Svedberg Open
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

CNNBi-LSTM-GCN-ATN: Combining multifolddeep learning models with attention methodology for an enhanced network intrusion detection system

A. Kalaivani[1*], R. Pugazendi[2]

[1*]Research scholar, PG & Research Department of Computer Science, Government Arts College (Autonomous) Salem, Affiliated to Periyar University, Salem-636011, Tamil Nadu, India, Email : kalai24.vinod@gmail.com, https://orcid.org/0000-0003-4658-3267

[2]Assistant Professor, PG & Research Department of Computer Science, Government Arts College (Autonomous) Salem, Affiliated to Periyar University, Salem-636011, Tamil Nadu, India, Email : Pugazendi1970@gmail.com, https://orcid.org/0000-0003-2815-4071

Abstract

Network systems and data have changed quickly as a result of recent developments in the communication technologies. New threats create security risksthat are extremely difficult to identify intrusions. An intruder will inevitably launch many network attacks. Ensuring robust security is a growing challenge in the era of increasingly complex cyber threats and high-volume network environments. Traditional system uses shallow ML, which has limited abilities to detect novel threats. A novel multi-model DL architecture is proposed by integrating CNN, Bi-LSTM,GCN models, and attention mechanism approach.In the proposed architecture, the packetand flow-level patterns are extracted from the network raw data by the CNN layers for spatial representations. The Bi-LSTM layers process the extracted spatial features to model temporal dependencies. A bidirectional time flow behavior is performed to enable accurate identification of attacks. Then, feature extraction is performed using spatial and temporal approaches. The converted data is mapped into a graph structure. The nodes in the graph denotes the communication sessions (entities) and the edges in the graph denotes the encoded flow interactions (similarities). Next, GCN layer is used to train the graph structured representations. An attention mechanism approach is merged to enhance the model's discriminative capability.The model is assessed for accuracy, capability and the ability to handle new attacks. The results of the proposed CNNBi-LSTM-GCN-ATNmodel outperforms the existing DL architectures in overall accuracy and identification of different attack categories.

Keywords: network security; anomaly detection; CNN; Bi-LSTM;graph neural network; attention

1. Introduction

The modern network set-ups are rising in terms of scalability and complexity. Recently, there is anincrease in digital services,like 5G network, cloud computing, IoT, and distributed corporate structures. These digital service developments have made network communications better, but these network connections are prone to a greater number of varied cyberattacks.There are many evolving cyberattacks that aim networked environments. It is vital to create a robust cybersecurity solution. IDS are vital elements for network security, ability to find and detect unauthorized activities (Gueriani et al. 2024, April).Traditional IDS like signature and rule-based methods, commonly neglect complex attack patterns and zero-day vulnerabilities. Encryptedcommand-and-control channels,polymorphic malware,stealthy reconnaissance approaches, and distributed denial-of-service (DDoS) are complex methods applied by attackers(Altunay et al.2023). An advanced surveillance approaches and adaptive training methods are required to handlehigh-dimensional network data.

DLapproach enhances the IDS performance, becauseof its capacity to extracthigh-level feature representations. DL approaches learn hierarchical representations automatically from raw network traffic which aids IDS to differentiate between malicious and normal behaviors precisely.To capture spatial correlations and temporal dependencies in network traffic,CNN, RNN and LSTM variants(Altunay et al.2023), are applied due to its strong capabilities. GNN, GCN(Saxena et al.2025)has the capacity to model relational structures between network entities. Hybrid or multimodal IDS architectures are integrated to aid the DL components to obtainhigh level of accuracy detection.

The consequent subsectionsdiscuss about the problem statement, research gap, contributions and organization of this paper.

1.1 Problem statement

There are numerous challenges in the existing DL based IDS approaches. It captures only partial features in network traffic either spatial features, temporal dependencies or relational interactions. The existing DL approaches captures only simple hybrid architectures; it fails to capture multi-dimensional cyber-attacks. There are IDS architectures that applies network flow as graphs to model the inter-host relationships. Many such architectures ignore the attention-based mechanismnotion which highlights the viral traffic patterns. It results in incorrect detection of zero-day attacks and the ability to adapt to varying threats. The current research gap is the absence of multi-model IDS framework that integrates spatial features, reliable sequential modeling, ability to inspect inter-entity relationships and an enhanced adaptive feature selection procedure.

1.2 Contributions

This study addresses these limitations by introducing a novel DL based IDS architecture that combines CNN, Bi-LSTM, and GCN layers, with an attention mechanism procedure. The contributions are stated as follows:

i) The multi-model design that extracts and fuses spatial, temporal, and graph based structural patterns for enhanced intrusion detection. To convert network flow into a relational graph representation, a graph construction approach using GCN is applied.
ii) To enhance the interpretability and detection accuracy, a global attention layer is incorporated to focus on the abnormal behavior.
iii) To handle the class imbalances in network attack data and reduce the false negatives, a LightGBM classifier is ensembled.
iv) CSE-CIC-ID2018 dataset is used for evaluation and an ablation study is performed to know the specificinfluence on performance.

The multi-model approach combines CNN, Bi-LSTM and GCNfor IDS architecture. This method works well for improving predictions for minority classes and managing unbalanced datasets. The three modules of multi-model approach are, opening with CNN for feature extraction to extract the spatial features. This stage is essential because it captures higher-level information through the layers of the network, improving the data representation. Followed by theBI-LSTM to detect temporal dynamic attacks. The overlapping feature issues are addressed in this phase. It ensures that all the temporal dependencies are taken, hence minimizing the feature redundancy. Then, graph data structured from network flows for GCN layers to learn node embeddings representing complex network interactions in graph learning.The combined outputs from Bi-LSTM and GCN through attention mechanism to enhance the detection accuracy.Finally, the LightGBM classifier is applied to categorize the attacks.This synergy results leads to a highly accurate, efficient, and more robust to network traffic complexity and evolving attack vectors.In conclusion, the model's design aims to handle class imbalance, lower noise, and improve feature quality to increase the classification accuracy.

This research article is organized as follows. Related reviews are elaborated in section 2. The description the proposed CNNBi-LSTM-GCN-ATN methodology such as the dataset pre-processing procedures, the architectures ofCNN, Bi-LSTM, GCN andattention mechanismare discussed in section 3. The experimental design, the evaluation metrics, experimental results and analysis of CNNBi-LSTM-GCN-ATNapproach are elaborated in section 4. Finally, the conclusion and future developments are discussedin section 5.

2. Related work

The interesting IDS research are reviewed in this part, with a focus on DL and ML. DL technology has been more popular in network IDS because of its remarkable capacity to handle large, complex datasets and identify the underlying characteristics of traffic data. As a result, this kind of application offers itself as a practical method for detecting security breaches. The intrusion classification problem has been addressed in recent years using a variety of DL based techniques. Several studies have applied ML and DL models to distinguish and classify attacks.

In their research, Dong et al. (2020)combines MCAand LSTM for IDS. The model chooses an optimal feature subset through a feature selection processcalled as information gain. The inputs of the TAM are given into the LSTM module. The model's outcomes are compared with existing CNN, RNN, SVM, KNN, and DF methods. The results show that the accuracyobtained is 82.15%, on NSL-KDD dataset and 77.74% accuracy on UNSW-NB15 dataset. Dutta et al. (2019) came up with a hybrid IDS model to resolve low detection rate and high false positive rate issues by combining classical auto encoder (CAE)and deep neural networks (DNN). In the first phase CAE is used for feature engineering and in the second phase DNN is used for classification. The results are analyzed based on thedetection rate, false-positive rate,ROCand F1-score. A comparative study is performed with the other algorithms used for network irregularity detection.

Injadat et al. (2020)came up with an optimized ML models for network IDS to minimize the computational complexity by combining RF and KNN algorithms.TRE is applied to optimize the hyperparameters. The detection performance and time complexity are analyzed based on the feature selection methods. The findings of the study are compared with other optimization methods like Bayesian. The results show that the essential training sample size is reducedto 74% and feature set size to 50%. Aljbali& Roy(2020) introduced an anomaly detection technique using Bi-LSTMalgorithm.Data preprocessing is performed and the processed data is given as input to the Bi-LSTM model for detecting anomalies.The Bi-LSTM model's outcomes compared to other ML and DL models.

Xiao et al. (2020)applied graphs with latent features for IDS.Graphs with many latent features are created by the communications between many hosts. The statistical features and the latent features are combined to train the ML classifiers. The latent features are acquired by the graph to a particular hostglobally.The test results indicate that it enabled an accurate detection of anomalies and effective learning of latent features and can identify unidentified attacks.Zhang et al. (2023) investigated on Botnet attacks that are targeting IoT devices. A novel approach using GNN is applied to extract graph features. The model learns from six ML models by embedded features. It is compared with other graph features to identify botnet nodes. To obtain an accurate and robust solution, the impact of features, data and algorithm is vital. Table 1 presents the key related studies on IDS using DL.

Table 1: Key studies of IDS

Author	Objective	Key contributions	Methodology & Datasets used
Basati et al. (2022)	Develop a lightweight, accurate IDS architecture suitable for resource-constrained IoT devices.	PDAE architecture is proposed that reduces parameters & memory while keeping high detection performance for IoT scenarios.	Parallel deep auto-encoders for feature representation and downstream classifier. Evaluated on IoT-focused benchmark datasets.
Caville et al. (2022)	Explore self-supervised GNNs to detect anomalies/attacks without heavy label reliance.	First practical self-supervised GNN approach for flow-level NIDS, leveraging edge features and topological structure; shows improved generalization to unseen traffic.	Graph construction from flows → GNN (self-supervised training) → anomaly scoring. Evaluated on benchmark NIDS datasets
Saurabh et al. (2022)	Design an LSTM-based model tuned for IoT traffic temporal patterns.	LSTM variants (stacked / bidirectional LSTM + autoencoder variants) and a compact DNN; reported better accuracy on IoT datasets and suitability for low-latency detection.	LSTM autoencoder + stacked/bidirectional LSTM classifiers. UNSW-NB15 and BoT-IoT

			datasets.
Altunay et al. (2023)	Improve detection of diverse attack types by combining spatial and temporal feature extractors.	CNN + LSTM hybrid attains enhanced accuracy and minimizes false alarms; detailed feature engineering and preprocessing steps for network flows.	Spatialfeature extractionand temporal modeling. Experiments on common IDS benchmarks datasets.
Debicha et al. (2023)	Detect adversarial/evasion attacks targeting DL-based IDS using transfer learning detectors.	Proposed a multi-detector transfer-learning framework that improves detection of adversarially perturbed traffic against state-of-the-art IDS models; shows robustness gains vs. single detectors.	Transfer learning detectors trained on subsets of features; evaluated adversarial attacks against standard IDS models (attack generation + detection experiments reported).
Sun et al. (2024, July)	Leverage graph learning to capture relations among hosts/flows for improved NIDS	Introduced an end-to-end GNN-based NIDS pipeline and showed advantages in modeling relational behavior; discusses graph construction strategies and scalability considerations.	Graph construction from flow/host interactions → GNN classifier. Experiments on benchmark datasets; ablation on graph constructions/feature sets
Ullah et al. (2024)	Address class imbalance and complex contextual patterns using transformers and transfer learning.	Proposed Transformer + transfer learning pipeline for imbalanced network traffic; demonstrated improved detection on minority attack classes and discussed balancing strategies.	Transformer encoder (pretrained fine-tuning / transfer learning) + imbalance mitigation (resampling / loss weighting). Evaluated on imbalanced NIDS datasets.
Tseng et al. (2024)	Apply Transformer architectures to multi-class IoT intrusion detection (temporal/contextual modelling).	Demonstrated that transformer-based models can capture long-range dependencies in IoT traffic and outperform several RNN/CNN baselines for multiclass detection on CIC-IoT data.	Transformer encoder (sequence modelling) for flow/time-series features. Evaluated on CIC-IoT-2023 and related IoT datasets, with multiclass metrics.
Li et al. (2024, July)	Survey recent DL-IDS developments and outline open problems (robustness, real-time deployment, explainability)	Comprehensive review of architectures (CNN/RNN/Transformer/GNN/autoencoders), adversarial threats, and dataset/reproducibility issues; proposes directions for robust, deployable IDS designs.	Literature survey and taxonomy; synthesizes methods and datasets; highlights benchmark gaps and evaluation best practices.
Liu et al. (2025, July)	Combine strengths of CNN, LSTM and Transformer for high-accuracy, low-latency IDS	Uses CNN-LSTM to extracts spatial features, models short-term temporal patterns, and captures long-range dependencies; reports strong detection and robustness results on modern benchmarks.	CNN front end- LSTM layer(s) - Transformer/block for context + classifier. Evaluated on contemporary NIDS datasets; compares latency and accuracy vs. baselines

3. Proposed CNN Bi-LSTM-GCN-ATN Methodology

This section discusses the proposedmethodology for identifying attacks using DL.Initially, the dataset pre-processing procedures are discussed, then CNN, Bi-LSTM, and GCN models are presented. Attention mechanism approach is discussed.Finally, the hybrid architecture to classify the network traffic are discussed.

3.1 Data preprocessing procedures

The data preprocessing procedures for the CSE-CIC-IDS2018 dataset involve several vital steps to ensure clean, normalized, and eloquent input for model training and evaluation.The dataset size is reduced by eliminating the unnecessary features are first removed. Lastly, normalization was carried out. The CSE-CIC-ID2018 dataset

contains eleven different types of attacks and more than 3 million records. The dataset contains 80 features, including statistical features like packet counts, byte counts, flow statistics, packet length, time interval, and flow-based features. The following lists the several preparation techniques used on the data set:

i) The dataset's zero or null characteristics are removed throughout the feature removal process. Samples of the same number from each type of attack were selected at random throughout the random selection process. The duplicates are eliminated according to the types of attacks during the duplicate elimination process.
ii) Since there are non-numerical features, a one-hot encoder is applied to transform into numerical features via the encoder.
iii) The ADASYN technique is used to generates synthetic samples and helps to address imbalance problems and improve the network's classification performance.
iv) To close the enormous gap between different dimensional feature data within the dataset, normalization is carried out.The MinMaxScaler (Bisong 2019) was applied for data mapping into the range(0,1) as:

$$X` = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \quad (1)$$

Where x_{max} denotes the maximum value and x_{min} denotes the minimum value.

v) A collection of features is chosen according to the criteria in the feature method. This method reduces the amount of time needed for training by enabling quick model building.
vi) The data is fragmented into learning and testing data.It is shuffled to ensure samples are randomly distributed, mitigating temporal bias.

3.2 CNN

Convolutional operations are part of CNN, that are capable of learning representations and the spatial hierarchy of incoming data(Wang et al. 2020). CNN processes data using multiple layers of arrays.Both supervised and semi-supervised learning can make use of the translation-invariant characteristics that CNN has learned. Input, convolutional, pooling, fully connected, and output are the layersofCNN. The convolutional layer (feature extraction)is the crucial component of a CNN (Zhang et al. 2021). CNNs have shown outstanding outcomes for certain challenges.Input neuron connections make up each subsequent layer of a neural network. The local receptive field is the term for this specific region. Unseen neurons are the focus of the local receptive field(Gu et al. 2018). The input and pooling layer, which comes before the convolutional layer, provides the input. The convolution layer's basic idea is to perform a convolution operation between the current layer's convolution core and the preceding layer. Lastly, the activation function generates the output with the matching bias.

3.3 Bi-LSTM

In the fields of DL and AI, LSTM is an artificial NN (Sherstinsky2020). Unlike traditional feedforward neural networks, LSTM has feed-back connections. RNNs perform less effectively as the gap size increases. LSTM can store data for a longer period of time by default(Tschannen et al. 2018). It is utilized for processing, forecasting, and classification. The structure ofBi-LSTM is shown in figure 1.

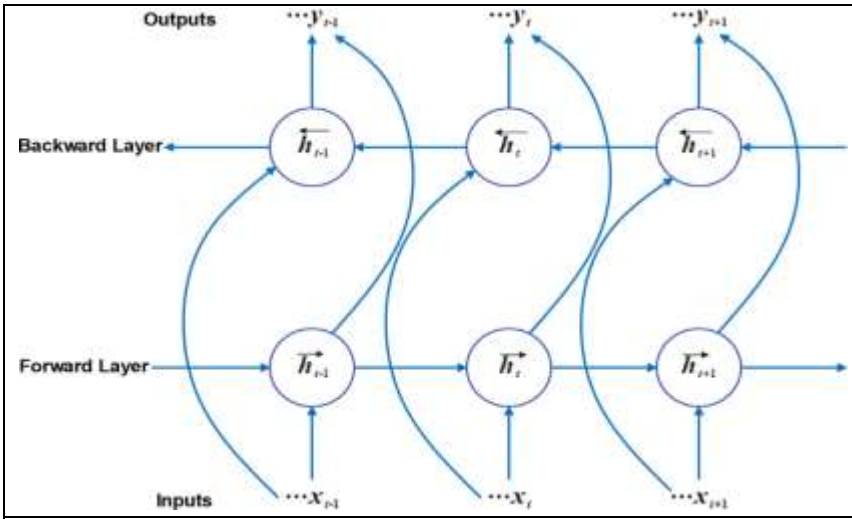

Fig. 1: Structure of Bi-LSTM

$$f_t = \Phi(\hat{w}_f.[h_{t-1}, x_t] + B_f) \quad (2)$$
$$i_t = \Phi(\hat{w}_i.[h_{t-1}, x_t] + B_i) \quad (3)$$
$$\tilde{C}_t = tanh(\hat{w}_C.[h_{t-1}, x_t] + B_C) \quad (4)$$
$$C_t = f_t * C_{t-1} = i * C_t \quad (5)$$
$$O_t = \Phi(\hat{w}_O.[h_{t-1}, x_t] + B_O) \quad (6)$$
$$h_t = O_t * \tanh(\Phi(C_t)) \quad (7)$$

Here, x_t denotes input, h_t denotes hidden layer output, Φrepresents sigmoid function, $C_t$denotes cell state, $\tilde{C}_t$ denotes candidate, $\hat{w}_O$, $\hat{w}_i$, $\hat{w}_C$, $\hat{w}_f$ are the weights for input, drop, output and memory cell.B_f,B_i, $B_c$are the bias for input, output, drop and memory cell.The cell records the processing state, output gate decides about the outcome, input gate decides about retaining input data, and drop gate decides about dataloss.

3.4 GCN

The GCN module is a graph structure of network traffic data for intrusion detection. It operates by modeling entities such as IP addresses, devices, or packets as nodes in a graph and their interactions or flows as edges.GCNs are used to perform convolutions over graph by combining and altering features from a node's neighbor. This aids to efficiently capture relational and structural dependencies unlike CNN. The feature representation of a node is updated in each layer by merging its own features with its neighbors.An adjacency matrix is weighted, node degree normalization is performed and finally, it is trained along with a nonlinear activation function like ReLU (Zhang et al. 2023).The contextual information is circulated across the graph, which enables the networkto train varied graph topologies.Usually, two to three GCN layers are stacked to develop each node's field across varied hops. The GCN module complements the CNN and Bi-LSTM modules. It captures complex patterns like anomalous communication links and coordinated attacks. The feature set is enriched by the GCN module which enhances the IDS's capacity to identify complex intrusion behaviors. Thus, there is a need for GCN module for converting raw traffic graphs into meaningful representations which, enhances the feature interactions within the network flow.

3.5 Attention Mechanism

To enhance the interpretability and predictive performance, attention mechanism approach is applied in DL.It is designed to focus on the model's input data.This approach acts like a filter, that assigns different weights to different input features. The model's vital information is prioritized while it conquers the noisy signals.The attention scores are used to measure the similarity between the vector and derived keys from input features. A SoftMax function is applied to normalize the scores that denotes the relative importance of input elements.The weighted sum of input values is computed, which results in a context vector. For classification, the context vector is merged with the other network modules (Niu et al. 2021).

This study merges CNN, Bi-LSTM, and GCN models and the attention mechanism approach is merged to enhance the effectiveness of the multi-model system. The spatial, temporal and relational features are selected to identify the intrusion behavior. The attention approach enhances the model's capacity to identify subtle and multi-dimensional attack patterns in a complex network.This selective feature weighting leads to improvements in detection accuracy, interpretability, and robustness against noise and irrelevant variations in the input.An attention mechanism is an effective part of advanced IDS since it empowers DL models to learn where to "look" within large and complex datasets.

3.6 The proposed CNNBi-LSTM-GCN-ATNmodelarchitecture

The proposed CNNBi-LSTM-GCN-ATN architecture for IDS consists of three modules,such as Bi-LSTM, GCN and ATN as illustrated in figure 2.Data pre-processing steps like feature removal, one hot encoding, data augmentation and normalization are performed. The proposed CNNBi-LSTM-GCN-ATN model contains a CNN_Moduleto extract spatial features from raw inputs, BiLSTM_Moduleworks on temporal dependencies.GCN_Module uses a graph convolution to learn relational features between entities/nodes.Attention_Module weighs more important fused features before classification.LightGBMclassifies the network traffic into normal and malicious. This studyuses CSE-CIC-ID2018datasetto classify the attacks. The pseudo code for the proposed multi-model which combines CNN, Bi-LSTM, GCN and ATN for intrusion detection are given below:

Input: Preprocessed network traffic data
Step 1: Spatial Feature Extraction via CNN
cnn_input = reshape_data_for_CNN(input_data)
cnn_features = CNN_Module(cnn_input) //Conv1D, MaxPooling, Flatten
Step 2: Temporal Feature Extraction via Bi-LSTM
lstm_input = reshape_for_LSTM(cnn_features)
lstm_features = BiLSTM_Module(lstm_input) //Bidirectional LSTM layers
Step 3: Graph-Based Feature Extraction via GCN
graph_data = create_graph_from_input(input_data) adjacency matrix + node features
gcn_features = GCN_Module(graph_data) // GCN layer(s)
Step 4: Feature Fusion
fused_features = concatenate([lstm_features, gcn_features])
Step 5: Attention Mechanism
attention_output = Attention_Module(fused_features)
Step 6: Classification
output = Dense_Layer(attention_output) // intermediate Dense layers
final_prediction = Softmax_or_LightGBM(output) // Multi-class or binary
Return final_prediction

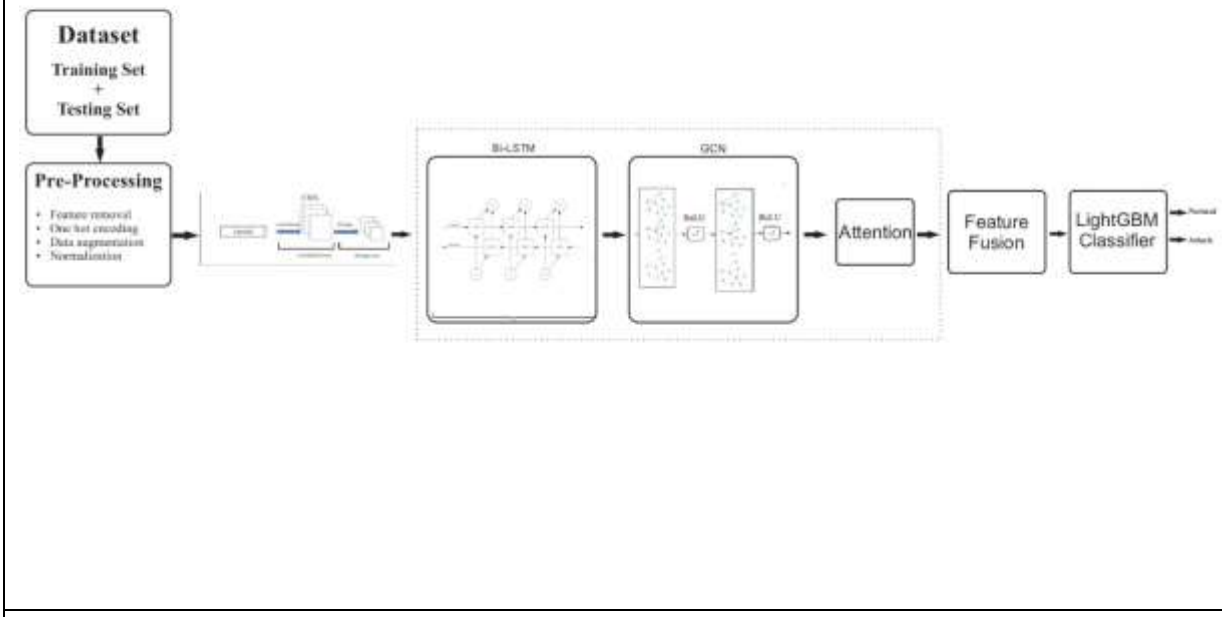

Fig. 2: Architecture of the proposed CNNBi-LSTM-GCN-ATN model

4. Experiment results

This section discusses the evaluation metrics, result analysis and comparative study. The experiments in this study were performed on 64-bit i7 processor, 16 GB RAM, NVIDIAGTX-1080Ti GPU and windows 10 OS. The simulationswere performed using Python 3.7 and sklearn libraries were used. The dataset containsreal features and the network movement has both malicious and benign traffics. They are categorized into malicious attack and normal using the proposed approach.

4.1 Evaluation metrics

The proposed CNNBi-LSTM-GCN-ATN model was evaluated using the regular performance valuations like accuracy (a), precision (p), recall (r) and f1-score (f1). Here, TP denotesthe attack is appropriatelycategorized as an attack.TN denotes the normal data is appropriatelycategorized as normal.FP denotes the normal data is inaccuratelycategorized as an attack.FN denotes the attack data is inaccuratelycategorized as normal.

$$a = \frac{TP + TN}{TP + FP + TN + FN} \tag{8}$$

$$p = \frac{TP}{TP + FP} \tag{9}$$

$$r = \frac{TP}{TP + FN} \tag{10}$$

$$f1 = \frac{2(TP + FP)(TP + FN)}{TP} \tag{11}$$

4.2 Result analysis

The performance of CNNBi-LSTM-GCN-ATN model is analyzed built on training and testing datasets. Table 1 shows the hyper-parameters and its value for tuning the parameters.In this research, ablation study is performed for understanding the proposed model's performance.

Table 1: Hyper-parameter Tuning

Hyper-parameter	Value
CNN layers	1-3
Filter count	128
Kernel size	11
Pooling size	5
Dropout rate	0.368
Bi-LSTM layers	1-3
GCN layers	2-3
Dense layer	3
Attention size	32
Light GBM Max depth	5-15
Learning rate	0.001
Batch size	64
Epoch count	50

Table 2 illustrates average results attained by the proposed CNN, Bi-LSTM-GCN, CNNBi-LSTM-GCN and CNNBi-LSTM-GCN-ATN modelson CSE-CIC-ID2018 dataset.The accuracy obtained byCNNBi-LSTM-GCNmodel is 98.83% and CNNBi-LSTM-GCN-ATNmodel is 98.99%. The hyper-parameters are tuned to maximize the classification accuracy. It is evident that CNNBi-LSTM-GCN-ATN model obtains more accuracy in detecting the attacks in the network. Hence, this multi-model approach, aids in enhancing the classification accuracy.

Table 2: Performance comparison of the proposed CNNBi-LSTM-GCN-ATN model on CSE-CIC-ID2018

Models	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
CNN	84.92	86.88	78.94	81.78
Bi-LSTM-GCN	88.76	91.27	89.14	90.47
CNNBi-LSTM-GCN	98.83	98.85	99.3	99.2
CNNBi-LSTM-GCN-ATN	98.99	98.96	99.49	99.7

Table 3 shows the proposed inferences with the existing approaches. The CNNBi-LSTM-GCN-ATN model outperforms the other dual models relating to the evaluation metrics. It is noted that the assessments are for references since there are variations in the datasets, dataset size, pre-processing, pre-processing and sampling by each researcher. Then the performance metrics also varies according to the training and testing time. However, the proposed CNNBi-LSTM-GCN-ATN model surpasses the recent former models in the literature. Hence, the outcomes ofCNNBi-LSTM-GCN-ATN model are capable for classifying attacks.

Table 3: Comparison between the proposed CNN Bi-LSTM-GCN-ATN model and existing approaches

Reference	Approaches	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Qazi et al.(2023)	CNN & RNN	98.90	98.64	99.15	99.03
Xu et al. (2023)	CNN-BiLSTM-Attention	88.27	91.54	89.13	90.18
Said et al., (2023)	CNN-BiLSTM	98.42	-	-	-
Proposed	CNNBi-LSTM-GCN-ATN	**98.99**	**98.96**	**99.49**	**99.7**

Figure 3 shows the detection rate of the proposed models. The Proposed CNNBi-LSTM-GCN-ATN model had the highest detection rate for the attack categories brute-force, web attack, DoS attack, DDoS attack, BotNet, Infiltration.The CNNBi-LSTM-GCN model had the highest detection rate of 98.96% for the benign category.

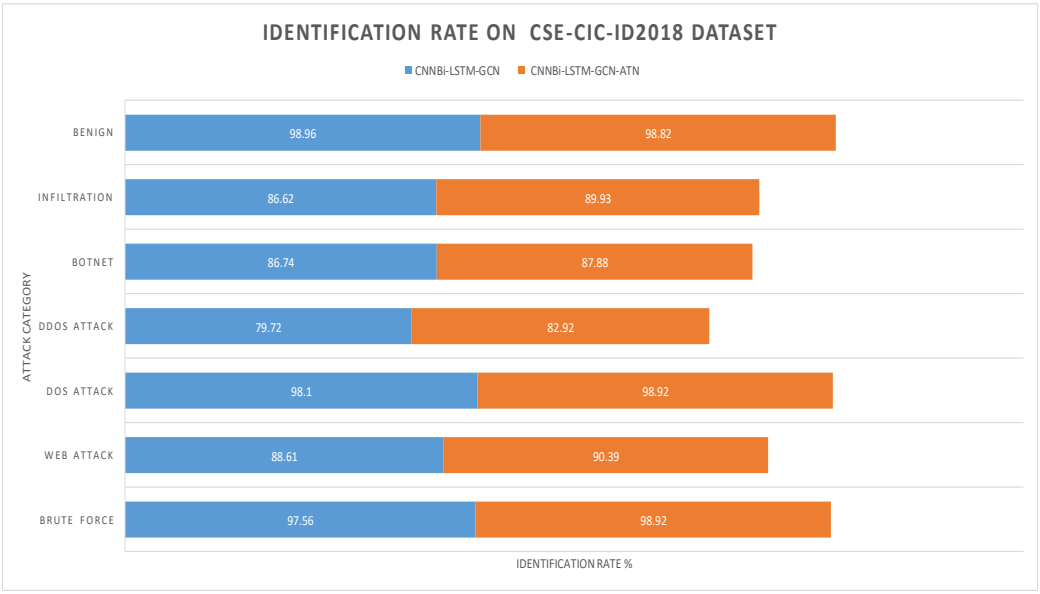

Fig. 3: Identification rate of different attacks categories on CSE-CIC-ID2018 dataset

5. Conclusion

This study introduced a novel multi-modal DL framework integrating CNN, Bi-LSTM and GCN models. An attention mechanism approach is incorporated in the integrated modelsfor robust network IDS. CNN extracts the spatial features, Bi-LSTM captures the temporal dependencies, and GCN learnsthe relational and structural embeddings from network traffic graphs. To enhance the interpretability and classification performance, the attention approach is applied to highlight therelevantfeatures.Experimental results shows that the proposed CNN-BiLSTM-GCN-ATN model outperformsthe single-model approaches. It increases the detection accuracy, decreases the false positive rate and diverse attacks.The challenges of modelling in different and high dimensional network data are addressed.Finally, the proposed model offers an interpretable and scalable solution for currentIDS in a cybersecurity network.In future work, real-time deployment, combining with other classifiers and applying an adaptive learning approach for zero-day attack detection can be explored.

References

1. Aljbali, S., & Roy, K. (2020, August). Anomaly detection using bidirectional LSTM. In Proceedings of SAI Intelligent Systems Conference (pp. 612-619). Cham: Springer International Publishing.
2. Altunay, H. C., & Albayrak, Z. (2023). A hybrid CNN+ LSTM-based intrusion detection system for industrial IoT networks. Engineering Science and Technology, an International Journal, 38, 101322.
3. Basati, A., & Faghih, M. M. (2022). PDAE: Efficient network intrusion detection in IoT using parallel deep auto-encoders. Information Sciences, 598, 57-74.
4. Bisong, E. (2019). Building machine learning and deep learning models on Google cloud platform (pp. 59-64). Berkeley, CA: Apress.
5. Caville, E., Lo, W. W., Layeghy, S., & Portmann, M. (2022). Anomal-E: A self-supervised network intrusion detection system based on graph neural networks. Knowledge-based systems, 258, 110030.
6. Debicha, I., Bauwens, R., Debatty, T., Dricot, J. M., Kenaza, T., & Mees, W. (2023). TAD: Transfer learning-based multi-adversarial detection of evasion attacks against network intrusion detection systems. Future Generation Computer Systems, 138, 185-197.
7. Dong, R. H., Li, X. Y., Zhang, Q. Y., & Yuan, H. (2020). Network intrusion detection model based on multivariate correlation analysis–long short-time memory network. IET Information Security, 14(2), 166-174.
8. Dutta, V., Choraś, M., Kozik, R., & Pawlicki, M. (2019, May). Hybrid model for improving the classification effectiveness of network intrusion detection. In Computational Intelligence in Security for Information Systems Conference (pp. 405-414). Cham: Springer International Publishing.
9. Gu, J., Wang, Z., Kuen, J., Ma, L., Shahroudy, A., Shuai, B., ... & Chen, T. (2018). Recent advances in convolutional neural networks. Pattern recognition, 77, 354-377.

10. Gueriani, A., Kheddar, H., & Mazari, A. C. (2024, April). Enhancing iot security with cnn and lstm-based intrusion detection systems. In 2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS) (pp. 1-7). IEEE.
11. Injadat, M., Moubayed, A., Nassif, A. B., & Shami, A. (2020). Multi-stage optimized machine learning framework for network intrusion detection. IEEE Transactions on Network and Service Management, 18(2), 1803-1816.
12. Li, Z., Fang, W., Zhu, C., Song, G., & Zhang, W. (2024, July). Toward Deep Learning based Intrusion Detection System: A Survey. In Proceedings of the 2024 6th International Conference on Big Data Engineering (pp. 25-32).
13. Liu, D., Zheng, X., Wang, P., Chuan, J., Lv, Y., Zhou, B., ... & Jiao, W. (2025, July). Deep Learning-Based Intrusion Detection: A CNN-LSTM-Transformer Approach for Enhanced Network Security. In Proceedings of the 10th International Conference on Cyber Security and Information Engineering (pp. 318-325).
14. Niu, Z., Zhong, G., & Yu, H. (2021). A review on the attention mechanism of deep learning. Neurocomputing, 452, 48-62.
15. Qazi, E. U. H., Faheem, M. H., & Zia, T. (2023). HDLNIDS: hybrid deep-learning-based network intrusion detection system. Applied Sciences, 13(8), 4921.
16. Said, R. B., Sabir, Z., &Askerzade, I. (2023). CNN-BiLSTM: A Hybrid Deep Learning Approach for Network Intrusion Detection System in Software Defined Networking with Hybrid Feature Selection. IEEE Access.
17. Saurabh, K., Sood, S., Kumar, P. A., Singh, U., Vyas, R., Vyas, O. P., &Khondoker, R. (2022, June). Lbdmids: LSTM based deep learning model for intrusion detection systems for IOT networks. In 2022 IEEE World AI IoT Congress (AIIoT) (pp. 753-759). IEEE.
18. Saxena, S., Grover, J., & Singhal, S. (2025). Exploring Graph Neural Networks for Robust Network Intrusion Detection. Procedia Computer Science, 258, 3630-3639.
19. Sherstinsky, A. (2020). Fundamentals of recurrent neural network (RNN) and long short-term memory (LSTM) network. Physica D: Nonlinear Phenomena, 404, 132306.
20. Sun, Z., Teixeira, A. M., & Toor, S. (2024, July). GNN-IDS: Graph neural network based intrusion detection system. In Proceedings of the 19th international conference on availability, reliability and security (pp. 1-12).
21. Tschannen, M., Bachem, O., & Lucic, M. (2018). Recent advances in autoencoder-based representation learning. arXiv preprint arXiv:1812.05069.
22. Tseng, S. M., Wang, Y. Q., & Wang, Y. C. (2024). Multi-class intrusion detection based on transformer for IoT networks using CIC-IoT-2023 dataset. Future Internet, 16(8), 284.
23. Ullah, F., Ullah, S., Srivastava, G., & Lin, J. C. W. (2024). IDS-INT: Intrusion detection system using transformer-based transfer learning for imbalanced network traffic. Digital Communications and Networks, 10(1), 190-204.
24. Wang, X., Yin, S., Li, H., Wang, J., & Teng, L. (2020). A network intrusion detection method based on deep multi-scale convolutional neural network. International Journal of Wireless Information Networks, 27(4), 503-517.
25. Xiao, Q., Liu, J., Wang, Q., Jiang, Z., Wang, X., & Yao, Y. (2020, June). Towards network anomaly detection using graph embedding. In International Conference on Computational Science (pp. 156-169). Cham: Springer International Publishing.
26. Xu, H., Sun, L., Fan, G., Li, W., & Kuang, G. (2023). A hierarchical intrusion detection model combining multiple deep learning models with attention mechanism. IEEE Access, 11, 66212-66226.
27. Zhang, B., Li, J., Ward, L., Zhang, Y., Chen, C., & Zhang, J. (2023). Deep graph embedding for IoT botnet traffic detection. Security and Communication Networks, 2023(1), 9796912.
28. Zhang, L., Huang, Z., Liu, W., Guo, Z., & Zhang, Z. (2021). Weather radar echo prediction method based on convolution neural network and long short-term memory networks for sustainable e-agriculture. Journal of Cleaner Production, 298, 126776.
29. R.Eswaramoorthi. (2025). AI-Driven Self-Healing IoT Networks for Fault-Tolerant Smart Renewable Energy Infrastructure. National Journal of Renewable Energy Systems and Innovation , 1-9. https://doi.org/10.17051/NJRESI/01.04.01
30. M. Kavitha. (2025). Interference-Adaptive Cooperative Learning Control for Electromagnetically Coupled Actuation Systems. Journal of Wireless Intelligence and Spectrum Engineering, 9–15.
31. A.Velliangiri, & Chuong Vana. (2025). Secure Runtime Reconfiguration Framework for FPGA-Based Embedded Systems in Mission-Critical Applications. SCCTS Journal of Embedded Systems Design and Applications , 3(2), 36-47. https://doi.org/10.31838/ESA/03.02.05