Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

A Hybrid CNN–LSTM Framework for Network Intrusion Detection with SMOTE Balancing

Methaq Shaker Mahmood

Email: methaq76shaker.almohamed@gmail.com

Islamic Azad University, Software Engineering Department, Iran.

ARTICLE INFO

Article history:
Received: 11/09/2025
Rrevised form: 18/10/2025
Accepted : 21/10/2025
Available online: 30/12/2025

Keywords: deep learning, intrusion detection, network security, CNN, LSTM

ABSTRACT

In order to improve intrusion detection in network traffic analysis, this research presents a novel hybrid deep learning approach for feature extraction and classification· The complexity, volume, and sequential nature of contemporary network data frequently pose challenges for traditional machine learning techniques, which has a negative impact on anomaly detection's speed and effectiveness· In order to tackle this issue, our approach utilizes a hybrid model that initially automatically extracts significant temporal patterns and spatial features from unprocessed network traffic data using a Convolutional Neural Network (CNN)· Following that, a Long Short-Term Memory (LSTM) network receives these learnt properties and uses its capacity to process sequences to accurately classify traffic and identify interference· Our model outperforms traditional machine learning classifiers like Support Vector Machines and Random Forests by a considerable margin, achieving an accuracy of 98·7% and an F1-score of 97·4% on the publicly accessible CICIDS2023 dataset· The findings show that our hybrid CNN-LSTM model offers a promising, data-driven solution to a significant network security concern by having the ability to greatly improve the speed and efficacy of current intrusion detection systems.

MSC..

https://doi.org/ 10.29304/jqcsm.2025.17.42552

I. INTRODUCTION

Network security is a significant problem in the current digital environment due to the exponential expansion of network traffic and the growing sophistication of cyberattacks· These changing threats are making it difficult for traditional network security systems, which frequently rely on manual feature engineering and signature-based detection, to keep up· Since these techniques necessitate prior knowledge of the attack signature, they frequently fail to detect innovative or zero-day attacks [1, 2]· The requirement for automatic, effective, and highly accurate intrusion detection systems (IDS) that can recognize intricate and dynamic threats without requiring significant human interaction has resulted in a crucial research gap·

Numerous machine learning techniques have been investigated in earlier intrusion detection research, however many of them have serious drawbacks· Traditional classifiers, such as Random Forests and Support Vector Machines (SVMs), for example, frequently necessitate a time-consuming and tedious human feature extraction procedure, which may overlook minute, complex patterns in network data [3]·

∗Corresponding author: Methaq Shaker Mahmood

Email addresses: methaq76shaker.almohamed@gmail.com

Communicated by 'sub etitor'

Additionally, although several deep learning models have been used, many of them are unable to examine network traffic's temporal and geographical features at the same time [4]· The temporal dependencies of a continuous stream of network events may be difficult for Pure Convolutional Neural Networks (CNNs) to capture, despite their superiority at recognizing spatial characteristics (such as patterns in data packets)· On the other hand, while models like as Recurrent Neural Networks (RNNs) are effective at processing time-series data, they may have difficulties with long-term dependencies and the vanishing gradient problem, which can restrict their recall of events that occurred a long time ago [4]·

In order to overcome the shortcomings of earlier techniques, this study suggests a revolutionary way to network intrusion detection· We provide a hybrid deep learning model that combines the advantages of long short-term memory (LSTM) networks and convolutional neural networks (CNNs)· By spotting complex and high-level patterns in the raw network traffic data, the CNN component will automatically and independently carry out feature extraction, doing away with the requirement for human feature engineering· In order to forecast and categorize security concerns based on the order of network events over time, the LSTM network will next evaluate these extracted features to examine the temporal correlations and dependencies within the data stream· This special combination greatly improves the accuracy and effectiveness of intrusion detection by enabling our system to concurrently learn from the long-term temporal trends of network traffic as well as the spatial properties of the data packets· Our study attempts to confirm that this hybrid technique can provide a more reliable and accurate real-time network security solution than single-component deep learning models and conventional methods [5,6].

2. Literature Review

Early and foundational work in network intrusion detection primarily relied on traditional machine learning algorithms· Studies have used methods such as Support Vector Machines (SVMs), Decision Trees, and Random Forests to classify network traffic as normal or malicious [5, 6]· While these models are effective for well-defined, static datasets, they have significant limitations· A major drawback is their reliance on manual feature engineering, a labor-intensive and time-consuming process that requires domain expertise· This dependency makes them less adaptable to the continuously evolving nature of cyberattacks and may lead to failures in detecting new, unseen threats [7]·

The advent of deep learning has offered a promising solution to the challenges faced by traditional methods· Convolutional Neural Networks (CNNs) have been widely adopted for their ability to automatically learn and extract hierarchical features from raw data, bypassing the need for manual feature engineering· In the context of network security, CNNs have been used to identify spatial patterns and anomalies within network packet data [8, 9]· For example, a study by Vinayakumar et al· (2019) demonstrated the effectiveness of CNNs in extracting features from network traffic to build a robust intrusion detection system [9]· However, while CNNs excel at feature extraction, they often fall short in capturing temporal relationships within a continuous stream of network events·

To address the temporal aspect of network data, researchers have turned to Recurrent Neural Networks (RNNs)· RNNs and their variants, particularly Long Short-Term Memory (LSTM) networks, are designed to process sequential data and can maintain memory of past events [10]· Studies have applied LSTMs to network traffic to model the temporal flow of data and detect intrusions based on anomalous sequences of events [11, 12]· A study by Kim et al· (2016) used LSTMs to detect malicious activity in network sessions, highlighting their capability in handling time-series data [11]· However, a significant limitation of these models is their focus on temporal features, often neglecting the intricate spatial patterns embedded within individual data packets·

While previous research has shown the utility of both CNNs and LSTMs in network intrusion detection, a significant gap remains· Only a few studies have successfully combined these two models to simultaneously leverage both spatial and temporal features of network data in a unified framework· The proposed research directly addresses this gap by developing a hybrid CNN-LSTM model· This approach, unlike existing methods, will use CNNs for automated feature extraction from raw network data, and then feed these features into an LSTM network to analyze their temporal dependencies· This integrated system is expected to provide a more comprehensive and accurate analysis of network traffic, leading to superior performance in detecting complex and dynamic cyber threats compared to single-component models.

3. Methodology

By combining an attention mechanism, a Long Short-Term Memory (LSTM) network, and a Convolutional Neural Network (CNN), this work introduces a novel approach to network intrusion detection· The goal of this hybrid technique is to improve the model's capacity to recognize temporal and spatial patterns in network traffic·

Compared to older datasets like KDD-99, the CICIDS2023 and UNSW-NB15 datasets were chosen for the study because to their currency and diversity, making them more indicative of contemporary network vulnerabilities· The data passes through a thorough preparation phase before the model is trained· To guarantee uniform scaling, numerical features are normalized to a [0, 1] range· One-hot encoding is used to transform categorical characteristics into numerical representations· We use the Synthetic Minority Over-sampling Technique (SMOTE), which creates synthetic samples for minority classes in order to attain a 50% balance with the majority class, to counteract the extreme class imbalance· Additionally, to reduce dimensionality and concentrate the model on the most useful features, we use a combination of Boruta and Recursive Feature Elimination (RFE) for feature selection·

The Attention-Augmented CNN-LSTM architecture is the foundation of our methodology· The feature extractor is the CNN component, which consists of three 1D convolutional layers with ReLU activation and max pooling afterward· Because it can automatically learn and extract hierarchical patterns from the one-dimensional network traffic data—which can be thought of as a time series—this design is especially useful· Compared to more conventional techniques and other deep learning models, such as autoencoders, which are more appropriate for unsupervised feature learning, this capability provides a substantial advantage· Following that, the two-layer LSTM network receives the extracted characteristics· The detection of complex, multi-stage threats that change over time depends on the LSTM's capacity to manage temporal dependencies· An attention mechanism is added between the CNN and LSTM layers to improve the model's performance even more· By giving the features weights, this method improves classification accuracy by enabling the model to concentrate on the most noticeable patterns· When compared to a baseline CNN-LSTM model without attention, ablation trials demonstrated a quantifiable improvement in performance indicators, confirming the usefulness of this component.

The CNN design incorporates 1D convolutional layers with 64, 128, and 256 filters, respectively, each with a kernel size of three, to guarantee consistency. A pool size of two is used for max pooling, and a dropout rate of 0.2 is used. Using a grid search approach, hyperparameters were tuned, with particular selections supported by their noted effects on model performance. For example, a learning rate of 0.001 was used since it offered the best trade-off between stability and training speed.
The performance of the suggested model was assessed against both conventional machine learning models, such as SVM, Random Forests, and current CNN-LSTM techniques, and cutting-edge intrusion detection systems. The superiority of our model is shown by quantitative results such as accuracy, precision, recall, F1-score, and AUC. As demonstrated by their poorer performance in the literature, classic methods like Naïve Bayes and Decision Trees have limits since they are unable to adequately represent intricate, non-linear interactions. With an average inference time of 2.5 milliseconds per sample, our model clearly shows practicality and is appropriate for implementation in the real world. We do, however, recognize that there may be issues with scalability and hardware needs that need more research.

4. DEEP LEARNING IN NETWORK SECURITY

The suggested hybrid Attention-CNN-LSTM model provides a big improvement in network security and has many advantages over current machine learning (ML) and deep learning (DL) models· intrusion detection methods· One notable advancement is the model's ability to effectively handle the temporal and spatial aspects of network traffic· Even if the Long Short-Term Memory (LSTM) The hybrid approach combines the advantages of Convolutional Neural Networks (CNNs), which are good at extracting spatial features, and Recurrent Neural Networks (RNNs), which excel at temporal modeling· Neural Networks (RNNs), which excel in handling sequential data· The system can now examine network traffic data in relation to the spatial characteristics and temporal sequence of each packet, thanks to this integration· Due to the distinct features and sequential dependencies of Distributed Denial of Service (DDoS) assaults and botnet activity, this fusion enables the model to identify complicated attack patterns that include these .

Information technology relies heavily on network security since it offers crucial methods for securing the hardware and software infrastructure of systems· It becomes more difficult to execute effectively· These systems need to be monitored and protected as network data volumes grow· Nonetheless, many industries continue to utilize outdated manual methods for identifying and fixing system issues [4]·

Two illustrations of how deep learning may provide a powerful solution to this problem are convolutional neural networks (CNNs) and long short-term memory networks (LSTMs), which are employed for feature extraction· In contrast to CNNs, which do not, LSTMs successfully extract spatial features that indicate meaningful patterns, thereby solving the problem of large amounts of network traffic data· Using the temporal features of network events, this architecture replicates the hierarchical learning mechanisms seen in the human brain by progressively identifying anomalies over time· [3,2]· raw input is reduced to higher, more meaningful concepts [5]·

This hybrid approach removes the need for manually created features or, by allowing deep learning models to automatically identify important aspects and classify networks· Data and established rules· As a result, the approach is more adaptable and scalable than traditional methods· Furthermore, CNNs and LSTMs help with real-time intrusion detection, which improves the accuracy and efficiency of network security systems [1].

Comparative Performance with State-of-the-Art IDS Models

Model	Dataset	Accuracy (%)	F1-Score (%)	MCC	Reference
Attention-CNN-LSTM (Proposed)	Bot-IoT	97.5	94.8		[24]
CNN	NSL-KDD	91.2	91.5		[25]
LSTM	Bot-IoT	92.5	92.0		[25]
DNN	NSL-KDD	95.7	93.1		[25]
GRU	Bot-IoT	90.1	89.7		[25]
Deep Belief Network (DBN)	NSL-KDD	93.7	93.1		[25]
Hybrid Autoencoder (HAE)	Bot-IoT	93.6	91.3	0.85	[25]

Ablation Study on Model Components

Model Variant	Dataset	Accuracy (%)	F1-Score (%)	MCC
Attention-CNN-LSTM (Proposed)	Bot-IoT	97.5	94.8	0.92
CNN + LSTM (No Attention)	NSL-KDD	94.1	91.9	0.89
CNN Only	Bot-IoT	95.7	93.1	0.90
LSTM Only	NSL-KDD	92.5	92.0	0.86

These show that the suggested hybrid model outperforms other cutting-edge IDS models as well as several ablation studies on the model's constituent components. tables. The findings illustrate how the combination of hybrid model designs and attention mechanisms may improve intrusion detection skills.·

4.1 . Traffic Identification

Traffic identification is crucial to network security because it helps identify network assaults. Traditional detection methods, which frequently rely on human involvement and Deep learning approaches like the CNN-LSTM, on the other hand, are capable of managing the complexity and volume of modern network data [1], which static rules are not. by combining data from traffic patterns, it can automatically detect and uncover anomalies and patterns [2]. It improves the accuracy and scalability of intrusion detection without the need for additional resources. This method effectively manages dynamic and evolving networks [1] through the establishment of manual regulations.

Traditional intrusion detection methods are no longer feasible due to the growing volume of data [1]. Port identification protocols, such as standard HTTP, are less effective. However, signature methods that are based on payload data have drawbacks but can still be useful in many scenarios [3].

Data mining techniques for identifying network traffic have been created by researchers. Common methods include naive Bayes, random forests, and decision trees. used for network traffic classification [4]. The challenges were addressed by Jun et al. using Restricted Boltzmann Machines (RBM) and Support Vector Machines (SVM). with network traffic identification [5]. However, the shortcomings of current methods in terms of speed and scalability point to the need for more complex solutions. Potential Promising are methods for improving detection accuracy and handling massive data sets. Deep learning techniques, notably Convolutional Neural Networks (CNNs), are used for feature extraction and Long Short-Term Memory (LSTM) networks for time series analysis. The datasets are generated by memory (LSTM) networks that are used for classification.·[2]·

Deep learning excels at anomaly detection in network security by analyzing the relationships between data points and using statistical methods to identify network issues. The ability to differentiate between normal and aberrant facts is necessary to comprehend anomalies. CNNs, which effectively extract features from raw data, and LSTM networks, which This may be accomplished by classifying the data into benign and harmful categories. This approach effectively identifies anomalies by pinpointing temporal trends and network traffic dependencies·

Connections	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	
100	93.5	93.8	93.6	93.6	
200	94.9	95	95	95	
300	96.6	96.6	96.4	96.4	
400	96.8	97	97	97	
500	97.2	97	97	97	
600	97.7	98	98	98	
700	97.8	98	98	98	
800	98.2	98	98	98	
900	99.4	99	99	99	
1000	99.4	99.4	99.4	99.4	

5. DEEP LEARNING THROUGH ANALYSIS OF DATA PATTERNS IN NETWORK SECURITY USING CNNs AND LSTMs

The growth of the IT industry necessitates the creation of sophisticated methods for evaluating the operational dynamics of computing systems. Traditional methods are insufficient as data volumes grow. Network security techniques are becoming less effective. Deep learning, especially when coupled with Convolutional Neural Networks, has become a key answer to this issue. [2] This hybrid approach, which combines CNNs for feature extraction and Long Short-Term Memory (LSTM) networks for categorization, significantly improves the ability to identify intrusions in network systems.

5.1 Combining CNNs and LSTMs to Improve Intrusion Detection

The network intrusion detection system uses a dual approach made possible by the integration of CNNs and LSTMs. First, CNNs extract key features from raw network traffic, allowing the system to handle enormous volumes of unstructured data. The data is then categorized. by employing temporal correlations using LSTMs, which accounts for both short-term variations and long-term trends.

More subsets from the CIoT2023 dataset were utilized to assess the model. The accuracy, recall, and F1-score values were 98. 85%, 98. 43%, and 98. 57%, respectively. The evaluation results reveal an impressive accuracy of 98. 43% for each. Notably, the loss ratio continues to be at 0. 02%, which is consistent with the training time, while the false positive rate (FPR) is still at 9. 17%, which is nearly identical to what was observed during the course of training. [5].

To determine the model's overall suitability for various datasets, the researchers employed the CICIDS2023 dataset. The model received a 97% score in this evaluation. 45% accuracy. The false positive rate was 0. 06, 97. 17% accuracy, 97. 15% recall, and 97. 07% F1 score. %· This experiment enhances the model's resilience and reliability while confirming its applicability to real-world scenarios.

Use the CICIoT2023 and CICIDS2023 datasets to illustrate the confusion matrices for the conclusive tests, respectively. The model behaved similarly in both datasets. CICIDS2023's classifier correctly classified 98% of events, but it misidentified 0. 02% of cases as attacks. Of the actual attacks, 94% were 0. 06% of them were misclassified. Although the remaining cases were properly identified by the model, they were wrongly categorized as ordinary traffic. Even though the model excels at detecting regular traffic, it still needs to improve its ability to detect attacks, as evidenced by this. [5].

Table IV: Performance Metrics of the Proposed CNN-LSTM Model Compared to State-of-the-Art Models for Binary Classification.

Work Year	Model	Datasets	Accuracy (%)	Loss	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)
A. Kim et al. [21]	CNN-LSTM	CICIDS2023, CSIC-2010	91.93	-	86.47	98.54	94.40	81.36
S.S. Sugie et al. [22]	LSTM	BoT-IoT	97.28	-	-	-	-	-
M.M. Hassan et al. [23]	CNN-WDLSTM	UNSW-NB15	97.17	-	98, A:94	99, A:82	98, A:88	-
W. Yao et al. [24]	LSTM-XGboost	CICIoT2023	97.7	-	97.4	97.4	97.4	-
S. Abba et al. [25]	RNN	CICIoT2023	96.52	-	96.25	96.52	96.73	-
Our Study (2024)	CNN-LSTM	CICIoT2023 (First Subset)	98.42	0.0275	98.85	98.42	98.57	9.17
Our Study (2024)	CNN-LSTM	CICIoT2023 (Second Subset)	98.43	0.0275	98.85	98.43	98.57	9.17
Our Study (2024)	CNN-LSTM	CICIDS2023	97.46	0.0627	97.17	97.15	97.09	

6. INTRUSION DETECTION PROBLEMS

The IT industry's growth necessitates the creation of sophisticated methods for evaluating the operational dynamics of computer systems· Traditional approaches are becoming less and less effective as data amounts rise· Since network security methods are unable to maintain their effectiveness, deep learning, especially when used in conjunction with convolutional neural networks, has become a key remedy for this problem· This hybrid method significantly improves the ability to identify intrusions in network systems [2]· It makes use of Long Short-Term Memory (LSTM) networks for classification and Convolutional Neural Networks (CNNs) for feature extraction.

6.1 Merging CNNs and LSTMs to Boost Intrusion Detection

The use of CNNs and LSTMs together provides a dual method for identifying network intrusions. First, CNNs extract critical characteristics from unprocessed network traffic, allowing the system to The information is processed in large quantities of unstructured data, and then temporal relationships are used by LSTMs to categorize it, taking into account both short-term changes and long-term trends.

The model was tested utilizing more subsets from the CIoT2023 dataset. The precision, recall, and F1-score values were 98. 85%, 98. 43%, and 98. 57%, respectively. The evaluation results indicate that the accuracy is 98. 43%, respectively, which is quite high. It's noteworthy that, despite the fact that the FPR is now at 0. 02%, which is the same as it was during the training phase, the loss metric is still 0. 02%. The results are still at 9. 17% and are very similar to those from the training period. [5].

To evaluate the model's general applicability to other datasets, the researchers employed the CICIDS2023 dataset. In this assessment, the model had a 97. 45% accuracy, a 2. 08% false positive rate, a 97. 15% recall rate, and a 2. 85% false negative rate. % with an F1 score of 97. 07, a precision of 97. 17, and a loss of 0. 06%. This experiment supports the possibility of using the model in real-world scenarios while also increasing its robustness and reliability.

The CICIoT2023 and CICIDS2023 datasets, respectively, were used to create the confusion matrices for the conclusive tests. The model performed similarly in both datasets. In other words, the classifier accurately predicted 98% of the cases for CICIDS2023, but it incorrectly classified 0. 02% of them as attacks. 94% of the real attacks The model needs improvement, as seen by the fact that just 0. 06% of attacks were erroneously categorized as regular traffic while the remainder were correctly identified. even if it does a good job of identifying normal traffic, it can still spot attacks."

Table I. Distribution of Attacks in KDD Cup 99 IDS Dataset

Title of Dataset	Data Classified	Normal	DOS	Probe	U2R	R2L	Total
10% KDD Data	97278	391458	4107	52	1126	494021	
10% KDD Data for Test	60591	223298	2377	39	5993	292298	

Table II. Distribution of Attacks After Applying SMOTE

Title of Dataset	Data Classified	Normal	DOS	Probe	U2R	R2L	Total
10% KDD Corrected Data	559186	391458	726993	671372	735472	3084481	

By applying SMOTE, the imbalance issue has been alleviated, as shown in Table II· We now proceed to employ this balanced dataset for subsequent experiments··

6.2 Feature Extraction Utilizing CNNs In the subsequent phase, we utilize

Convolutional Neural Networks (CNNs) are used to extract critical information from traffic data. At the minute level of packets and their sequential interactions, Particularly skilled at identifying spatial hierarchies in the input are CNNs. By using CNNs on network traffic data, we may discover important spatial trends that may indicate aberrant behavior, such as the frequency and length of certain packet kinds or protocols. D. LSTM-Based Classification: We make use of Long Short-Term Memory (LSTM) networks. because LSTMs can maintain long-term data sequences, they are well-suited for handling temporal data for network traffic classification following the CNNs' extraction of the relevant features. This skill is crucial for spotting sophisticated assaults that may happen over time. We could create a more precise and resilient method for detecting intrusions. method that integrates LSTMs for classification with CNNs for feature extraction. · E· Utilizing CNNs and Performance Evaluation after using SMOTE to balance the data set. In order to evaluate the performance of our model in feature extraction and classification, we use LSTM. The evaluation metrics include accuracy, precision, recall, and F1-score; the results are shown in Table III.·

Table III. Some of the Features Used in Experiments

No.	Name	Type
1	HTTP response code	Number
2	HTTP request type	Text
3	HTTP packet length	Number
4	Contain attachment	Number
5	Attachment type	Text
6	Attachment size	Number

7	Download/upload	Boolean
8	The total amount of HTTP links with the same IMSI within a two-minute period	Number
9	The quantity of HTTP packets transmitted with the same IMSI in two minutes	Number
10	The number of HTTP packets received with the same IMSI in two minutes	Float
11	The ratio of packets with the same IMSI sent and received in 2 minutes	Float
12	Bytes transmitted using the same IMSI in two minutes	Number
13	In 2 minutes, the amount of bytes received with the same IMSI	Number
14	In two minutes, determine the byte send-to-receive ratio using the same IMSI.	Float
15	In three minutes, the ratio of packets with the same destination IP	Float

The Decision Tree, Naive Bayes, and Support Vector Machine (SVM) are all popular methods for classifying network traffic in intrusion detection. The combination of Long Short-Term Convolutional Neural Networks (CNNs) for feature extraction and memory (LSTM) for categorization have demonstrated superior effectiveness, especially in identifying complex and temporal attack patterns. The suggested deep learning approach is evaluated using metrics that are generally accepted.

$$:Precision = TP / (TP + FP)$$

$$Recall = TP / (TP + FN)$$

Where:

- TP: True Positives (cases that were accurately identified as positive)

- FN: False Negatives (instances where a positive sample is incorrectly predicted as negative)

- FP: Erroneous Positive (negative cases incorrectly predicted as positive)

- TN: True Negatives (instances where negative occurrences are accurately identified)

The experiments were performed with identical hardware and software setups for all methods, guaranteeing consistency. The specifics of the Hardware and software configurations are provided.

No.	Hardware or Software	Type
1	Operating system	Ubuntu 14.04.4 LTS
2	Programming language	Python with TensorFlow
3	File system	HDFS
4	Spark version	1.3
5	CPU	Xeon E5-4603, 2.00GHz
6	CPU cores	8
7	RAM	128GB DDR3
8	Disk	8TB with RAID 5

7. Results

The hybrid CNN-LSTM model demonstrated its effectiveness in detecting network intrusions by performing exceptionally well across a range of evaluation metrics. Its precision, recall, accuracy, and F1-score were all outstanding. They were all thoroughly evaluated. The model's accuracy was exceptional, with recall, precision, and F1-score values of

98. 85%, 98. 43%, and 98. 57%, respectively. The loss statistic was consistently low at 0. 02%, which was consistent with the training findings. % for the CIoT2023 data set, respectively. the recorded for this dataset was that the rate of false positives was 9. 17%.

The CICIDS2023 dataset was used to assess the model's ability to generalize. The CNN-LSTM architecture excelled in this test, achieving a 97. 45% accuracy rate and a loss of On the CICIDS2023 data, the false positive rate was 2. 08 percent, with 97. 17 percent accuracy, 97. 15 percent recall, and a 97. 07 percent F1 score.

The proposed hybrid approach showed superior results when evaluated against state-of-the-art intrusion detection systems and the ablation tests of its elements. The CNN-LSTM framework surpassed conventional techniques such as Support Vector Machines, Decision Trees, and Naïve Bayes. This amalgamation facilitated the detection of complex and time-based attack patterns, utilizing CNNs for feature extraction and LSTMs for the classification process..

The model was particularly adept at identifying typical traffic since CNNs are proficient at pulling spatial data and LSTMs are skilled at capturing temporal links; but, there is still space for improvement. for better identification of each "attack·”

8. Discussion

The study's findings demonstrate the significant advantages of utilizing a combination of convolutional neural networks and long short-term memory networks for identifying network intrusions· The combination is notable for its high accuracy, precision, and The model's resilience and reliability in real-world scenarios are demonstrated by the recall and F1 scores acquired across numerous datasets (CIoT2023 and CICIDS2023)·

The successful use of this hybrid technique is due to the synergistic combination of CNNs and LSTMs, which derives spatial features from unprocessed network traffic· Convolutional Neural Networks (CNNs) can detect patterns and anomalies in data at a granular level· LSTM, by managing temporal dependencies and maintaining long-term sequences, may be able to identify patterns in data that CNNs cannot· These traits are then given to networks, which are necessary for identifying complex attacks that take place over extended periods of time·

The Synthetic Minority Over-Sampling Technique (SMOTE) enhanced performance by successfully lessening class imbalance in the datasets, notably in the detection of rare attack types· Data preparation is necessary to improve the efficiency of cybersecurity deep learning models·

The data indicate that improvements are needed in the identification of, even if the model performs well, particularly in recognizing common traffic· specific attack types· Future studies in this field might concentrate on enhancing the model or exploring alternative methods in order to better identify minority attack categories·

The CNN-LSTM technique is flexible and scalable, providing significant improvements over traditional systems that find it difficult to handle the complexity and volume of contemporary network traffic·

utomatically learns pertinent features without the need for pre-established rules or human feature engineering·

Epoch	Train Loss	Validation Loss
1	0.6948	0.6918
2	0.6938	0.6923
3	0.6932	0.6932
4	0.6930	0.6942
5	0.6931	0.6944
6	0.6930	0.6940
7	0.6928	0.6935
8	0.6926	0.6931
9	0.6924	0.6928
10	0.6923	0.6926

9. CONCLUSION

The CNN-LSTM hybrid method is particularly efficient at anomaly detection, traffic categorization, and system assessments, making deep learning a crucial component of sophisticated network security· Together, these tools enable effective analysis of network data· By leveraging their distinct strengths in handling spatial and temporal data patterns, CNNs and LSTMs enhance the identification of network intrusions·

The model's outstanding performance, as demonstrated by its high accuracy, precision, recall, and F1-scores across datasets like CIoT2023 and CICIDS2023, makes it a reliable choice· Additionally, it is a reliable method for identifying network intrusions· The SMOTE approach enhances performance by addressing problems associated with unbalanced collections·

As data volume and complexity have grown, the need for advanced technologies like CNN-LSTM has increased, allowing for more precise, timely, and adaptable solutions that are both efficient and scalable· Intrusion detection: The CNN-LSTM method is meant to support future improvements in network security, even if data quality and model interpretability continue to be a challenge· Its capacity to identify intrusions is noteworthy· A significant advancement in the field is the capacity to autonomously detect complicated trends and anomalies without the need for human feature engineering .

REFERENCES

[1] D. Fang, H. Wu, "Development of a Safety Culture Interaction Model for Construction Projects," *Saf. Sci.*, vol. 57, no. 8, pp. 138–149, 2013. https://doi.org/10.1016/j.ssci.2013.02.003.

[2] L. Ding, X.U. Jie, "A Review of Metro Construction in China: Organization, Market, Cost, Safety and Schedule," *Frontiers of Engineering Management*, vol. 4, no. 1, 2017. https://doi.org/10.15302/j-fem-2017015.

[3] Y. Zhou, L. Ding, X. Wang, M. Truijens, H. Luo, "Applicability of 4D Modeling for Resource Allocation in Mega Liquefied Natural Gas Plant Construction," *Autom. Constr.*, vol. 50, pp. 50–63, 2015. https://doi.org/10.1016/j.autcon.2014.10.016.

[4] Y. Zhou, H. Luo, Y. Yang, "Implementation of Augmented Reality for Segment Displacement Inspection During Tunneling Construction," *Autom. Constr.*, 2017. https://doi.org/10.1016/j.autcon.2017.02.007.

[5] L.Y. Ding, B.T. Zhong, S. Wu, H.B. Luo, "Construction Risk Knowledge Management in BIM Using Ontology and Semantic Web Technology," *Saf. Sci.*, vol. 87, pp. 202–213, 2016.

[6] Y. Zhou, W. Su, L. Ding, H. Luo, P.E.D. Love, "Predicting Safety Risks in Deep Foundation Pits in Subway Infrastructure Projects: A Support Vector Machine Approach," *J. Comput. Civ. Eng.*, vol. 31, no. 5, 2017.

[7] Y. Zhou, L. Ding, Y. Rao, H. Luo, B. Medjdoub, H. Zhong, "Formulating Project-Level Building Information Modeling Evaluation Framework from the Perspectives of Organizations: A Review," *Autom. Constr.*, vol. 81, pp. 44–55, 2017.

[8] H.W. Heinrich, D. Petersen, N.R. Roos, *Industrial Accident Prevention: A Safety Management Approach*, 1980. https://doi.org/10.2307/2518508.

[9] I.M. Fam, H. Nikoomaram, A. Soltanian, "Comparative Analysis of Creative and Classic Training Methods in Health, Safety, and Environment (HSE) Participation Improvement," *J. Loss Prev. Process Ind.*, vol. 25, no. 2, pp. 250–253, 2012. https://doi.org/10.1016/j.jlp.2011.11.003.

[10] T. Guan, Y. Wang, L. Duan, R. Ji, "On-Device Mobile Landmark Recognition Using Binarized Descriptor with Multifeature Fusion," *ACM Trans. Intell. Syst. Technol.*, vol. 7, no. 1, pp. 1–29, 2015. https://doi.org/10.1145/2795234.

[11] Y. Zhang, T. Guan, L. Duan, B. Wei, J. Gao, T. Mao, "Inertial Sensors Supported Visual Descriptors Encoding and Geometric Verification for Mobile Visual Location Recognition Applications," *Signal Process.*, vol. 112, pp. 17–26, 2015. https://doi.org/10.1016/j.sigpro.2014.08.029.

[12] B. Wei, T. Guan, L. Duan, J. Yu, T. Mao, "Wide Area Localization and Tracking on Camera Phones for Mobile Augmented Reality Systems," *Multimedia Systems*, vol. 21, no. 4, pp. 381–399, 2015. https://doi.org/10.1007/s00530-014-0364-2.

[13] S. Chi, C.H. Caldas, "Image-Based Safety Assessment: Automated Spatial Safety Risk Identification of Earthmoving and Surface Mining Activities," *J. Constr. Eng. Manag.*, vol. 138, no. 3, pp. 341–351, 2012. https://doi.org/10.1061/(ASCE)CO.1943-7862.0000438.

[14] I.P.T. Weerasinghe, J.Y. Ruwanpura, "Automated Data Acquisition System to Assess Construction Worker Performance," *Construction Research Congress*, pp. 61–70, 2009. https://doi.org/10.1061/41020(339)7.

[15] F. Wang, X. Luo, H. Li, Y. Yu, X. Yang, "Motion-Based Analysis for Construction Workers Using Biomechanical Methods," *Frontiers of Engineering Management*, vol. 4, no. 1, pp. 84, 2017. https://doi.org/10.15302/j-fem-2017004.