Deep Learning Models for Advanced Intrusion Detection in Next-Generation Networks

Abstract

The rapid evolution of next-generation networks like Software Defined Networks (SDN), Internet of Things (IoT), and 5G infrastructures has made cybersecurity issues extremely complex. The traditional intrusion detection system (IDS) mostly depends upon signature-based intrusion detection techniques that fail to detect sophisticated and unknown cyber attacks. Therefore, the integration of deep learning techniques with intrusion detection has become a promising solution to improve network security. In this paper, a deep learning-based intrusion detection framework has been proposed to detect complex and unknown attacks in next-generation networks. The proposed framework uses a hybrid deep learning architecture that combines Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to detect unknown attacks in next-generation networks. The proposed framework has been evaluated using benchmark datasets like NSL-KDD and UNSW-NB15 datasets that contain different categories of network attacks like DoS, Probe, R2L, and U2R attacks. The experimental results have been compared with other machine learning algorithms like Support Vector Machines (SVM), Random Forest (RF), and K-Nearest Neighbors (KNN), which prove that the proposed hybrid deep learning architecture outperforms other machine learning algorithms in intrusion detection. The accuracy of the proposed model is 98.6%, precision of 97.9%, recall of 98.2%, and F1-score of 98.0%. Moreover, the proposed system has the potential to reduce false alarm rates and improve detection capabilities for zero-day attacks. The results of this study have demonstrated the potential of deep learning-based intrusion detection systems to improve network security in advanced network infrastructures. The proposed framework has the potential to provide a scalable and intelligent solution for detecting emerging threats in advanced network infrastructures. Future research will investigate federated learning and explainable artificial intelligence approaches to improve the flexibility of intrusion detection systems.

Keywords: Intrusion Detection System, Deep Learning, CNN, LSTM, Cybersecurity, Network Security, Next-Generation Networks.

Introduction

With the rapid development of digital technology, modern networks have become more complex and interconnected [1], [2]. With the advent of next-generation network technologies such as 5G, Cloud Computing, Software Defined Network (SDN), and Internet of Things (IoT) technology, the threat of cyber threats has increased manifold [3], [4]. These technologies can be used for a high volume of data transmission and can be used for real-time communication [5]. Therefore, network security has become a major challenge for organizations and governments around the globe. Intrusion Detection Systems (IDS) are used to monitor network activity and detect malicious activity [6]. Conventional Intrusion Detection Systems can be broadly classified into signature-based intrusion detection systems and anomaly-based intrusion detection systems [7], [8]. Signature-based intrusion detection systems depend on a database containing a list of attack signatures [9]. This type of intrusion detection system is effective against known attacks but is ineffective against zero-day attacks. Anomaly-based intrusion detection systems detect network activity anomalies but are prone to high false alarm rates [10]. Several machine learning techniques have been employed for enhancing the performance of intrusion detection systems [11]. Techniques such as Support Vector Machines (SVM), Decision Trees (DT), Random Forest (RF), and K-Nearest Neighbor (KNN) have shown good results in detecting intrusions in a network. However, these techniques face difficulties in handling high-dimensional data related to network traffic. Moreover, for dealing with evolving types of attacks in modern computing systems, advanced techniques are needed that can learn automatically [12], [13]. Recently, deep learning techniques have been recognized for their ability to learn automatically in various cybersecurity applications. Deep learning techniques include Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) networks. These techniques have shown good results in detecting various types of attacks in a network. Deep learning techniques can learn automatically from large amounts of data and can analyze complex types of attacks in a network [14], [15].

The proposed research in this paper suggests the idea of a hybrid deep learning technique that incorporates the CNN and LSTM models for the detection of sophisticated attacks in the context of next-generation network systems [16], [17]. The CNN model is utilized to detect the spatial features of the network traffic data, whereas the LSTM model is utilized to detect the temporal features of the network traffic data [18]. The contributions of the proposed research can be summarized as follows:

- Development of a hybrid CNN-LSTM Deep Learning Architecture for Intrusion Detection.
- Evaluation of the proposed model using existing intrusion detection datasets.
- Comparison of the proposed model with existing machine learning algorithms.
- Detection accuracy, precision, recall, and false alarm analysis.

The rest of the paper is organized in the following manner. In Section 2, we discuss the existing research works in machine learning and deep learning-based intrusion detection systems. In Section 3, materials and methods used in this research are discussed. In Section 4, experimental results and performance evaluations are discussed. Finally, in Section 5, conclusions and future research directions are given.

Related Works

Several researchers have worked on various machine learning and deep learning techniques for intrusion detection systems. Earlier models of IDS used statistical and rule-based techniques [19], [20]. However, with the increase in complexity of attacks, researchers have started using intelligent machine learning techniques for accurate results. The first publicly available dataset for IDS was the KDD Cup '99 dataset. Later, researchers like Tavallaee et al. proposed a new dataset called NSL-KDD to overcome the redundancy and imbalance problems in the original KDD Cup '99 dataset [21]. Machine learning algorithms like Support

Vector Machine (SVM), Random Forest (RF), and Decision Trees (DT) have been utilized for intrusion detection [22], [23]. The algorithms have been able to achieve reasonable accuracy in detecting network intrusions [24]. However, they require feature engineering and data preprocessing, which can be tedious. Additionally, traditional machine learning algorithms have limitations in detecting complex cyber attacks, especially multi-stage attacks [25]. Deep learning models have been receiving significant research attention in recent times, especially for their potential in learning complex patterns from data [26]. Kim et al. proposed a deep neural network model for network intrusion detection using stacked autoencoders [27]. The proposed model was able to attain higher classification accuracy compared to traditional machine learning models [28].

Convolutional Neural Networks (CNN) have also been used to deal with intrusion detection issues. The CNN architecture has been effective in extracting spatial features from network data through the analysis of packet structures and flows [29]. Yin et al. proposed a deep learning-based intrusion detection system using CNN and reported promising results with the NSL-KDD dataset. Recurrent Neural Networks (RNN) and LSTM networks have been used to analyze network data [30]. These networks have been effective in dealing with time-series data in networks, which is essential in intrusion detection since attacks may be multi-stage attacks. Research carried out by Hochreiter and Schmidhuber showed that LSTM networks outperform RNN networks in dealing with long-term dependencies [31]. Hybrid deep learning models, which combine CNN and LSTM, have also been proposed for improving the performance of intrusion detection systems. The proposed hybrid models utilize the feature extraction ability of CNN and the temporal analysis ability of LSTM for improving intrusion detection accuracy [32]. Research has revealed that hybrid deep learning models can effectively detect intrusion attacks, even though they individually perform poorer than other deep learning models [33]. Even though significant research has been conducted on intrusion detection for next-generation networks, there are still some challenges that need to be addressed for the deployment of intrusion detection systems in real-world scenarios.

Materials and Methods

System Architecture

The proposed intrusion detection framework consists of five main components shown in Figure 1:

Data Collection

Data Preprocessing

Feature Extraction

Deep Learning Model Training

Intrusion Detection and Evaluation

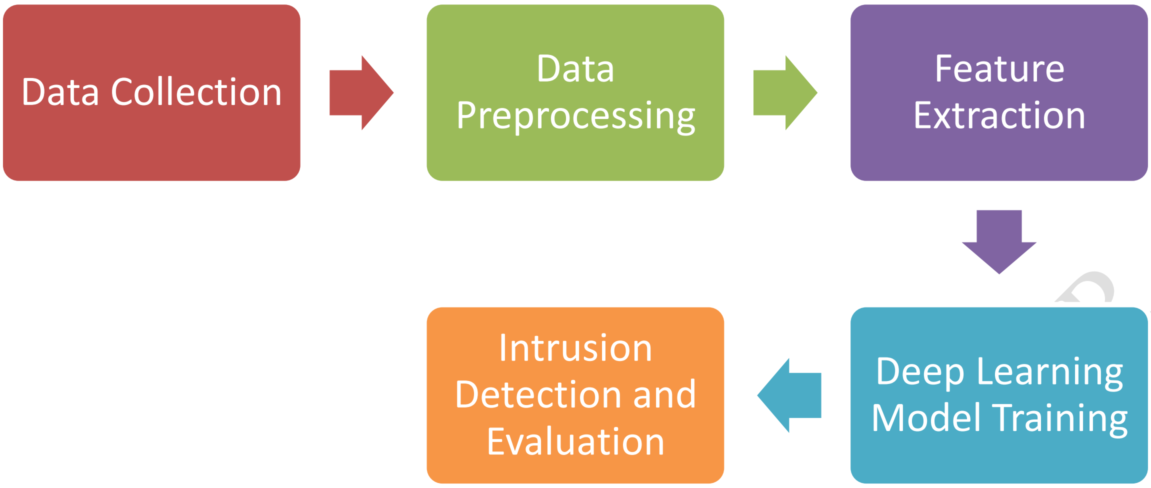
Data Collection
Data Preprocessing
Feature Extraction
Deep Learning Model Training
Intrusion Detection and Evaluation

Figure 1: Proposed architecture

Dataset Description

Two publicly available datasets were used in Table 1:

Table 1: Dataset

Dataset	Instances	Features	Attack Types
NSL-KDD	125973	41	DoS, Probe, R2L, U2R
UNSW-NB15	257673	49	Generic, Exploits, Fuzzers

These datasets include both normal network traffic and various types of cyber attacks.

Data Preprocessing

The following preprocessing steps were applied:

Data cleaning and removal of duplicate records

Encoding of categorical attributes using one-hot encoding

Normalization using Min-Max scaling

Splitting dataset into training and testing sets (70:30)

Normalization formula: The equation 1 shows the normalization.

$$X_{Norm} = \frac{X - X_{min}}{X_{max} - X_{min}} \qquad (1)$$

Proposed Deep Learning Model

The proposed deep learning model will be a combination of CNN and LSTM models.

CNN Component: CNN will be responsible for extracting spatial features from network traffic.CNN layers:

Convolution Layer

ReLU Activation

Max Pooling Layer

Flattening Layer

LSTM Component: LSTM will be responsible for extracting sequential dependencies from network flows.

LSTM Gate Equations: The LSTM gate equation 2, equation 3, and equation 4 are mentioned below. The CNN LSTM architecture is shown in Figure 2.

$$f_t = \sigma\left(W_f[h_{t-1}, x_t] + b_f\right) \qquad (2)$$

$$i_t = \sigma(W_i[h_{t-1}, x_t] + b_i) \qquad (3)$$

$$o_t = \sigma(W_o[h_{t-1}, x_t] + b_o) \qquad (4)$$

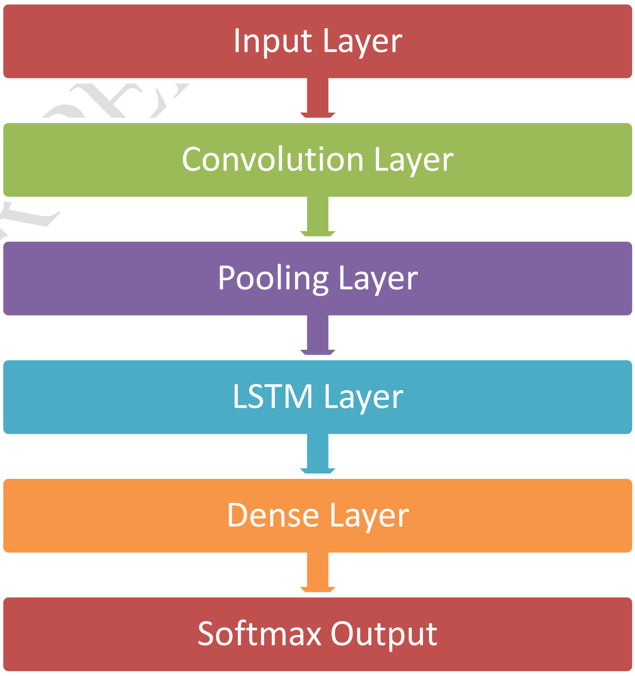

Figure 2: CNN LSTM architecture

Training Parameters: The training parameter is shown in Table 2.

Table 2: Training parameter

Parameter	**Value**
Epochs	50
Batch Size	128
Learning Rate	0.001
Optimizer	Adam
Activation	ReLU

Performance Metrics

Evaluation metrics used is shown in Table 3.

Table 3: Performance metrics

Metric	**Formula**	**Description**
Accuracy	(TP + TN) / (TP + TN + FP + FN)	Overall classification correctness
Precision	TP / (TP + FP)	Correct positive predictions
Recall	TP / (TP + FN)	Ability to identify true positives
F1 Score	2 × (Precision × Recall) / (Precision + Recall)	Balance between precision and recall
AUC-ROC	Area under ROC curve	Classification discrimination ability

Results

The proposed deep learning model was evaluated with NSL-KDD and UNSW-NB15 datasets. The performance of CNN-LSTM was compared with other traditional machine learning techniques like SVM, Random Forest, and KNN. The performance comparison is shown in Table 4.

Table 4: Performance comparison

Model	Accuracy	Precision	Recall	F1 Score
SVM	91.4	90.1	89.8	90
Random Forest	94.6	93.9	94.2	94
KNN	92.3	91.7	91.2	91.4
CNN	96.8	96.2	96	96.1
Proposed CNN-LSTM	98.6	97.9	98.2	98

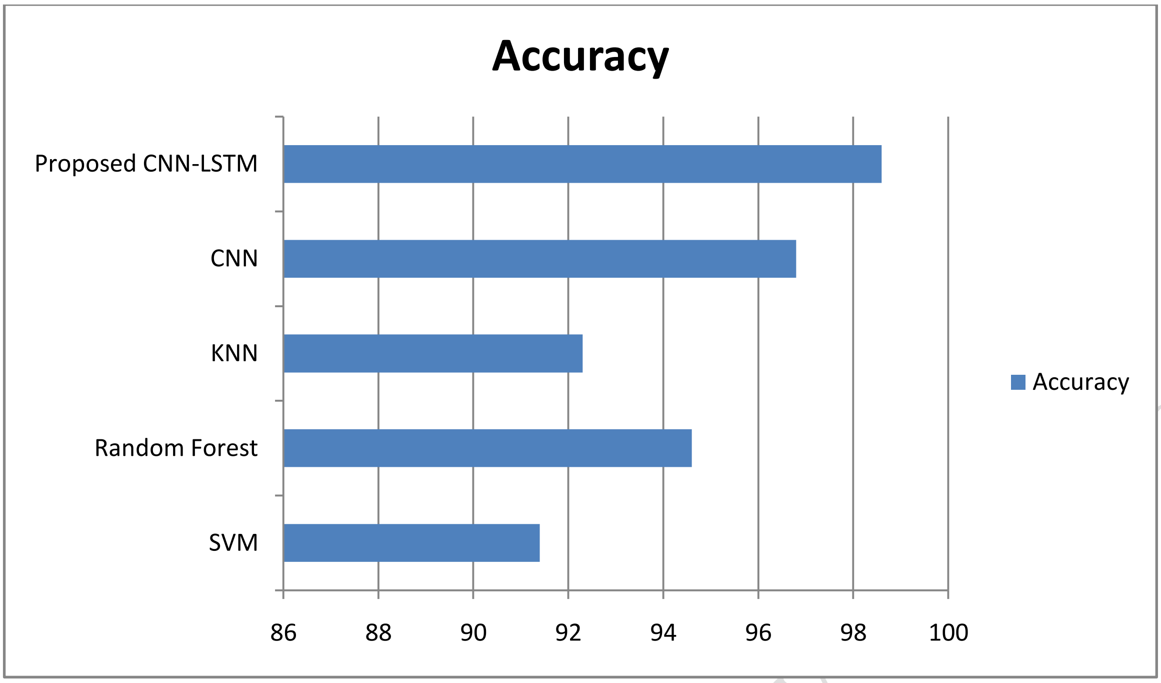

Figure 3: Accuracy Comparison Graph

As seen in the results, the hybrid model of CNN-LSTM performs better than other models, especially in the detection of known and unknown attacks. The hybrid model reduces false positives while improving the accuracy of detection.

Conclusion

This study presented a hybrid framework of deep learning models for enhanced intrusion detection systems for next-generation networks. The model utilizes a combination of Convolutional Neural Networks and Long Short-Term Memory models to extract both spatial and temporal features of network traffic data. The results obtained by implementing the CNN-LSTM model on standard data sets showed that it performs better than conventional machine learning algorithms in terms of accuracy, precision, recall, and F1-score.The proposed model offers an intelligent solution for detecting complex intrusion attacks on modern network infrastructures. Future studies will concentrate on incorporating Explainable AI models and Federated Learning models to further enhance the transparency and scalability of intrusion detection systems.

References

1. T. Tavallaee et al., “A detailed analysis of the KDD CUP 99 dataset,” IEEE CISDA, 2009.
2. M. Tavallaee et al., “NSL-KDD dataset for network intrusion detection,” IEEE, 2009.
3. M. H. Bhuyan, D. Bhattacharyya, and J. K. Kalita, “Network anomaly detection,” IEEE Communications Surveys, 2014.
4. I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. MIT Press, 2016.
5. S. Kirmani and P. Raghavan, “Scalable parallel graph partitioning,” in SC ’13: Proceedings of the International Conference on High Performance Computing, Networking, Storage and Analysis, 2013, pp. 1–10, doi: 10.1145/2503210.2503280.

6. M. Nadeem, P. C. Pathak, M. Ahmad, and N. A. Farooqui, “Identification of security factors in cloud computing: Defence security perspective,” in Computational Intelligence Applications in Cyber Security, CRC Press, 2024, pp. 78–99.
7. M. Nadeem et al., “Deep Learning Approach for Classifying DDoS Attack Traffic in SDN Environments,” J. Inf. Secur. Cybercrimes Res., vol. 7, no. 2 SE-, pp. 109–126, Dec. 2024, doi: 10.26735/VNFU3495.
8. F. Kirmani, B. J. Lane, and J. R. Rose, “Exploring Machine Learning Techniques to Improve Peptide Identification,” in 2019 IEEE 19th International Conference on Bioinformatics and Bioengineering (BIBE), 2019, pp. 66–71, doi: 10.1109/BIBE.2019.00021.
9. M. Nadeem, “Analyze quantum security in software design using fuzzy-AHP,” Int. J. Inf. Technol., 2024, doi: 10.1007/s41870-024-02002-w.
10. W. Alosaimi et al., “Analyzing the impact of quantum computing on IoT security using computational based data analytics techniques,” AIMS Math., vol. 9, no. 3, pp. 7017–7039, 2024, doi: 10.3934/math.2024342.
11. S. Kirmani, J. Park, and P. Raghavan, “An embedded sectioning scheme for multiprocessor topology-aware mapping of irregular applications,” Int. J. High Perform. Comput. Appl., vol. 31, no. 1, pp. 91–103, 2017, doi: 10.1177/1094342015597082.
12. A. Attaallah, S. Khatri, M. Nadeem, S. A. Ansar, A. K. Pandey, and A. Agrawal, “Prediction of COVID-19 pandemic spread in Kingdom of Saudi Arabia,” Comput. Syst. Sci. Eng., vol. 37, no. 3, 2021, doi: 10.32604/CSSE.2021.014933.
A. Alharbi et al., “Managing Software Security Risks through an Integrated Computational Method,” Intell. Autom. Soft Comput., vol. 28, no. 1, p. 179, Mar. 2021, doi: 10.32604/IASC.2021.016646.
13. S. Kirmani, H. Sun, and P. Raghavan, “A Scalability and Sensitivity Study of Parallel Geometric Algorithms for Graph Partitioning,” in 2018 30th International Symposium on Computer Architecture and High Performance Computing (SBAC-PAD), 2018, pp. 420–427, doi: 10.1109/CAHPC.2018.8645916.
14. A. Alharbi et al., “Selection of data analytic techniques by using fuzzy AHP TOPSIS from a healthcare perspective,” BMC Med. Inform. Decis.Mak., vol. 24, no. 1, p. 240, 2024, doi: 10.1186/s12911-024-02651-8.
15. M. Ahmad et al., “Healthcare device security assessment through computational methodology,” Comput. Syst. Sci. Eng., vol. 41, no. 2, 2022, doi: 10.32604/csse.2022.020097.
16. F. Kirmani, B. Lane, and J. Rose, “Identifying Proteotypic Peptides via Deep Learning,” in Proceedings of the 11th International Conference on Bioinformatics Research and Applications, 2025, pp. 42–47, doi: 10.1145/3700666.3700691.
17. J. Tyler, J. Pastor, M. N. Huhns, S. Kirmani, and H. Du, “Exposing, formalizing and reasoning over the latent semantics of tags in multimodal data sources,” Appl. Ontol., vol. 8, pp. 95–130, 2013, doi: 10.3233/AO-130124.
18. S. Kirmani and M. Shankar, “Generating keywords by associative context with input words.” Google Patents, 2022.
19. A. Mishra, S. Kirmani, and K. Madduri, “Fast Spectral Graph Layout on Multicore Platforms,” 2020, doi: 10.1145/3404397.3404471.
20. S. Kirmani and K. Madduri, “Spectral Graph Drawing: Building Blocks and Performance Analysis,” in 2018 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW), 2018, pp. 269–277, doi: 10.1109/IPDPSW.2018.00053.
21. H. Alyami et al., “Analyzing the data of software security life-span: Quantum computing era,” Intell. Autom. Soft Comput., vol. 31, no. 2, 2022, doi: 10.32604/iasc.2022.020780.
22. Fawad Kirmani, Ananthavishnu S Unni, Varsha P Kulkarni, Kyle Lackey, John R Rose, Detecting Polar Ring Galaxies via Deep Learning, RAS Techniques and Instruments, 2025;, rzaf043, https://doi.org/10.1093/rasti/rzaf043
23. H. Alyami et al., “The evaluation of software security through quantum computing techniques: A durability perspective,” Appl. Sci., vol. 11, no. 24, 2021, doi: 10.3390/app112411784.
24. O. Samuel, N. Javaid, T. A. Alghamdi, and N. Kumar, “Towards sustainable smart cities: A secure and scalable trading system for residential homes using blockchain and artificial intelligence,” Sustain. Cities Soc., vol. 76, p. 103371, 2022, doi: https://doi.org/10.1016/j.scs.2021.103371.

25. A. Alharbi et al., “Novel 59-layer dense inception network for robust deepfake identification,” Sci. Rep., vol. 15, no. 1, p. 24159, 2025, doi: 10.1038/s41598-025-03889-6.

A. Hakami et al., “Clinical characteristics and early outcomes of hospitalized COVID-19 patients with end-stage kidney disease in Saudi Arabia,” Int. J. Gen. Med., vol. 14, 2021, doi: 10.2147/IJGM.S327186.

26. M. Nadeem, M. Ahmad, M. Ahmad, P. C. Pathak, S. Gupta, and H. Pandey, “Evaluating the Factors of CGTMSE Scheme in Bank by Using Fuzzy AHP,” in 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), 2023, vol. 6, pp. 56–61, doi: 10.1109/IC3I59117.2023.10397669.

27. F. Alassery, A. Alzahrani, A. I. Khan, A. Khan, M. Nadeem, and M. T. J. Ansari, “Quantitative Evaluation of Mental-Health in Type-2 Diabetes Patients Through Computational Model,” Intell. Autom. Soft Comput., vol. 32, no. 3, 2022, doi: 10.32604/IASC.2022.023314.

28. Y. LeCun et al., “Deep learning,” Nature, 2015.

29. S. Hochreiter and J. Schmidhuber, “Long Short-Term Memory,” Neural Computation, 1997.

30. W. Wang et al., “HAST-IDS: Learning hierarchical spatial-temporal features,” IEEE Access, 2017.

31. Y. Yin et al., “Deep learning approach for intrusion detection using recurrent neural networks,” IEEE Access, 2017.

32. N. Moustafa and J. Slay, “UNSW-NB15 dataset,” Military Communications Conference, 2015.

33. A. Javaid et al., “A deep learning approach for network intrusion detection,” IEEE MILCOM, 2016.