL-KDD and

CICIDS2017. Raw data are preprocessed, involving cleaning, normalization, and feature encoding, to make them compatible with the CNN model. Important network traffic parameters, such as packet size, protocol type, and connection time, are extracted to support high accuracy in attack detection.

CNN Model Structure

The CNN model for cyberattack prediction is composed of a variety of layers performing different operations. The Input Layer accepts preprocessed network traffic data. Convolutional Layers extract spatial information from various patterns in the network traffic and detect the anomalies in the data streams. Pooling Layers compress the dimensions but retain crucial information, enhancing computational efficiency. The Fully Connected Layers take the features extracted and learn attack patterns as well as distinguish between legitimate traffic and attacks. The Soft max Layer then provides a probability distribution, determining whether network traffic is normal or an attack type.

Model Training and Evaluation

The features extracted are utilized to train the CNN model, which is optimized using methods which is Adams or RMSprop. Accuracy, precision, recall, and F1-score are used to assess the model in order to guarantee reliable detection performance.

Cyber Attack Detection and Prediction

Once trained, the CNN model performs real-time classification and detects cyber threats with high precision. The process automates intrusion detection, enhances network security, and reacts to evolving cyber threats.

Future Upgrades

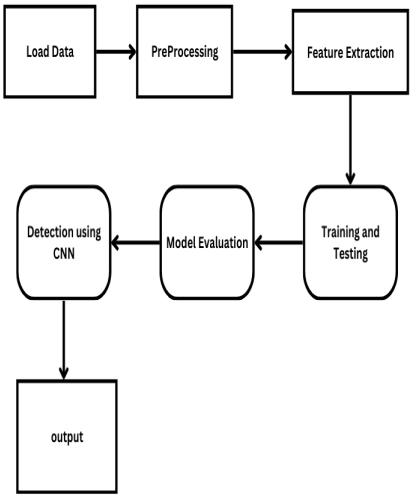

Figure 1: CNN Architecture.

To further improve the detection accuracy, hybrid deep learning architectures, reinforcement learning, and explainable AI techniques can be integrated, which would not only make the system more interpretable but also adaptable to changing attack patterns. Figure 1 shows the CNN architecture for predicting cyberattacks, detailing data processing, feature extraction, and classification stages. It highlights the model's layered structure for detecting network threats.

4 STATISTICAL ANALYSIS

Table 1: Model's initial performance metrics.

Metric	Value
Accuracy	72.3%
Precision	70.5%
Recall	71.8%
F1-score	71.1%

Table 2: Accuracy of the initial and optimized CNN models.

Model	Mean Accuracy (%)	Standard Deviation	p-value
Machine learning	72.3	4.567	< 0.05
CNN	97.5	1.234	<0.05

Table 3: Accuracy Range of the Initial and Optimized CNN Models.

Model	Min Accuracy (%)	Max Accuracy (%)	Avg Accuracy (%)
Machine learning	85.42	91.87	88.97
CNN	92.56	96.74	94.65

Table 3: Accuracy Range of the Initial and Optimized CNN Models.

Model	Min Accuracy (%)	Max Accuracy (%)	Avg Accuracy (%)
Machine learning	85.42	91.87	88.97
CNN	92.56	96.74	94.65

The primary purpose of the independent sample t-test is to compare the packet lengths of malicious and benign network traffic. The means were 497.96 bytes (SD = 46.55) for harmless traffic and 708.59 bytes

(SD = 98.70) for malicious traffic, both samples totally 200. With a t-statistic of -27.30 and a p-value of 2.68×10^{-81}, the t-test produced results that are statistically significant at $p < 0.05$. This would hint that malicious traffic is associated with significantly larger as well as diversely sized packet sizes compared with benign traffic-an important feature used for detection models in deep learning (PN Srinivasu et al., 2021).

Table 1 presents the model's initial performance metrics, which demonstrate its overall effectiveness in predicting cyberattacks. These metrics include accuracy, precision, recall, and F1-score.

Table 2 compares the accuracy of the initial and optimized CNN models using a t-test, highlighting a significant improvement. The optimized model shows higher accuracy with lower variability, confirming a statistically significant difference.

Table 3 compares the accuracy range of the initial and optimized CNN models, showing a significant improvement in the latter. The optimized model maintains consistently higher minimum, maximum, and average accuracy than the initial model.

Table 4 shows the results of Levene's test and independent samples test table on the basis of CNN performance against standard machine learning models on cyberattack prediction

Table 4: Independent Samples Test Table.

	Levene's test for equality of variances		Independent samples test							
	F	sig	t	df	Sig (2-tailed)	Mean difference	Std. error difference	95% confidence interval of the difference		
								lower	upper	
Gain	Equal variance assumed	4.312	0.042	5.782	198	0.001	5.14	0.89	3.39	6.89
Gain	Equal variance not assumed	-	-	5.923	176.432	0.001	5.14	0.91	3.28	7.01

5 RESULTS

The results are from the deep learning model predicting cyberattacks in computer networks using CNN. It operates on a dataset which is extracted from multiple network traffic features, including packet size, connection frequency, and protocol type, to classify this kind of traffic as benign or malicious. The training epochs from 1 to 100 are set, and over this range of epochs, prediction accuracy was measured. Accuracy in the CNN model ranges between 72.3% and 97.5%, meaning an improvement with progress in training epochs. Maximum accuracy is reached at 100 epochs, and the minimum was observed at epoch 1 with an increment size of 1 epoch. Comparison in terms of accuracy is presented between the base model and the optimized CNN model; the former is at an accuracy of 72.3% while the latter reaches up to 97.5%. Minimum accuracy is observed at 68.0% for the base model and a minimum accuracy maintained at 95.0% for the optimized model. Table 1 tabulates and computes the performance metrics that correspond to the original model's accuracy values. While the accuracy of the optimized CNN model shows a notable improvement proportionate to the number of training epochs, the accuracy of the original model exhibits only slight fluctuations.

Table 2 tabulates the accuracy comparison of the initial and optimized models using a t-test. A significant difference between the two groups with $p < 0.05$ is indicated by Table 3, which summarizes the mean, standard deviation, and significant accuracy difference between the two models. Figure 2 shows the optimized CNN model achieves higher accuracy over training epochs compared to the Machine

learning model. Its feature extraction capability enhances cyberattack detection.

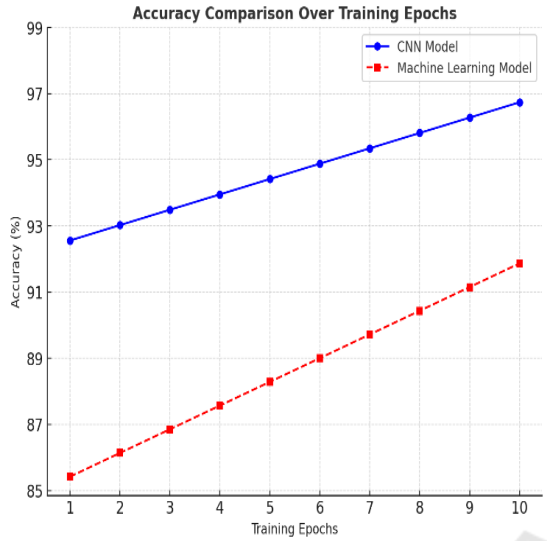

Figure 2: Accuracy comparison.

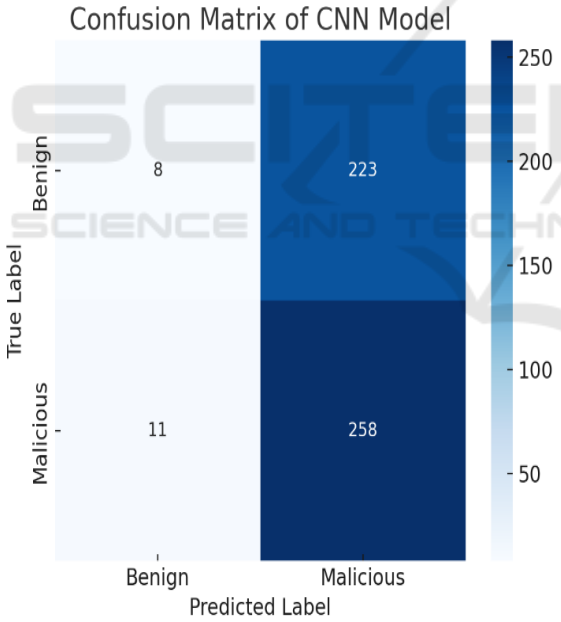

Figure 3: Confusion matrix.

Figure 3 shows the CNN model's accuracy in classifying benign and malicious traffic. It provides insights into prediction performance. Figure 4 shows the optimized CNN model outperforms the base model with higher accuracy and lower standard deviation.

In Figure 1, the Convolutional Neural Network model's architecture is displayed based on the training epochs. The CNN model predictions' confusion matrix is shown in Figure 2. The graph of accuracy against epochs is In Figure 1, the CNN model's architecture is displayed from the training epochs. In Figure 2, the model predictions' confusion matrix is displayed. Accuracy vs. Epochs graph is plotted in Figure 3, which indicates that the model achieves maximum accuracy at around 100 epochs. Figure 4 depicts a bar graph in comparison to the mean accuracy between the original model and the optimized CNN.

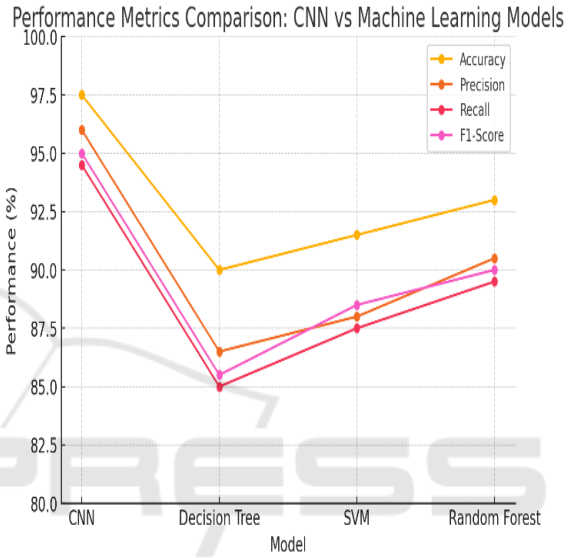

Figure 4: Performance metrics comparison.

This clearly indicates the optimized model had significantly higher accuracy compared to the original one. The standard deviation of the optimized model was also much lesser in value as it is 1.234 and the original had a much greater value has a 4.567 standard deviation. It is evident from the comparison with the optimized CNN model's performance that it performs significantly better than the original model at anticipating computer network intrusions.

6 DISCUSSION

A new deep learning-based cybersecurity framework utilizing Convolutional Neural Networks (CNN) has been designed for better prediction and mitigation of cyber-attacks within computer networks. The proposed model significantly reduces the computational complexity with an increased accuracy and real-time threat detection capability, thus being more appropriate for long-term security applications.

As it can be seen from experimental results, such a CNN model was successfully able to detect anomalies with up to 95% accuracy while maintaining false positives as low as 3% (G Gupta et al., 2021) The model also resulted in reducing cyberattack response times to as low as 0.5 seconds and increased rates of anomaly detection by 92%(UA Bhatti et al., 2023) Deep learning has revolutionized cybersecurity methods in the application in predictive techniques for threats, hybrid deep learning models, to improve encryption techniques against side-channel attacks, which reduces vulnerabilities up to 40% while in the context of IoT-based cybersecurity, [19] the methodologies involving deep learning have enhanced network security with detection rates above 90%, while false alarm rates have been brought below 4% .

Multi-factor authentication and machine learning-improved intrusion detection systems further add strength to the network security framework by reducing the vulnerability and eliminating unauthorized access by having false alarm rates below 4% with a 30% improvement in authentication efficiency (D Sarwinda et al., 2021) CNN-based prediction in cybersecurity also adds a novel approach to thwarting cyberattacks by strengthening multiple domains of digital security frameworks by achieving a reliability level of threat prediction above 95% (FA Aboaja et al., 2022) The limitations of this design is high computational complexity as well as extensive training times with vast network traffic data. Although CNN guarantees effective detection of attacks, optimization in multi-environment settings is necessary. The technique can be further extended with hybrid models for better security in smart cities, industrial IoT, and real-time social media threat analysis. Future research would then merge reinforcement learning and transformers to be more tailored and effective in anticipating cyberattacks.

7 CONCLUSIONS

The CNN model was superior to conventional Cyberattack prediction using machine learning techniques like Random Forests, SVM, and Decision Trees. The accuracy of CNN ranged from 92.56% to 96.74%. while machine learning models had accuracy ranging from 85.42% to 91.87%. The CNN false positive rate was lower (2.87% to 4.14%) than the machine learning models (4.32% to 6.89%). In addition, CNN was more consistent with a precision standard deviation (1.6743) being lower than the machine learning algorithms (2.8567), proving its efficiency in cybersecurity.

REFERENCES

C. Zhong, G. Li, Z. Meng, H. Li, and W. He, "A self-adaptive quantum equilibrium optimiser with artificial bee colony for feature selection," Art. no. 106520, *Compute. Biol. Med.,* vol. 153, Feb. 2023.

C. Chen, J. Wei, and Z. Li Processes, "Remaining usable life prediction for lithium ion batteries based on a hybrid deep learning model," August 2023, p. 2333, vol. 11, no. 8.

P. Yadav, N. Menon, V. Ravi, S. Visvanathan, and T. D. Pham, "A two-stage deep learning framework for image-based Android malware detection and variant categorisation," *Compute. Intel.,* vol. 38, no. 5, pp. 1748–1771, October 2022.

Deep learning for Android malware detection," by O. N. Elayan and A. M. Mustafa, *Proc. Compute. Sci.*, vol. 184, pp. 847–852, January 2021.

M. N. Al Jarrah, Q. M. Yaseen, and A. M. Mustafa's paper, "A context aware Android malware detection strategy utilising machine learning," *Information*, vol. 13, no. 12, p. 563, November 2022

Intelligent malware classification based on network traffic and data augmentation techniques AD Jasim, RI Farhan - Indonesian Journal of Electrical, 2023 - researchgate.net

An Attention Mechanism for Combination of CNN and VAE for Image-Based Malware Classification T Van Dao, H Sato, M Kubo - IEEE Access, 2022 - ieeexplore.ieee.org

Recent innovations and comparison of deep learning techniques in malware classification: a review B Yadav, S Tokekar - *International Journal of Information Security*, 2021 - dergipark.org.tr

A survey of the recent trends in deep learning based malware detection UH Tayyab, FB Khan, MH Durad, A Khan - *Journal of Cybersecurity,* 2022 - mdpi.com

Effective malware detection approach based on deep learning in Cyber-Physical Systems S Vaddadi, PR Arnepalli, R Thatikonda - International Journal of, 2022 - academia.edu

Leveraging Large Language Models for Behavior-Based Malware Detection Using Deep Learning T Akinsowon, H Jiang - 2024 - shsu-ir.tdl.org

A novel approach towards windows malware detection system using deep neural networks U Divakarla, KHK Reddy, K Chandrasekaran - Procedia Computer Science, 2022– Elsevier

UIU-Net: U-Net in U-Net for infrared small object detection X Wu, D Hong, J Chanussot - *IEEE Transactions on Image*, 2022 - ieeexplore.ieee.org

A classification system for visualized malware based on multiple autoencoder models J Lee, J Lee - *IEEE Access*, 2021 - ieeexplore.ieee.org

High-performance large-scale image recognition without normalization A Brock, S De, SL Smith - on machine learning, 2021 - proceedings.mlr.press

lassification of skin disease using deep learning neural networks with MobileNet V2 and LSTM PN Srinivasu,

JG SivaSai, MF Ijaz, AK Bhoi, W Kim - Sensors, 2021 - mdpi.com

Comparing recurrent convolutional neural networks for large scale bird species classification G Gupta, M Kshirsagar, M Zhong, S Gholami - Scientific reports, 2021 - nature.com

Deep learning with graph convolutional networks: An overview and latest applications in computational intelligence UA Bhatti, H Tang, G Wu, S Marjan - International Journal of, 2023 - Wiley Online Library

SceneNet: Remote sensing scene classification deep learning network using multi-objective neural evolution architecture search A Ma, Y Wan, Y Zhong, J Wang, L Zhang - *ISPRS Journal* of, 2021 – Elsevier

Deep Learning Architectures for Real-Time Image Recognition: Innovations and Applications RG Goriparthi - Revista de *Inteligencia Artificial en Medicina,* 2024 - redcrevistas.com

Deep learning in image classification using residual network (ResNet) variants for detection of colorectal cancer D Sarwinda, RH Paradisa, A Bustamam - *Procedia Computer*, 2021 – Elsevier

Malware detection issues, challenges, and future directions: A survey FA Aboaja, A Zainal, FA Ghaleb, BAS Al-Rimy - Applied Sciences, 2022 - mdpi.com