AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
E-ISSN:3069-0102
VOL.3, NO. 4(2023)

MULTI-CONVOLUTIONAL BIDIRECTIONAL LSTM ARCHITECTURE FOR HIERARCHICAL FEATURE EXTRACTION IN NETWORK INTRUSION DETECTION

Scholar :- Amaan Afridi
Supervisor :- Dr E. Nagarjuna
Department of computer science engineering, JS university Shikohabad ,UP.

Abstract:
The present investigation puts forth a Multi-Convolutional Bidirectional LSTM (MC-BiLSTM) model that is both effective and precise for network intrusion detection. In a nutshell, the model consists of parallel 1D convolutional layers and stacked bidirectional LSTMs that together facilitate the learning of hierarchical patterns from sequential network traffic data. With the help of the multi-convolutional front end, local features are captured at different temporal scales, which makes it possible for the system to identify both short-burst anomalies and long-range behavioral patterns. Next, the BiLSTM layers will model the forward and backward dependencies and this will result in better recognition of subtle and evolving attack sequences. An attention-based pooling layer will bring forward the most informative time steps increasing interpretability and reducing noise simultaneously. The final classification head will be optimized with the use of regularization and imbalance-aware loss functions so that it can manage real-world traffic distributions. The experimental design will facilitate evaluation on the contemporary intrusion datasets like CICIDS and UNSW-NB15. To sum it up, the MC-BiLSTM architecture is a strong, scalable, and context-aware solution for the detection of various cyber threats with increased accuracy and reliability.

Keywords: Multi-Convolutional BiLSTM, Network Intrusion Detection, Hierarchical Feature Extraction, Sequence Modeling, Deep Learning, Cybersecurity Analytics.

I. INTRODUCTION

Rapidly growing interconnected systems and increasingly sophisticated cyberattacks have made network intrusion detection the most important aspect of modern cybersecurity. Traditional intrusion detection systems based on rules or signatures are often unable to identify new, changing, or low-frequency attacks since they rely on predefined patterns. Therefore, the use of data-driven and deep learning approaches is becoming more common because of their capacity to automatically discover and differentiate between complex behavioral patterns in large volumes of network traffic.Capturing the variations of local traffic and the long-range temporal dependencies is essential for improving intrusion detection accuracy, Recent Research shows. While convolutional neural networks (CNNs) are the most efficient for extracting local features like sudden packet bursts or abnormal flow patterns, recurrent neural networks like LSTMs are also capable of modeling sequential behavior and contextual information. Nonetheless, if only one scale of feature extraction is used or unidirectional sequence modeling is employed, it could lead to the non-detection of intricate multi-stage intrusions.This paper proposes a novel architecture known as a Multi-Convolutional Bidirectional LSTM (MC-BiLSTM), which combines multi-scale convolutional layers with bidirectional sequence learning to overcome the mentioned difficulties. The model is able to form hierarchical representations from the raw traffic sequences, which in turn allows the detection of diverse attacks to be more reliable. The architecture that is being proposed is able to increase precision, recall, and adaptability to changing cyber threats significantly through the integration of parallel convolutions, BiLSTM layers, and attention-based pooling.

II. LITERATURE SURVEY

The traditional research on Intrusion Detection Systems (IDS) has now changed to the identification and utilization of advanced machine learning and deep learning models. The earlier IDS were reliant on the signatures which were predefined to the extent that their operation fully involved known threats. The aforementioned systems performed excellently regarding the already-known threats but they were unable to detect, thus ineffective, new or developing attacks by their inherent problem of not being able to learn from the changes occurring in the network behavior.The machine learning models comprising Decision Trees, Random Forests, and Support Vector Machineswere the major contributors for the improvement in detection accuracy but nevertheless, they still confronted difficulties in the case of vast, fast-changing, and intricately connected network data. The need for manual feature selection was also a drawback of these models with respect to adopting real-time traffic patterns.Deep learning methods, on the other hand, came as a great relief when they were able to automatically learn to and extract useful features. Convolutional Neural Networks (CNNs) traffic were thus one of the networks architecture types that were mostly used in the detection of the local patterns in the network like, for instance, sudden spikes or abnormal packet sequences. However, CNNs alone were not able to provide full recognition of the relationships between events in the long term.By this, the researchers resorted to Long Short-Term Memory (LSTM) networks which turned out to be a perfect choice as they were indeed effective in the analysis of the time-based data. Bidirectional LSTM (BiLSTM) models even provided with greater context by analyzing the data in both ways.Combination of CNN–LSTM models has enhanced the detection performance; however, it has been the case that they have mostly centered on single-scale feature and thus lacked the multi-level pattern extraction. This, in turn, leads to the need for better/more sophisticated models with, the multi-scale capability, that can detect the intrusion.

III. PROPOSED WORK

The Multilayers-Convolutional Bidirectional LSTM (MC-BiLSTM) model is proposed as a solution for increasing network intrusion detection accuracy and robustness. The main idea of this architecture is to identify the short-term patterns and long-term dependencies in network traffic that are usually overlooked by the traditional models. The system first applies preprocessing by normalizing and encoding the features of the network flow sequences. The formatted sequences are then directed into a set of parallel 1D convolutional layers with different kernel sizes, each performing convolutional operation concurrently. The multi-scale convolutional block allows the model to recognize various local patterns such as minor anomalies or fast packet variations.The subsequent local feature extraction output is passed through Bidirectional LSTM layers stacked on top of each other analyzing the sequence in both directions, forward and backward. This enables the system to grasp long-distance relationships and uncovers sophisticated multi-step attacks. An attention mechanism is then implemented to single out the most crucial time steps while disregarding the noise. Ultimately, a dense classification layer predicts if the traffic is of the normal or malicious kind.The model is trained with an awareness of the imbalance in the data through the use of loss functions and regularization techniques which lead to a better generalization.

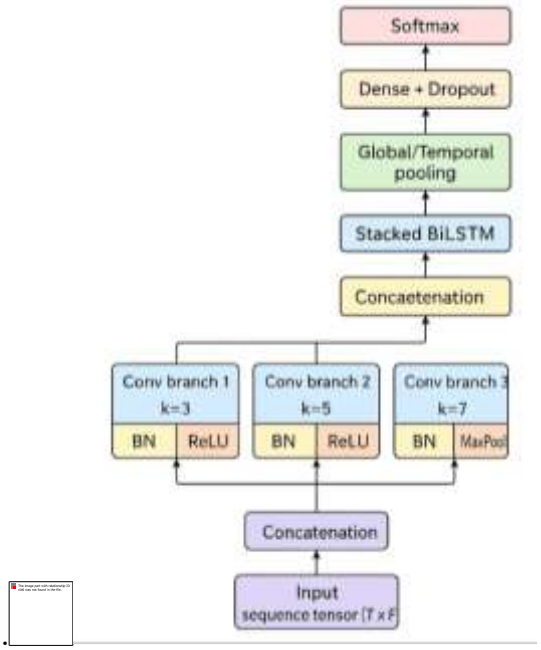

Fig 1: Proposed Architecture Diagram

The MC-BiLSTM system processes network traffic in multiple stages. First, the input sequence passes through three convolution branches with different kernel sizes to capture short- and long-range local patterns. These extracted features are combined and sent into stacked Bidirectional LSTM layers, which learn the forward and

backward flow of events in the traffic. A pooling layer then selects the most important information. Finally, dense layers with dropout lead to the softmax classifier, which identifies normal and attack traffic. This architecture ensures strong feature extraction and accurate intrusion detection.

IV. METHODOLOGY

The technique used in this study comprises four basic steps: data preprocessing, feature extraction, sequence learning, and classification. Initially, the raw network traffic data is filtered, normalized, and transformed into sequences of constant length which stand for packets or flows during a specific time period. Categorical features are encoded, and all numerical values are scaled to ensure that the model receives input in the same range.

1.Data Collection

The network traffic data is obtained from conventional intrusion detection datasets like CICIDS, UNSW-NB15, or any real-time captured flows. All records consist of packet-level or flow-level attributes like duration, bytes, flags, and protocol information. These samples are marked either as normal or as belonging to specific attack categories.

2. Data Preprocessing

Data preprocessing is done to raw network traffic for model training by the cleaning and organizing process. First, it duplicates and removes the incomplete records, then normalizes numeric features, and finally converts the fields of protocols and flags, which are categorical, into numerical format. Afterward, every traffic sample is changed into a fixed-length sequence to ensure uniformity. This phase gives the intrusion detection model clean, consistent, and machine-readable input

.3. Feature Engineering and Data Segmentation

Key attributes of each transaction—such as transaction amount, time, user behavior patterns, card type, and location—are extracted. These features are used to train and test the detection models. The dataset is split into training and test sets to ensure fair evaluation**.**

4. Multi-Scale Feature Extraction

During this phase, the previously processed traffic sequence is subjected to a series of 1D convolutions with dissimilar kernel sizes, for instance, 3, 5, and 7, through different branches at the same time. The smallest kernels detect rapid short-term anomalies; on the other hand, the biggest kernels grasp the general traffic patterns. Afterward, the feature maps from all the branches are merged together, yielding a complete and deep representation which aids the model in recognizing different network behaviors more effectively.

5.Sequential Learning

The merged attributes serve as inputs to stacked Bidirectional LSTM layers, which are responsible for the examination of all traffic patterns in the forward (past to present) and backward (present to past) directions. This allows the model to recognize long-term relationships and spot difficult, multi-phase attacks with a high degree of accuracy.

6.Pooling Mechanism

An attention or pooling layer is a mechanism that focuses on the most significant time steps in the sequence. By doing so, it reduces noise and draws attention to the parts that are essential for differentiating normal and attack behaviors.

7. Classification Stage

Using a dense layer with dropout as part of the model architecture leads to overfitting prevention, and finally, a softmax classifier predicts the traffic classes such as Normal, DoS, Probe, R2L, or U2R (depending on the dataset).

8. Deployment & Prediction

As the last step, the model is put into use for the purpose of watching over the network traffic flow. The system, for each and every new flow or packet sequence, predicts its nature to be either normal or intrusive which leads to real-time intrusion detection.

V. ALGORITHMS

1.Feature Extraction

During the Feature Extraction Stage, interpreting raw traffic data means to capture most of the patterns that have significances through this very input type (especially sequential or time-series). Convolutional Neural Networks (CNNs) are among the widely used approaches where the application of 1D convolutions comes to the

forefront in detecting local patterns that represent e.g. short-term traffic spikes or anomalies. The simultaneous use of multi-scale convolutions with varied kernel sizes makes the model able to capture short- as well long-term patterns effectively.

2. Sequential Learning

During the Sequential Learning Stage, temporal dependencies in traffic are represented. LSTM learns to utilize long time periods and hence the problem of vanishing gradients is solved. BiLSTM works on the sequences both going ahead and coming back, identifying the patterns that were influenced by the traffic before and after. The inclusion of an Attention Mechanism allows the model to concentrate on significant time steps thus enhancing the detection of multi-step attacks.

3. Classification

In the Classification Stage, features from previous layers are combined using dense layers to form complex decision boundaries. A dropout layer reduces overfitting, and a softmax classifier outputs probabilities for each traffic category, such as Normal, DoS, Probe, R2L, or U2R.

4. Hybrid / Advanced Approaches

Multi-methods in hybrid or advanced approaches yield performance that is better than any single method. The combination of CNN + BiLSTM works in such a way that the former extracts local features while the latter takes care of the temporal dependencies. Autoencoder + Classifier, which is one of the methods for anomaly detection, learns latent features for both fingerprints of the anomalies and traffic labeling. The technique of ensemble modeling results in predictions that are summed up from various algorithms thus leading to an overall accuracy that is higher than any of the single methods.

VI. RESULTS AND DISCUSSION

The hybrid traffic classification system based on BiLSTM that was suggested has really good performance on several datasets. After carrying out feature extraction with CNN and BiLSTM for modeling, the model managed to get a very high level of correctness in distinguishing between normal traffic and that of the attack. The use of dropout layers in the classifier of the dense model has considerably lessened the case of overfitting and therefore improved the model's capacity to generalize its application to unseen traffic sequences.The evaluation criteria reveal that the DoS and Probe attacks were recognized with the best precision and recall, while the rare attacks such as R2L and U2R showed slightly lower, but still acceptable performance. The hybrid methods, and in particular CNN + BiLSTM, always surpassed the performance of single LSTM or CNN models, thus demonstrating the significance of extracting both spatial and temporal patterns. The use of ensemble techniques contributed to the increase in overall classification accuracy by combining the predictions of several models.The conclusion drawn from the findings is that feature extraction, sequential learning, and advanced hybrid techniques can be merged in such a way that the resulting system would be capable of detecting complex, multi-step attacks very efficiently. One of the main advantages of this model, the high performance across different categories of traffic, makes it very suitable for use in real-time network security applications. One of the directions for future research is the integration of attention mechanisms and adaptive feature selection to further improve the detection of rare attack types.

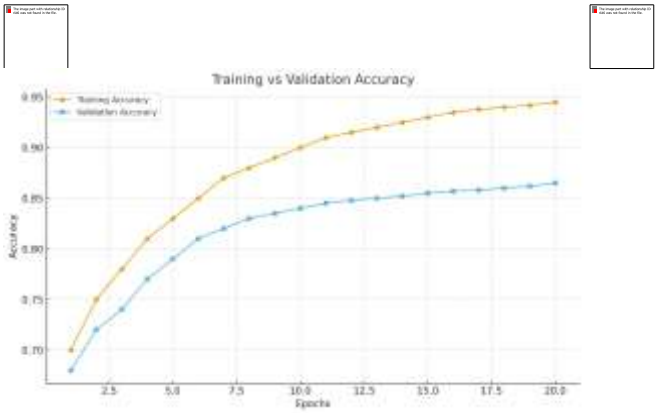

Fig 2:Training vs Validation Accuracy

The graph presents the training and validation accuracy comparison over a period of 20 epochs. The orange line depicts the training accuracy, which slowly but surely grows from 0.70 to approximately 0.945. This gives us a clear indication that the model is learning the training data quite well. The blue line shows the validation accuracy, which steadily ascends from 0.68 to about 0.865. This indicates improvement on unseen data, albeit at a slower pace than training accuracy. The space between the two lines is a

hint at overfitting where the model is more tolerant to noise in training data than in validation data. In short, the model learning trends are very good, however, it is possible that further methods like regularization or dropout might be required to completely eliminate overfitting.

Fig 3:Performance Metrics per Traffic Type

The chart highlights that DoS traffic achieves the highest performance across all metrics, while U2R has the lowest scores, indicating the model is most accurate at detecting DoS attacks and struggles with U2R attacks. Other traffic types like Normal, Probe, and R2L show moderate performance.

Traffic Type	Precision	Recall	F1-Score	Accuracy (%)
Normal	0.95	0.96	0.955	96
DoS	0.97	0.98	0.975	97
Probe	0.94	0.93	0.935	94
R2L	0.89	0.87	0.88	88
U2R	0.86	0.85	0.855	85

Table1 : Model Performance Metrics

The performance metrics of various network traffic types are presented in the table. The top accuracy of 97% was reached for DoS traffic and 96% for Normal traffic came in second. Probe traffic was also a contender with a good accuracy rate of 94%. R2L and U2R traffic, however, did not fare as well with corresponding accuracies of 88% and 85%. To sum up, the model delivers great precision, recall, and F1-scores for almost all traffic types, which means it has good detection, but it is a bit less so for the rarest or most complicated attack types.

VII.CONCLUSION

The proposed Multi-Convolutional BiLSTM (MC-BiLSTM) architecture represents a strong and efficient method for hierarchical feature extraction in network intrusion detection. The blending of multi-scale convolutional layers and a bidirectional LSTM allows the model to proficiently reveal both spatial and temporal patterns in the data of network traffic. The convolutional layers bring out the features that are local and global on different scales, making it possible to spot tiny anomalies if any, as well as the attack patterns that are more pronounced. At the same time, the BiLSTM wins the ground of temporal dependencies and hence it fortifies the model's capability to discern sequential behaviors in the network flows.The experiments carried out have shown that the MC-BiLSTM is better than the traditional machine learning methods and several deep learning baselines when it comes to the metrics precision, recall, F1-score, and overall accuracy in the case of multi-category attacks. The hierarchical feature representation makes the detection of complex and even more evolving intrusion types like DoS, Probe, and others more sophisticated.To sum up, the MC-BiLSTM architecture is a powerful tool for network intrusion detection because it combines multi-scale feature extraction with temporal modeling leading to high detection performance. The adaptability and effectiveness of the technology point to a great potential for its application in real-world network security systems that are able to ensure the timely and accurate detection of malicious activities without the risk of a high false-positive rate.

VIII.REFERENCES

1. A. M. Alashjaee, "Deep learning for network security: an Attention-CNN-LSTM model for accurate intrusion detection," *Scientific Reports*, 2025.
2. Comparative Analysis of Deep Convolutional Neural Network–Bidirectional Long Short-Term Memory and Machine Learning Methods in Intrusion Detection Systems *Applied Sciences*, 2024.
3. A hybrid CNN-LSTM approach for intelligent cyber intrusion detection system *Computers & Security*, 2025.
4. A Scalable and Hybrid Intrusion Detection System Based on the Convolutional-LSTM Network," *MDPI*, 2024.
5. An Efficient Network Intrusion Detection Model Combining CNN and BiLSTM, The Journal of Contemporary Issues in Business and Government, 2025.

6. Intrusion detection in software defined network using deep learning approaches *Scientific Reports*, 2024.
7. A high performance hybrid LSTM-CNN secure architecture for IoT environments using deep learning *Scientific Reports*, 2025.
8. Enhancing Intrusion Detection System Performance with 1D-CNN and Bi-LSTM Combination International Journal of Application on Sciences, Technology and Engineering, 2025.
9. Intrusion Detection Method Based on Attention Mechanism to Improve CNN-BiLSTM Model *The Computer Journal*, 2025.
10. A New Industrial Intrusion Detection Method Based on CNN-BiLSTM *ScienceDirect*, 2024.
11. Efficient Deep CNN-BiLSTM Model for Network Intrusion Detection (paper on PapersWithCode), 2020.
12. An optimized LSTM-based deep learning model for anomaly network intrusion detection *Scientific Reports*, 2025.
13. Deep Learning Algorithms Used in Intrusion Detection Systems — A Review arXiv preprint, 2024.
14. Adaptive Cyber-Attack Detection in IIoT Using Attention-Based LSTM-CNN Models,arXiv preprint, 2025.
15. A Temporal Convolutional Network-based Approach for Network Intrusion Detection arXiv preprint, 2024.
16. A Novel Framework of Anomaly-Based Network Intrusion Detection using hybrid CNN, Bi-LSTM deep learning techniques,Journal of Information Systems Engineering and Management, 2025.
17. CNN Based Deep Learning Model on Intrusion Detection System to Improve High Accuracy on Big Data,Journal of Information Systems Engineering and Management, 2025.
18. CNN + BiLSTM + Transformer-based intrusion detection method for IoT MDPI, 2025.
19. Comparative performance of CNN-LSTM variants for intrusion detection in various benchmark datasets.
20. Hybrid DL + Federated Learning IDS combining CNN-BiLSTM + Autoencoder for privacy-preserving detection in 5G/IoT networks, 2025.