# INTEGRATED CNN AND LSTM WITH A CLASSIFIER FOR A CYBER-INTRUSION DETECTION SYSTEM

Shweta Lavaniya[1] and Sandeep Kumar Jain[2]

[1]Department of Computer Science, IET, Dr.Bhimrao Ambedkar University, Agra, India

## ABSTRACT

*The rapid growth of onlineusers and digital devices hasintensified the challenge ofensuring secure data transmissionover the openinternet. IntrusionDetection Systems (IDSs)and IntrusionPreventionSystems (IPSs) play a critical role in safeguarding organizations and their network infrastructure. To enhance security, AI-based approaches have gained prominence, as machine learning and deep learning techniques have demonstrated high effectiveness in this domain. In this study, we propose an integrated intrusion detection system that combines a Convolutional Neural Network (CNN) and Long Short-Term Memory(LSTM)network with an XG Boost classifier. The proposed model is trained and tested for binary classification on the synthesized real-world UNSW-NB15 dataset. The experimental results demonstrate that the model effectively classifies network traffic and validates its predictive performance.*

## KEYWORDS

*Intrusiondetection,CNN,LSTM,featureengineering,cybersecurity,machinelearning,deeplearning*

## 1. INTRODUCTION

An Intrusion Detection System (IDS) is a critical security mechanism designed to monitor, analyze, and identify suspicious activities within a network [5]. By continuously observing network traffic and system behaviors, IDS helps detect potential threats, such as unauthorized access attempts, malicious software activities with traffic patterns. Once suspicious behavior is identified, the system generates alerts for network administrators, enabling them to take immediate action to mitigate risks. In doing so, IDS not only strengthens the overall security posture of an organization but also reduces the likelihood of data breaches, service disruptions, and economic losses. There are different categories of IDS such as anomaly based IDS, signature-based IDS, host IDS, network IDS, etc [7]. Furthermore, modern IDS solutions often incorporateadvancedtechniquessuchasmachinelearninganddeeplearning, employing several information processing layers to improve detection accuracy, minimize false alarms, and adapt to evolving cyber threats [8][9]. The intrusion detection system based on deep learning techniques and an integrated approach is effective and the process of integrating CNN with LSTM to extract the features from the UNSW NB15 dataset and then stacked with boosting classifier is developed in this study.

## 2. BACKGROUND WORK

Jo et al. [1] constructed an Intrusion Detection System (IDS) using a Convolution Neural Network (CNN) with direct preprocessing, and proposed a preprocessing method for IDS based on the field-to-pixel philosophy, called Direct. This method utilized kernel attributes with reduced protocol data, offset, and field size. Additionally, they suggested two moretechniques—Compressed and Weighted—both of which required network information. The Direct method

Bibhu Dash et al: ICFCSAI-2025
pp. 143-149, 2026. IJCI – 2026 DOI:10.5121/ijci.2026.150115

applied field to-pixel conversion to demonstrate convolutional characteristics, whiletheother two methods, WeightedandCompressed, were usedto validatethe effectiveness of the Directmethod. Khan M. A. [2] presented a hybrid intrusion detection framework basedondeep learning. Hedevelopeda Convolutional Recurrent Neural Network(CRNN)-basedIDS capableof detectingandclassifyingnetworkattacks. Inthis framework, theCNN captures local attributes through convolution, while the Recurrent Neural Network (RNN) identifies temporal attributes. The model was evaluated using the publicly available CSE-CIC-IDS2018 dataset. Mendonça et al. [3] proposeda hierarchical Tree-CNN-basedIDS incorporatinga soft root sign activation function, which reduced model training time and computational complexity. The performance of the model was evaluated through implementation in a mid-sized company. Experimental results demonstrated a significant reduction in training time along with improved accuracy.

SeoW. andPakW. [4]developeda two-levelclassifier for intrusiondetection. Inthefirst level, real-time attacks in incoming network traffic are identified. If the first level fails to classify an instance, the classification is deferred until the flow terminates. In the second level, statistical attributes of the network flow are gathered for more precise classification. The proposed two-levelclassifierachievedbetterperformance intermsofbothdetectiontime andaccuracy.XiC.

[5] presented an intrusion detection model based on a multi-scale transformer, referred to as IDS-MTran. The model first employs a convolution operator with kernels to extract multi scale attributes. It then utilizes a pooling–patching bridge to enhance branch interaction and improve feature representation. The multi-scale transformer models the attributes at a wider scale, enabling more effective intrusion detection. In addition, a cross-feature enrichment mechanism was proposed to fully exploit the potential of multi-scale branches. Experimented with the accuracy on NSL-KDD, CIC-DDoS 2019, and UNSW NB15 dataset.

W is anwanichthan and Thammawichai [6] introduced a double-layered hybrid approach to address the limitations of single classifiers in detecting uncommon attacks such as Remote-to-Local (R2L) and User-to-Root (U2R). They utilized Principal Component Analysis (PCA) to analyzedifferent attack classes. In theproposed approach, thefirst layer employed NaïveBayes to detect DoS and Probe attacks, while the second layer used Support Vector Machines (SVM) to classify R2L and U2R samples. The model was trained and tested on the NSL-KDD dataset. Al-Daweri et al. [7]analyzed attributes fromtheKDD99and UNSW-NB15 datasets usingthree methods: Rough Set Theory (RST), a discrete variant of the Cuttlefish Algorithm, and a Backpropagation Neural Network (BPNN). First, they used RST to analyze attributedependency ratios. The results of RST were then used as inputs to the BPNN for classifying samples into different classes. Feature extraction was carried out through multiple iterations.The experiments demonstrated improved accuracy for certain attributes of the KDD99 dataset, withsomefeatures contributingsignificantlytoclassificationperformance. Thestudyconcluded that a lightweight and precise IDS with fewer selected attributes can aid cybersecurity researchersindevelopingefficientintrusiondetectionsystems. Wangetal. [8]designeda CNN- based IDS aimed at providing an efficient, automated, and real-time system. The model utilized open-source tools such as Tcpdump, Bro, and TensorFlow for packet capture, traffic analysis, and machine learning, respectively. The system comprised data preprocessing, followed by training and testing using the publicly available NSL-KDD dataset. Mohammadpour et al. [12] employed an advanced deep learning approach to develop a detection system addressing key challenges such as flexibility, effectiveness, high false alarm rates, and low detection accuracy. Their CNN-based IDS was trained and evaluated using the NSL-KDD dataset, achieving an accuracy of 99.79% in experimental results.

## 3. PROPOSED INTEGRATED IDS MODEL AND METHODOLOGY

This section presents the proposed IDS model for intrusion detection, including details of its architecture and the workflow from data loading and preprocessing to model-specific tuning. The model is trained and evaluated on a widely used dataset that provides insightful attributes and encompasses various types of attacks. The experimental results demonstrate that the proposed approach outperforms previous research.

### 3.1. Data Pre-Processing

The data was loaded and pre processed in several steps represented in fig 1. First, feature selection was performed by dropping the attack_cat column while retaining the binary label, and low-variance features were discarded to reduce noise. Next, label encoding was applied to convert categorical variables into numerical features. Afterward, the data was standardize dusing Standard Scaler to approximate a normal distribution. The resulting dataset was then split into training and testing sets. Since the dataset used for model training was highly imbalanced, which ledtopoor modelperformance, weappliedSMOTE oversamplingtobalancethesamples effectively.

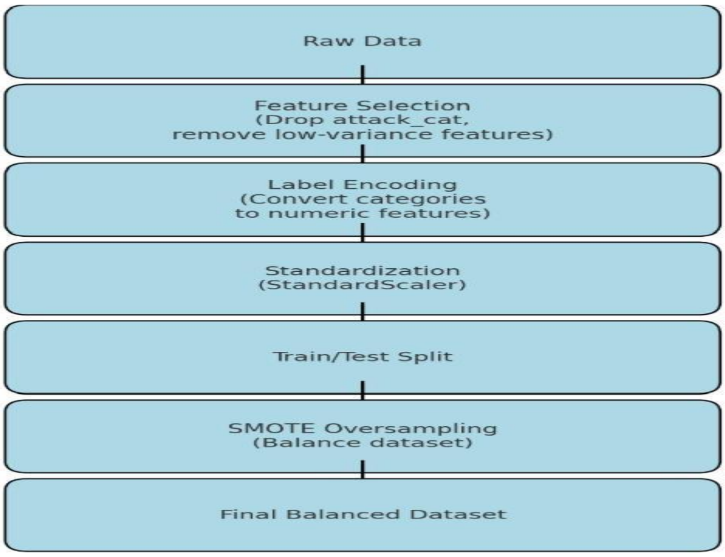

Figure1.Data preprocessing process

### 3.2. Model Architecture

This section discusses the simulated model and its layer arrangement. The system developed in this study integrates a 1D Convolutional Neural Network (Conv1D) with an LSTM for feature extraction, followedbya boostingclassifier. As summarizedinTable1, thepre-processedinput sequence (features) is first passed to a Conv1D layer to extract local patterns, followed by a max-pooling layer witha poolsizeof2 anda dropout rateof0.3. Next, anLSTM layer captures temporalattributes, alsowitha dropout rateof0.3, and is followedbya denselayer. Finally, the output layer uses a sigmoid activation function to classify samples as normal or abnormal. The model was trained for 20 epochs with a batch size of 128, using the Adam optimizer with a learning rate of 0.001. The model classifies the test sample using an XGBoost classifier with 1000 estimators, depth = 10, and a learning rate of 0.03.

Table1. Proposed model simulation design

| | |
|---|---|
| **Conv1D** | 64filters,kernel=3,relu |
| **Maxpooling** | Poolsize=2 |
| **LSTM** | 128units |
| **Dense** | 128,relu |
| **Output** | sigmoid |

### 3.3. Result and Discussion

The evaluation metrics used to assess the model's performance are presented in Table 2, including precision, recall, F1-score, and an overall accuracy of theproposed integrated IDS for binaryclassificationis 97.47%. Inaddition, various visualizations (fig:2-4)areprovidedto give a clearer understanding of the model's behaviour. These metrics were calculated using:

- ✓ Accuracy=(TP+TN)/(TP+TN+FN+FP)
- ✓ Precision=TP/(TP+FP)
- ✓ Recall=TP/(TP+FN)
- ✓ F1score=2*(precision*recall)/(precision+recall)

Table2:Evaluation matrix for binary classification

| | Precision | Recall | F1score | Support |
|---|---|---|---|---|
| Normal | 0.95 | 0.98 | 0.97 | 18600 |
| Attack | 0.99 | 0.97 | 0.98 | 32935 |

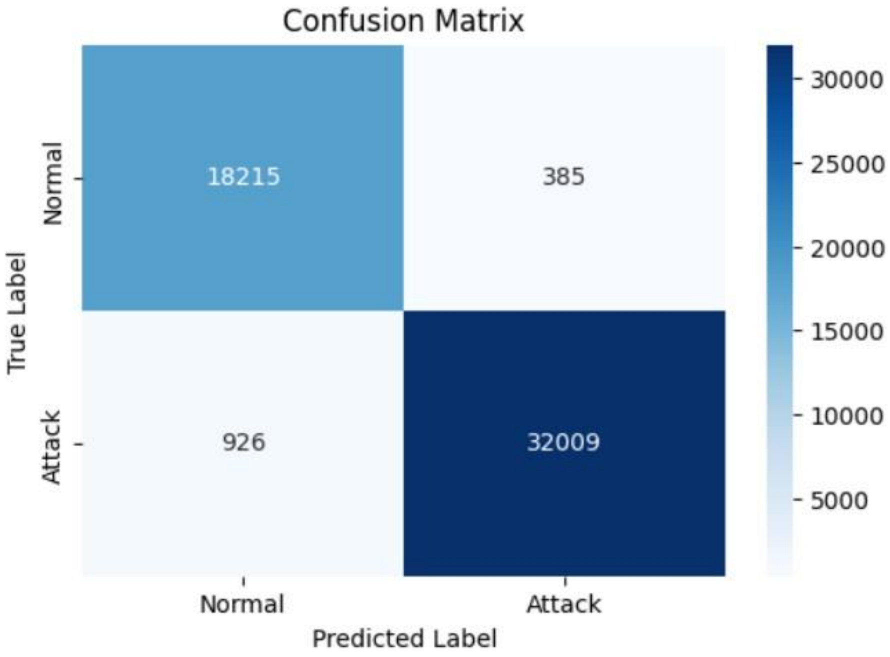

Figure2.Confusion matrix for binary classification

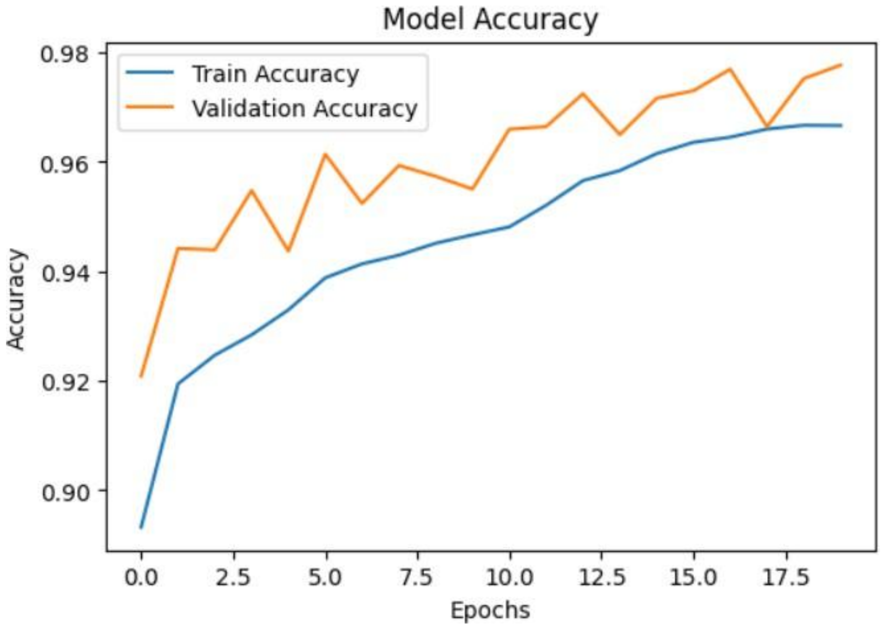

Figure3.Binary classification model accuracy

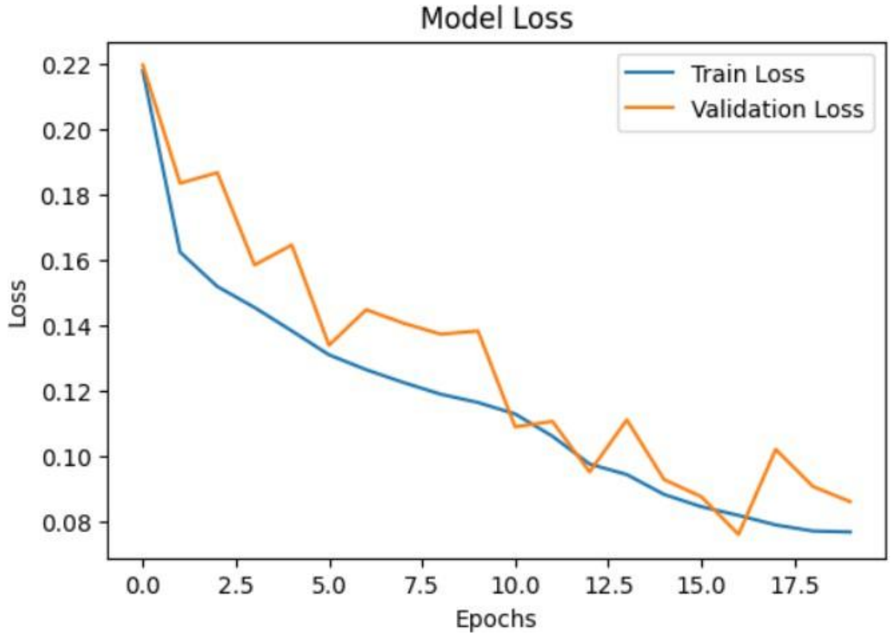

Figure4.Binary classification model loss

## 3.4. References

References should be cited in the main text, in passing [1] or explicitly as in [2].The full references should be given as below (essentially IEEE format), in the order in which they are cited, in 10 pt. Times New Roman, with a 6pt spacing between each.

# 4. CONCLUSIONS

In this work, we present an integrated approach that combines a Convolutional Neural Network (CNN) to extract local features with a Long Short-Term Memory (LSTM) network to capture temporal features. These components are further stacked with a boosting classifier to perform binary classification of network traffic as either normal or abnormal. The proposed detection system was trained and tested on the publicly available UNSW-NB15 dataset, achieving an accuracy of 97%. This method demonstrates the effective integration of machine learning and deep learning techniques for intrusion detection. The feasibility of the system is validated through its implementation, as detailed in the model architecture and results sections. The system is capable of monitoring network traffic in real time and detecting suspicious activities. In future work, we plan to extend this approach to further improve performance byincorporating a multi-class classification model and evaluating the system with additional metrics such as detection rate, false alarm rate, and others.

## REFERENCES

[1] W. Jo, S. Kim, C. Lee, and T. Shon, “Packet preprocessing in CNN-based network intrusion detection system,” *Electronics*, vol. 9, no. 7, p. 1151, 2020.

[2] M. A. Khan, “HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system,” *Processes*, vol. 9, no. 5, p. 834, 2021, doi: 10.3390/pr9050834.

[3] R.V.Mendonça,A.A.Teodoro,R.L.Rosa,M.Saadi,D.C.Melgarejo,P.H.Nardelli,andD.

[4] Z. Rodríguez, “Intrusion detection system based on fast hierarchical deep convolutional neural network,” *IEEE Access*, vol. 9, pp. 61024–61034, 2021.

[5] W. Seo and W. Pak, “Real-time network intrusion prevention system based on hybrid machine learning,” *IEEE Access*, vol. 9, pp. 46386–46397, 2021.

[6] C. Xi, H. Wang, and X. Wang, “A novel multi-scale network intrusion detection model with transformer,” *Scientific Reports*, vol. 14, no. 1, p. 23239, 2024.

[7] T. Wisanwanichthan and M. Thammawichai, “A double-layered hybrid approach for network intrusion detection system using combined naive Bayes and SVM,” *IEEE Access*, vol. 9, pp. 138432–138450, 2021.

[8] M. S.Al-Daweri,K.A.ZainolAriffin,S. Abdullah,andM.F. E. Md.Senan,“An analysisofthe KDD99 and UNSW-NB15 datasets for the intrusion detection system,” *Symmetry*, vol. 12, no. 10, p. 1666, 2020.

[9] H. Wang, Z. Cao, and B. Hong, “A network intrusion detection system based on convolutional neural network,” *Journal of Intelligent & Fuzzy Systems*, vol. 38, no. 6, pp. 7623–7637, 2020.

[10] Aleesa, M. O. H. A. M. M. E. D. Younis, A. A. Mohammed, and N. Sahar, “Deep-intrusion detection system with enhanced UNSW-NB15 dataset based on deep learning techniques,” *Journal of Engineering Science and Technology*, vol. 16, no. 1, pp. 711–727, 2021.

[11] G.Logeswari, S. Bose, andT. J.Anitha, “An intrusion detection system for SDNusingmachine learning,” *Intelligent Automation & Soft Computing*, vol. 35, no. 1, pp. 867–880, 2023.

[12] E. Alpaydin, “Multilayer perceptrons,”in *IntroductiontoMachine Learning*, 3rded. Cambridge, MA, USA: MIT Press, 2014, pp. 267–316.

[13] L. Mohammadpour, T. C. Ling, C. S. Liew, and C. Y. Chong, “A convolutional neural network for network intrusion detection system,” in *Proc. Asia-Pacific Advanced Network*, vol. 46, pp. 50–55, 2018.

## AUTHORS

**Shweta Lavaniya** holds an M.Sc. in Computer Science and has qualified the UGC-NET examination in the same discipline. She is currently pursuing her Ph.D. at Dr. Bhimrao Ambedkar University, Agra. Her research interests include cybersecurity and emerging areas of computer science and information technology. She has presented three papers at national and international conferences and possesses over two years of teaching experience in higher education, where she has actively contributed to academic instruction, student

**Dr. Sandeep Kumar Jain** is a Professor in the Department of Computer Science at Dr. Bhimrao Ambedkar University Agra. He holds a Ph.D. in Computer Science from thesameUniversity. Hehasnearly30 years ofteaching experiencetoPG classes. His research interest includes software reliability, computer network, network security and machine learning. Dr. Jain has published twelve research papers in thereputed journals.