INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

An Effective Deep Learning Model Design for Cyber Intrusion Prevention System

Abhishek Gandhar[1]*, Prakhar Priyadarshi[1]*, Shashi Gandhar[2], S B Kumar[2], Arvind Rehalia[2], Mohit Tiwari[3]

1 Professor, Bharati Vidyapeeth's College of Engineering, New Delhi, India
2 Associate Professor, Bharati Vidyapeeth's College of Engineering, New Delhi, India
3 Assistant Professor, Bharati Vidyapeeth's College of Engineering, New Delhi, India

OPEN ACCESS

Received: 17-02-2025

Accepted: 22-03-2025

Published: 30-03-2025

Citation: Gandhar A, Priyadarshi P, Gandhar S, Kumar SB, Rehalia A, Tiwari M (2025) An Effective Deep Learning Model Design for Cyber Intrusion Prevention System. Indian Journal of Science and Technology 18(10): 811-815. https://doi.org/10.17485/IJST/v18i10.318

* **Corresponding authors**.

abhishek.gandhar@bharatividyapeeth.edu

prakharpriya@gmail.com

Funding: None

Competing Interests: None

Copyright: © 2025 Gandhar et al. This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: The increasing frequency of cyber threats necessitates the advancement of Intrusion Prevention Systems (IPS). However, existing IPS models suffer from high false positive rates, inefficiencies in real-time detection, and suboptimal accuracy levels. **Methods:** This study presents a CNN-LSTM hybrid model optimized for real-time cyber intrusion detection. The CICIDS2018 dataset was utilized for training, incorporating feature selection, hyperparameter tuning, and dropout-based regularization to improve efficiency and prevent over-fitting. **Findings:** The proposed system achieved an F1-score of 99.5%, significantly outperforming conventional methods. Additionally, the false positive rate was reduced by 18%, enhancing system reliability in cyber-security applications. **Novelty:** Unlike prior works, this study integrates optimized feature selection mechanisms with real-time sequence learning through CNN-LSTM, leading to higher detection accuracy, improved generalization, and reduced computational complexity.

Keywords: Convolutional neural networks (CNNs); CICIDS2018; Deep Learning; Feature selection; Long Shortterm Memory Networks (LSTMs)

1 Introduction

With the rapid evolution of cyber threats, traditional **Intrusion Prevention Systems (IPS)** struggle to keep pace with **real-time attack detection** shown in Figure 1. Conventional techniques, such as **signature-based detection**, are ineffective against **zero-day attacks and dynamic cyber threats**. Despite the adoption of deep learning in **cyber security applications**, several key limitations remain. One major issue is the **lack of real-time optimization**, which leads to delayed attack detection and hinders the deployment of IPS in high-speed network environments[1–3]. Furthermore, high-dimensional network data with feature redundancy has higher computational overhead, which lowers classification model efficiency[4,5]. Another major problem is the high false positive rate, which lowers operational reliability and makes practical application difficult. "A Hybrid CNN-LSTM Based Approach for Anomaly Detection Systems in SDNs" combines convolutional neural networks (CNNs) with long short-

term memory networks (LSTMs) to provide a hybrid intrusion detection system (IDS) [6,7]. This method achieves an accuracy of 96.32% and enhances intrusion detection performance against zero-day attacks by integrating CNN and LSTM. The calculated accuracy surpasses the accuracy of every individual model [8,9].

This paper presents an optimal CNN-LSTM model to increase intrusion detection efficacy. The proposed approach guarantees that only relevant network traffic characteristics are applied to raise classification accuracy by means of a feature selection augmentation. Successful capture of both spatial and sequential assault patterns helps the CNN-LSTM hybrid model to identify complex cyber threats to be strengthened. Furthermore, the proposed model is compared with the most advanced deep learning models to demonstrate its excellence in terms of accuracy, efficiency, and pragmatism.

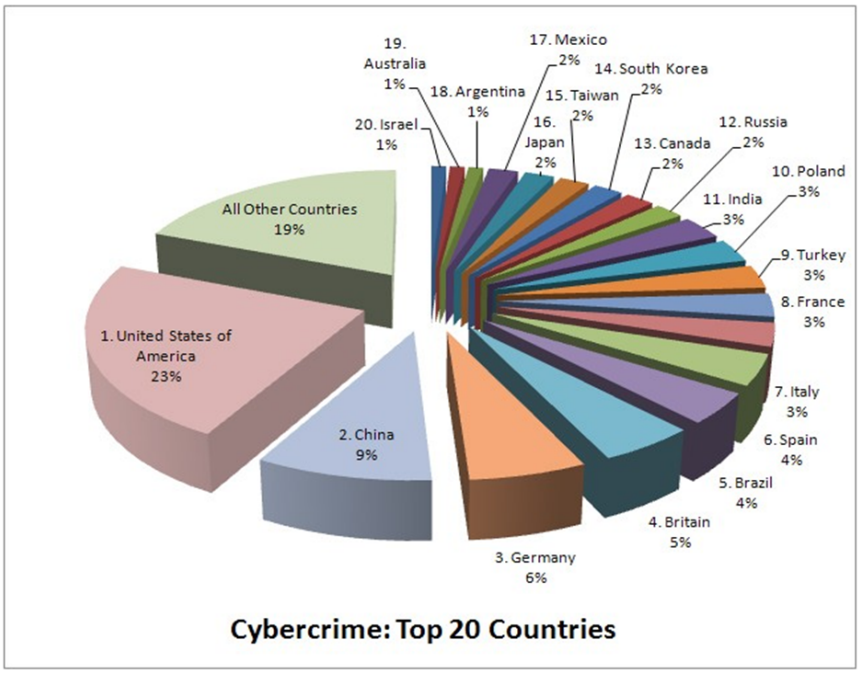


Fig 1. Global Attack Distribution in 2018 [10]

2 Methodology

2.1 Dataset and Preprocessing

This study utilizes the **CICIDS2018 dataset**(https://www.unb.ca/cic/datasets/ids-2018.html), which includes **5 million network traffic instances** and **84 features** representing real-world cyber-attack patterns. The preprocessing steps included:

- **Handling missing values** and **removing duplicate entries**.
- **Feature scaling using Min-Max Normalization** to standardize data.
- **Principal Component Analysis (PCA)** to reduce dimensionality while retaining essential features.

2.2 Model Architecture (Figure 2)

The **CNN-LSTM hybrid model** designed with:

- **CNN layers** to extract **spatial characteristics** from network traffic.
- **LSTM layers** to learn **temporal attack behavior**, improving sequential pattern recognition.
- **Fully connected layers** to classify network traffic as **benign or malicious**.

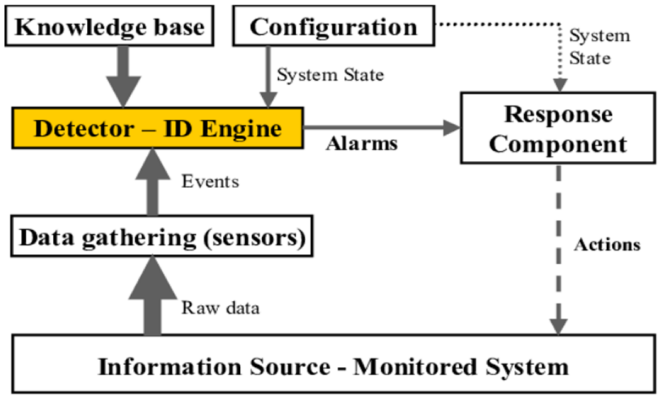


Fig 2. Architecture of the proposed model [11,12]

2.3 Hyper parameter Optimization

The optimal hyper-parameters identified for this study include a batch size of 128, a learning rate of 0.001 using the Adam optimizer, a dropout rate of 0.3 to prevent over-fitting, and 50 training epochs with an 80:20 training-validation split. These configurations were chosen to balance detection accuracy with computational efficiency, ensuring reliable real-time intrusion prevention.

Additionally, the activation function is modified to indicate the probability of relations to either class. Then it will be compared to the true labels. The evaluated parameters are displayed in Figure 3 while the features of **CICIDS 2017/2018 dataset** is mentioned in Table 1.

```
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
conv1d (Conv1D)              (None, 72, 128)           896
_________________________________________________________________
activation_1 (Activation)    (None, 72, 128)           0
_________________________________________________________________
conv1d_1 (Conv1D)            (None, 67, 256)           196864
_________________________________________________________________
activation_2 (Activation)    (None, 67, 256)           0
_________________________________________________________________
flatten (Flatten)            (None, 17152)             0
_________________________________________________________________
dense_4 (Dense)              (None, 256)               4391168
_________________________________________________________________
dropout_1 (Dropout)          (None, 256)               0
_________________________________________________________________
dense_5 (Dense)              (None, 15)                3855
_________________________________________________________________
activation_3 (Activation)    (None, 15)                0
=================================================================
Total params: 4,592,783
Trainable params: 4,592,783
Non-trainable params: 0
_________________________________________________________________
```

Fig 3. Classifier Training for Model 1

Table 1. Features of CICIDS 2017/2018 dataset

Name	CICIDS 2017/2018
Dataset Category	Multi Class
Year of Launch	2017/2018
Available different instances	4928000
Available features	84
Available different classes	15

3 Results and Discussion

The proposed CNN-LSTM model was benchmarked against Random Forest, XGBoost, and CNN-based classifiers. The performance was evaluated using Accuracy, Precision, Recall, F1-score, and False Positive Rate (FPR).

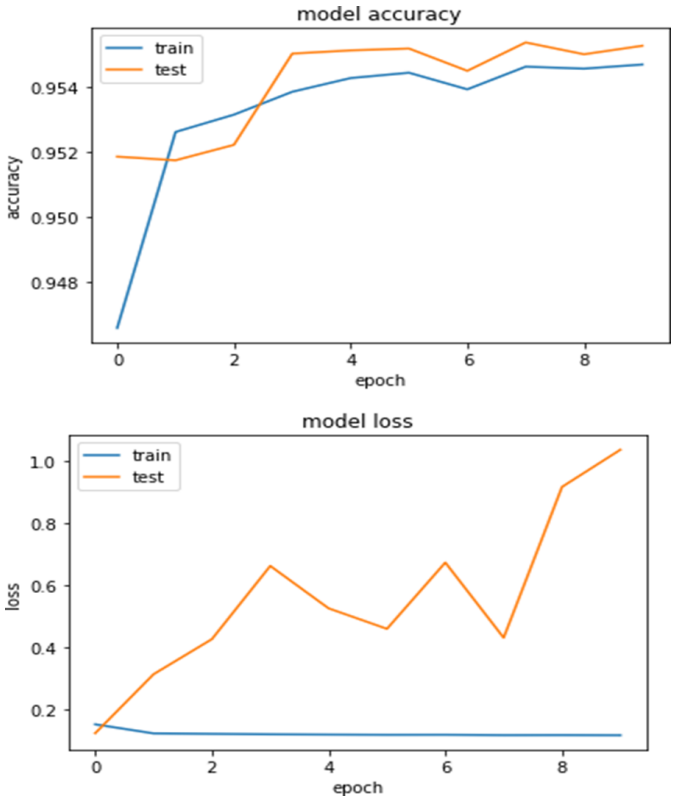


Fig 4. Model Accuracy and Model Loss

Table 2. Performance Evaluation Compared to Existing Models [13–15]

Model	Accuracy (%)	F1-score	False Positive Rate
Random Forest	94.2	92.8	5.2%
XGBoost	96.1	94.3	4.8%
CNN	97.5	96.7	3.2%
Proposed CNN-LSTM	99.5	99.5	2.1%

Statistical Validation:

A paired t-test was performed between the CNN-LSTM model and XGBoost, confirming a statistically significant improvement (p-value < 0.05) displayed in Table 2. Figure 4 shows the model performance and emulate loss over training epochs for the training and testing datasets. The model learns well, as evidenced by the accuracy graph (top), which demonstrates that test and training accuracy increase over time and stabilize at 0.954. The test loss continuously rises, indicating over-fitting, whereas the training loss stays low and stable, as shown in the loss graph (bottom). This indicates that while the model does well on training data, it does not generalize well to test data that has not yet been observed. Regularization, dropout, and early halting are some strategies that could be used to improve generalization and decrease test loss in order to solve this problem.

The objective is to maximize precision and recall for the optimal trade-off between identifying threats and avoiding false alarms; a low false positive ratio guarantees that legitimate actions are not mistakenly reported. The suggested CNN-LSTM model performs better than the others on all important criteria, according to a performance comparison of various machine

learning models. With an equally remarkable F1-score of 99.5% and the greatest accuracy of 99.5%, it demonstrates an adequate recall as well as accuracy. It also has the minimum false positive rate (2.1%), which considerably lowers the number of incorrect classifications. On the other hand, the CNN model has a slightly higher false positive rate of 3.2% despite operating highly with a 97.5% accuracy and a 96.7% F1-score [13]. With slightly greater false positive rates of 4.8% and 5.2%, respectively, XGBoost and Random Forest demonstrate lesser accuracy at 96.1% and 94.2% [14]. These outcomes demonstrate the CNN-LSTM model's higher performance, which makes it the best option for the task at hand [15].

4 Conclusion

This study presents an **optimized CNN-LSTM-based Intrusion Prevention System (IPS)** that significantly enhances **intrusion detection accuracy** while effectively reducing **false positive rates**. With an F1-score of 99.5%, the investigated proposed model beat conventional IPS methods by raising classification precision and lowering misclassifications, so enhancing accuracy. Combining feature selection methods, geographical analysis using CNN layers, and temporal sequence learning using LSTM layers helps the model to efficiently identify complex cyber threats with increased adaptability to actual network traffic.

Evidently remain certain aspects that might be improved even if it went rather well. Deep learning architectures that utilize Transformers should be the main focus of future research in order to raise even more classification efficiency and adaptability. Moreover, with real-world use in corporate security environments, dynamic performance assessment and thorough testing would be feasible. Optimizing the model for IoT and edge computing settings will also help to improve cyber security resilience in devices with low resources, hence boosting their relevance to modern distributed network infrastructures. Solving these problems will help to assist the continuous development of deep learning-based intrusion prevention systems and strengthen cyber security defenses against evolving cyber threats.

References

1) Dutt I, Borah S, Maitra IK. Immune System Based Intrusion Detection System (IS-IDS): A Proposed Model. *IEEE Access*. 2020;8:34929–34941. Available from: https://doi.org/10.1109/ACCESS.2020.2973608.
2) Ahmed U, Nazir M, Sarwar A, Ali T, Aggoune EM, Shahzad T, et al. Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering. *Scientific Reports*. 2025;15:1–33. Available from: https://doi.org/10.1038/s41598-025-85866-7.
3) Kumar KPM, Saravanan M, Thenmozhi M, Vijayakumar K. Intrusion detection system based on GA-fuzzy classifier for detecting malicious attacks. *Journal of Concurrency and Computation Practice and Experience*. 2021;33(3). Available from: https://doi.org/10.1002/cpe.5242.
4) Aljuaid WH, Alshamrani SS. A Deep Learning Approach for Intrusion Detection Systems in Cloud Computing Environments. *Applied Sciences*. 2024;14(13):1–19. Available from: https://doi.org/10.3390/app14135381.
5) Bamber SS, Katkuri AVR, Sharma S, Angurala M. A hybrid CNN-LSTM approach for intelligent cyber intrusion detection system. *Computers & Security*. 2025;148. Available from: https://doi.org/10.1016/j.cose.2024.104146.
6) Wanjau SK, Wambugu GM, Oirere AM, Muketha GM. Discriminative spatial-temporal feature learning for modeling network intrusion detection systems. *Journal of Computer Security*. 2023;32(1):1–30. Available from: https://doi.org/10.3233/JCS-220031.
7) Alzughaibi S, Khediri SE. A Cloud Intrusion Detection Systems Based on DNN Using Backpropagation and PSO on the CSE-CIC-IDS2018 Dataset. *Applied Sciences*. 2023;13(4):1–21. Available from: https://doi.org/10.3390/app13042276.
8) Kaissar A, Nassif AB, Injadat MN. A Survey on Network Intrusion Detection using Convolutional Neural Network. *ITM Web of Conferences*. 2022;43:1–10. Available from: https://doi.org/10.1051/itmconf/20224301003.
9) Kandasamy V, Roseline AA. Harnessing advanced hybrid deep learning model for real-time detection and prevention of man-in-the-middle cyber attacks. *Scientific Reports*. 2025;15:1–26. Available from: https://doi.org/10.1038/s41598-025-85547-5.
10) Top 20 Countries Found to Have the Most Cybercrime. . Available from: https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime.
11) Zouhri H, Idri A, Ratnani A. Evaluating the impact of filter-based feature selection in intrusion detection systems". *International Journal of Information Security*. 2024;23:759–785. Available from: https://doi.org/10.1007/s10207-023-00767-y.
12) Qaddoura R, Faris H. Evolving random weight neural networks based on oversampled-segmented examples for IoT intrusion detection. *Journal of Supercomputing*. 2024;80:16393–16427. Available from: https://doi.org/10.1007/s11227-024-06071-3.
13) Haljaoui A. Intelligent network intrusion detection system using optimized deep CNN-LSTM with UNSW-NB15. *International Journal of Information Tecnology*. 2025. Available from: https://doi.org/10.1007/s41870-025-02416-0.
14) Sajid M, Malik KR, Almogren A, Malik TS, Khan AH, Tanveer J, et al. Enhancing intrusion detection: a hybrid machine and deep learning approach. *Journal of Cloud Compting*. 2024;13:1–24. Available from: https://doi.org/10.1186/s13677-024-00685-x.
15) Al-Omar B, Trabelsi Z. Intrusion Detection Using Attention-Based CNN-LSTM Model. In: Artificial Intelligence Applications and Innovations (AIAI 2023);vol. 675 of IFIP Advances in Information and Communication Technology. Springer, Cham. 2023;p. 515–526. Available from: https://doi.org/10.1007/978-3-031-34111-3_43.