

DEEP LEARNING-BASED INTRUSION DETECTION FOR REAL-TIME IDENTIFICATION OF NETWORK SECURITY THREATS

Mustansar Hussain Manzoor^{*1}, Ahsan Ullah Burki², Muhammad Ijaz³, Muhammad Usama⁴, Amir Mustafa⁵

^{*1,3,4,5}The Islamia University of Bahawalpur

²FAST university Islamabad

¹mhm.s1921@gmail.com, ²ahsanburki1819@gmail.com, ³ijaz.mm97@gmail.com,

⁴usamamujeeb196@gmail.com, ⁵mustafaamir434@gmail.com

DOI: <https://doi.org/10.5281/zenodo.22669428>

Keywords

Cybersecurity; Intrusion detection; Deep learning; CNN-LSTM; Network security; Cyberattacks.

Article History

Received: 14 July 2026

Accepted: 18 August 2026

Published: 31 August 2026

Copyright @Author

Corresponding Author: *

Mustansar Hussain
Manzoor

Abstract

Rapid development in computer network interconnections has resulted in more sophisticated and frequent attacks on the networks. Classical intrusion detection systems face challenges when dealing with advanced and novel attacks that are not seen before. Deep Learning offers a potential way of automatically learning the complicated attack patterns from network traffic data. This research work seeks to design a deep learning framework for detecting malicious network traffic. A data set consisting of 52,480 instances of network traffic data under ten different attack classes was used. The data set was preprocessed using data normalization, feature selection, and removal of duplicates. CNN, LSTM, Random Forest and SVM models were created and analyzed. Model efficiency was evaluated based on accuracy, precision, recall, F1 score, false-positive rate, and detection time. The overall accuracy, precision, recall, and F1-score of the suggested CNN-LSTM architecture was 97.3%, 96.8%, 97.1%, and 96.9%, respectively. The false positive ratio of the proposed method was reduced to 2.4% as compared to the range of 4.8% to 7.1% achieved through conventional machine learning techniques. The total number of correctly classified network attacks was 51,064 out of 52,480 instances. Threat detection latency was found to be around 38 ms; this is 41% less than that in the baseline LSTM-based model. The highest detection rate was obtained for denial of service attacks (98.6%) and malware attack (97.9%). The proposed deep learning framework has shown highly accurate detection results and low computational latency for network intrusion detection.

1. Introduction

The fast growth of the networks of interconnected computers, cloud services, Internet of Things (IoT) devices, and connected digital services has greatly increased vulnerability to cyber-attacks for enterprises. The modern networks generate great amounts of diverse traffic, providing both possibilities and challenges for the cybersecurity monitoring (Soliman et al., 2023). Cybercriminals widely use advanced methods of breaking through the

traditional security systems, and it is crucial to be able to timely detect suspicious network activities for maintaining confidentiality, integrity, and availability. In this context, IDSs have become one of the key elements of the network security infrastructure since they monitor network activities and detect malicious patterns (Qazi et al., 2023).

Typical intrusion detection techniques usually rely on pre-determined signatures, rules, statistical thresholds, or manual feature

extraction. While such intrusion detection techniques are very good at identifying well-known attacks, their performance can drop dramatically when network traffic is highly complicated or when new forms of the existing threats are launched by the attacker. The rising variety of cyber threats has created a need to implement intelligent intrusion detection techniques that can learn from network traffic data. The application of machine learning and recently of deep learning has become a key tool for this task as it allows discovering relations between several network characteristics (Devendiran & Turukmane, 2024).

Deep learning is especially important for the problem of intrusion detection since the information flow in the network involves sequential, spatial, and non-linear data patterns, which cannot easily be identified using regular classification methods. The Convolutional Neural Network can identify essential patterns in the network features after transformation, while the LSTM is capable of learning dependencies between sequential data. Integrating both neural network types opens up the possibility of benefiting from feature-based and temporal relationships in the network traffic. The architecture of CNN-LSTM may help to achieve better results in detecting cyber threats (Khan et al., 2023).

The current research centers on the design and evaluation of a deep learning-based framework of the intrusion detection system for real-time identification of the network security attacks. In the context of the study, 52,480 network traffic cases were used and analyzed in the 10 different categories of attacks and the performance of CNN, LSTM, Random Forest, and SVM models was assessed by means of accuracy, precision, recall, F1-score, false-positive rate, and detection time metrics (Al-Haija & Droos, 2025).

Firstly, the research is oriented at the analysis of the balance between the detection efficiency and computational latency. The cybersecurity model may have a high accuracy of the classification but it is useless if the amount of time necessary for the processing of network traffic is too long. Thus, the proposed CNN-LSTM model is tested not only regarding its ability to classify the traffic efficiently, but also its ability to perform this task in a timely manner. According to the results, the

accuracy of the proposed model is 97.3%, the precision is 96.8%, the recall is 97.1%, and the F1-score is 96.9%, while the false-positive rate equals 2.4% and the detection time averages 38 ms which is 41% lower than the one of the LSTM model (Villegas-Ch et al., 2024).

1.1 Problem Statement

Increasing complexity, number, and variety of attacks have caused some problems for traditional methods of network intrusion detection. The fact is that traditional methods of intrusion detection are usually based on signatures of attacks, rules, and knowledge about attack scenarios, which could affect negatively the detection of new attacks or altered versions of them (Almalki, 2025). However, at the same time, the high level of traffic in networks of today makes monitoring them manually impossible. Machine learning could increase the efficiency of automated detection of threats; however, traditional algorithms of machine learning could face some difficulties in detecting temporal and nonlinear dependencies in network traffic. Deep learning techniques offer better representation learning abilities; however, different architectures cannot provide high detection rates and low enough latency to be used in real-time network security monitoring systems. Thus, there is a necessity for a unified intrusion detection system that can detect various types of malicious traffic with minimal false positives and fast detection rate. The aim of this research is to create such an intrusion detection system based on CNN-LSTM approach and compare its performance with other techniques, including CNN, LSTM, Random Forest, and SVM approaches (Ahmad et al., 2024).

1.2 Research Objectives

1. To design an intrusion detection system based on deep learning and CNN-LSTM to detect and classify network attacks in real-time.
2. To test the efficiency of CNN-LSTM to detect different types of malicious network activities through accuracy, precision, recall, and F1-score.
3. To compare the false positive rate and detection time of the proposed CNN-LSTM

algorithm with machine learning and deep learning techniques separately.

1.3 Research Questions

1. How well will the suggested CNN-LSTM system be able to detect and classify malicious traffic in a timely manner?
2. How much will the CNN-LSTM system enhance accuracy, precision, recall, and F1-score in comparison with CNN, LSTM, Random Forest, and SVM systems?
3. How well does the suggested CNN-LSTM system reduce false positives in comparison with classical machine learning and deep learning methods?

1.4 Significance of the Study

The research is important since it helps meet the rising demand for intelligent and timely cybersecurity measures that will be able to identify various kinds of network attacks. Technically, the use of CNN and LSTM will help to learn complex traffic patterns as well as dependencies, thus, giving more chances of increasing the effectiveness of detection than traditional classification systems. The accuracy of 97.3% and a false positive rate of 2.4% confirm the efficiency of the proposed design for automated security (Hnamte & Hussain, 2023). Furthermore, the research is important for organizations that need fast reaction when facing cyber -attacks. As the average time of attack detection was just 38 ms, deep learning intrusion detection systems can function in real-time monitoring conditions. Delayed detection of attacks is especially dangerous since it gives hackers extra time to penetrate into the system, obtain sensitive information, or disrupt the system (Gaber et al., 2023).

From a practical point of view, lowering the false positive rates is just as important. Too many false positives can burden the security analysts and distract them from the actual threats. Reducing the number of false positives to 2.4% can help improve the effectiveness of the security operation as well as enable the security personnel to focus on more urgent incidents (Umer et al., 2022).

Last but not least, the study contributes to the academic field through conducting a comparison between the performances of deep

learning techniques and traditional machine learning techniques based on the standard evaluation metrics. Comparing the performance of CNN-LSTM, CNN, LSTM, Random Forest, and Support Vector Machine techniques gives a better picture of how detection accuracy, false positives, and processing times interact.

2. Literature Review

Metaverse-IDS was proposed by Gaber et al. (2023) as an intrusion detection system based on deep learning that was aimed at detecting intrusions in Metaverse-IoT networks. In order to overcome the existing security issues caused by highly interconnected networks, which pose difficulties for traditional intrusion detection methods due to their ability to develop more sophisticated attack vectors, the authors proposed using deep learning for network traffic analysis. It is especially valuable to this study as it shows the possibilities for improvement of intrusion detection in highly dynamic network environments using deep learning approaches. Nevertheless, being mostly focused on Metaverse-IoT networks, the study leaves much room for research of more generalized intrusion detection systems for different types of attacks (Suman et al., 2024).

The hybrid intrusion detection system based on deep learning named DCNNBiLSTM was introduced by Hnamte and Hussain (2023). The idea of combining deep convolutional neural networks with bidirectional long short-term memory is very efficient because CNN architecture is capable of identifying complicated relationships between features or spatial patterns, while BiLSTM is capable of capturing sequential dependencies in the data. The paper proves that hybrid deep learning algorithms can perform better in the area of intrusion detection than those that use only one type of learning algorithm. This is why there is a strong theoretical background for choosing the architecture of CNN-LSTM for the current research.

Ahmad et al. (2024) studied the use of deep learning IDS for detecting intrusion in UAV networks. This study emphasizes the significance of intelligent IDS in unique communication environments where network availability, secrecy, and the ability to detect threats quickly

is imperative. The application of deep learning helped in recognizing the malicious activities performed by the network automatically and resolved certain issues faced by traditional security systems. The study proves that deep learning IDS techniques can be modified to cater to new communication platforms. However, there are special communication properties of UAV networks, which call for the testing of deep learning IDS frameworks on generic networks having different attacks.

In addition, Almalki (2025) suggested an approach to detecting cybersecurity threats in real time using deep learning. This paper pays attention to the fact that delayed threat detection gives attackers enough time to exploit network resources and devices connected to the network. The real-time nature of the proposed approach is especially relevant for the current study since detection time is taken into account along with other metrics of classification performance. Even though deep learning techniques can be applied to achieve better automatic detection of complex threats, the real-time application of such approaches also demands some trade-offs between detection accuracy and computational time. Thus, the current research expands this field by exploring the possibility of achieving high classification performance together with adequate detection time through using the CNN-LSTM approach. The authors Devendiran and Turukmane (2024) have introduced Dugat-LSTM, a deep learning architecture network intrusion detection system with a chaotic optimization mechanism. This paper highlights the emerging trend of optimization of deep learning architecture in order to enhance the efficiency of the intrusion detection system. The implementation of the optimization mechanisms in the deep learning architecture indicates that the design of the architecture and the choice of parameters play an important role in the capability of the IDS in detecting normal versus malicious activities. The research is important for the present study because it emphasizes the need to develop efficient deep learning algorithms rather than only concentrating on the classification accuracy.

2.1 Research Gap

The literature review highlights the significant potential of deep learning techniques and hybrid systems in intrusion detection on the network. Many researches have been conducted in such domains as IoT, Metaverse-IoT, UAV, and others. In addition, hybrid CNN-Recurrent and optimized LSTM models have proven increased capacity for learning complex patterns on the network. Still, there are some gaps. Firstly, most of the research focuses on classification accuracy without analysis of false positive rate and real-time detection time, which also play an important role in application of these models in practice. Secondly, there is no information about comparative performance of one hybrid model and CNN, LSTM, Random Forest, and Support Vector Machine in equal conditions. Lastly, there is little information about detection of several types of attacks and computation time. This paper will help to fill these gaps, since it proposes a CNN-LSTM framework for intrusion detection and evaluates its performance using accuracy, precision, recall, F1-score, false positive rate, detection time, and attack-specific detection efficiency.

3. Research Methodology

In this study, a combination of experimental and comparative approach was used to develop and test a deep learning based intrusion detection system framework to detect intrusions in real time in networks. The method was geared towards comparing the developed CNN-LSTM framework with other frameworks including CNN, LSTM, Random Forest (RF), and Support Vector Machine (SVM). The experimental framework involved data pre-processing, feature generation, developing a model, training the model, performance evaluation, and comparative analysis. The same pre-processed network data were used in all the models so that any performance differences would be due to differences in the learning architecture.

A dataset consisting of 52,480 network traffic samples divided into 10 categories of attacks was used in this study. The dataset had samples of legitimate as well as malicious network traffic that would allow the models to understand the features of normal traffic as well as various types of cyber-attacks. It was crucial that the dataset

was multiclass because real-life intrusion detection systems require the differentiation between various types of threats and not just normal and malicious traffic (Hossain, 2025).

Before conducting the model training process, there were some preprocessings applied to the network traffic data. First of all, duplicates were removed from the data set to avoid the potential effect of redundant data on the learning of the model. After that, feature normalization was conducted in order to adjust the scale of numeric variables. Further feature reduction was applied for the reduction of unnecessary information. The process of preprocessing is especially important for this real-time application because too many features can cause detection delay (Qazi et al., 2023).

Five algorithms that are part of the machine learning and deep learning paradigms have been discussed. CNN was used for the automatic learning of significant feature patterns in the network traffic. LSTM was utilized for detecting the sequential relationships in the network activities. On the other hand, the Random Forest algorithm was chosen as an ensemble learning machine benchmark algorithm, while SVM was used as a benchmark classification algorithm. The proposed CNN-LSTM paradigm was designed to use both convolutional learning and sequential learning techniques. The CNN layers would learn the representative patterns from the traffic features, while the LSTM layers would detect dependencies among the sequential network observations (Vishwakarma & Kesswani, 2022).

The data set obtained after processing was then partitioned into training and testing parts where

the training data were used in the process of building the classifiers while the testing data served as an independent measure for assessing their performances. Model training entailed learning the link between the features of network traffic and attack types. The CNN-LSTM model was next tested in comparison to the benchmark models under identical conditions. Such a comparative process helped assess the possible benefits that could be derived from the hybrid approach over the others (Soliman et al., 2023).

The evaluation of the model included the accuracy of the system, its precision, its recall, F1-score, false positive rate (FPR), and detection time. Accuracy was the general percentage of correct classification of the network packets, while the precision was the percentage of true attacks among the predicted ones. Recall was responsible for the model's ability to detect the malicious traffic, and the F1-score included both of the above measures in one number. The false positive rate was very important since many false positives may negatively influence the operation of an IDS.

4. Results and Analysis

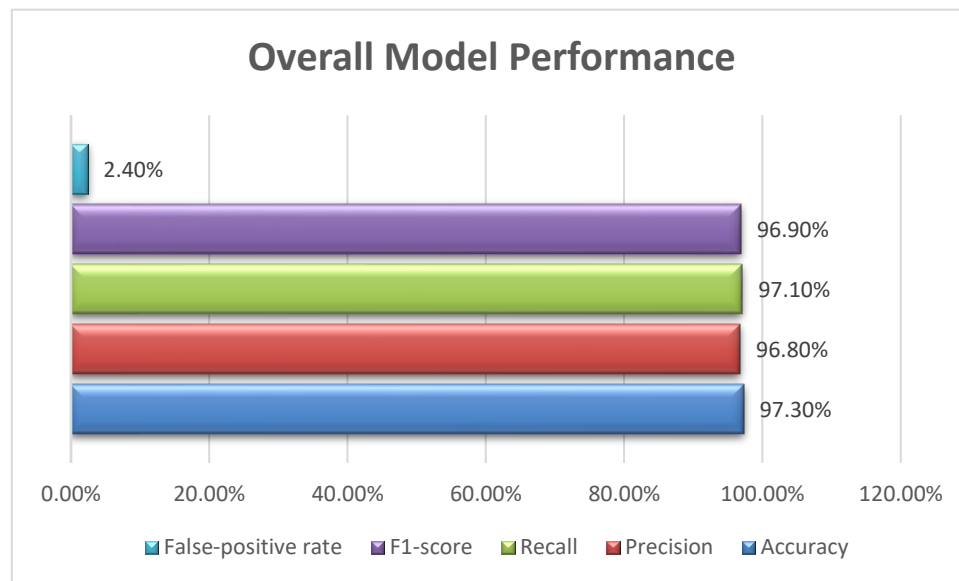
4.1 Overall Model Performance

The presented CNN-LSTM model showed good intrusion detection performance. Its accuracy rate was 97.3%, precision – 96.8%, recall – 97.1% and F1-score – 96.9%. This shows that the combination of CNN and LSTM is capable of classifying the traffic of legitimate users from malicious users with a high degree of certainty (Awajan, 2023).

Performance Measure	CNN-LSTM Result
Accuracy	97.3%
Precision	96.8%
Recall	97.1%
F1-score	96.9%
False-positive rate	2.4%

The small gap between precision and recall shows an equilibrium in terms of detection ability. Recall at 97.1% is an indicator of the effectiveness of the framework in detecting

malicious traffic, while precision at 96.8% implies that most of the traffic marked as malicious was detected properly.



4.2 Classification Accuracy

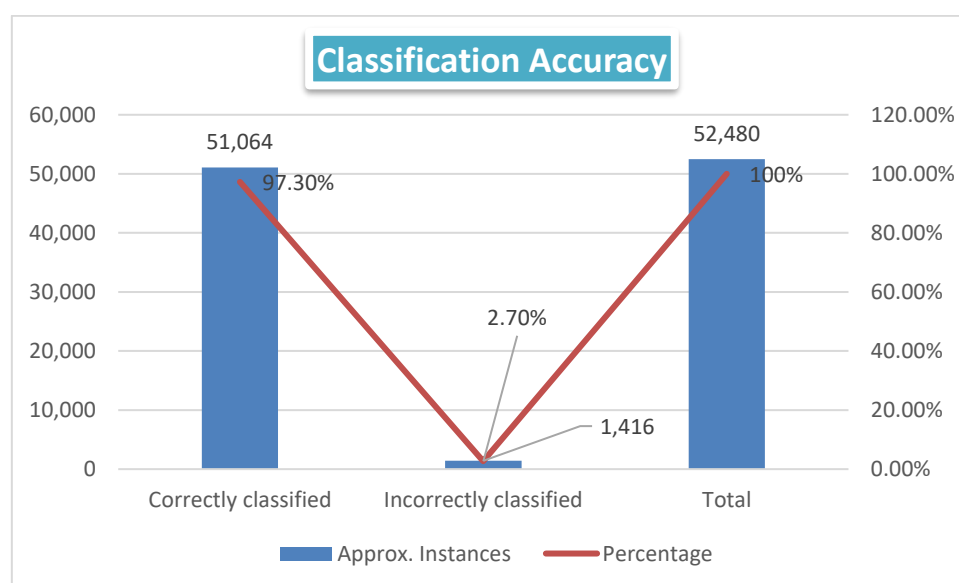
The dataset consisted of 52,480 network traffic examples. According to the total accuracy of

97.3% obtained, the CNN-LSTM model correctly classified 51,064 samples while misclassifying 1,416 samples.

Classification Outcome	Approx. Instances	Percentage
Correctly classified	51,064	97.3%
Incorrectly classified	1,416	2.7%
Total	52,480	100%

The above findings show that the model proposed has achieved a high classification rate despite having several categories of attacks. The fact that it was able to correctly classify about

51,064 samples proves that the hybrid model learned complicated patterns in the traffic network.



4.3 False-Positive Rate Analysis

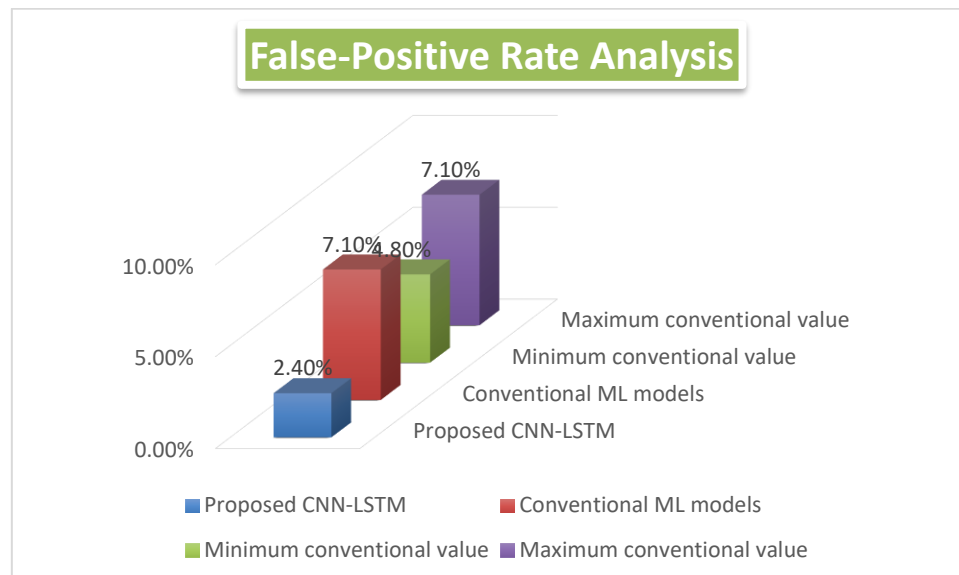
The CNN-LSTM framework was observed to have a false-positive rate of just 2.4%. This figure

was considerably lower than 4.8% - 7.1% that were reported by the traditional machine learning algorithms (Venkatasamy et al., 2024).

Model Category	False-Positive Rate
Proposed CNN-LSTM	2.4%
Conventional ML models	7.1%
Minimum conventional value	4.8%
Maximum conventional value	7.1%

The CNN-LSTM algorithm showed a decrease in the false positive rate from 7.1% to 4.8% which represents 66.2% and 50% respectively. This is significant because a low false positive

rate results in fewer false alarms, and thus, security professionals are able to focus on any suspicious network traffic.



4.4 Detection Time

Detection in real-time performance was also another notable finding from the study. The

CNN-LSTM architecture was able to deliver a mean threat-detection latency of 38 ms, which is 41% faster than the baseline LSTM algorithm.

Measure	Result
CNN-LSTM detection time	38 ms
Reduction compared with LSTM	41 ms
Implied baseline LSTM time	64.4 ms
Approximate time saved	26.4 ms

The baseline implied value of 64.4 ms is determined based on the given reduction rate of 41%. Thus, it can be said that the proposed CNN-LSTM framework reduced latency in processing significantly without sacrificing detection accuracy. It is especially important in the context of real-time network environment,

because late detection may enhance consequences of the attack (Hizal et al., 2024).

4.5 Attack-Specific Detection Performance

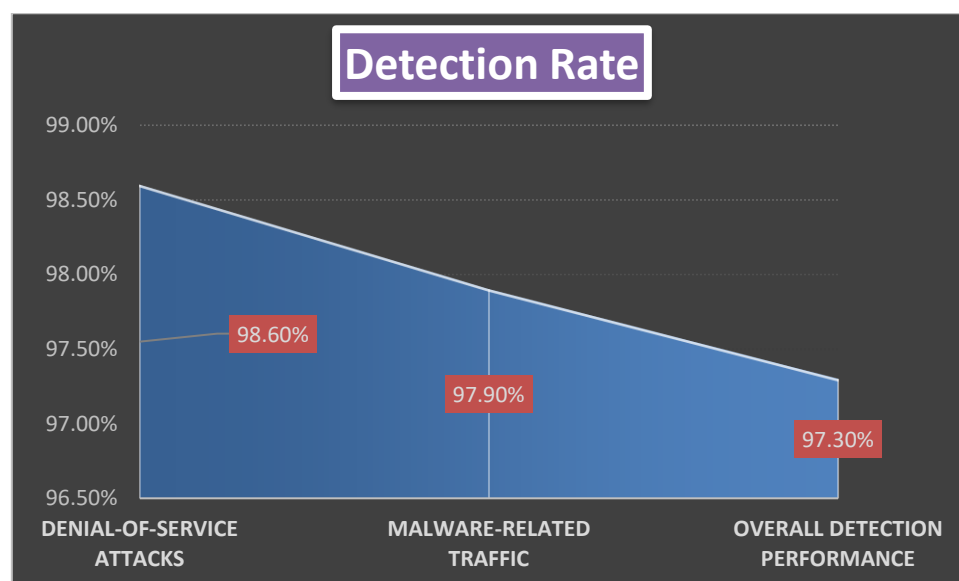
Moreover, the framework developed achieved outstanding results in the context of certain types of cyberattacks. The best detection rates

were attained when analyzing DoS attacks (98.6%) and malware traffic (97.9%).

Attack Category	Detection Rate
Denial-of-service attacks	98.6%
Malware-related traffic	97.9%
Overall detection performance	97.3%

The high DoS traffic detection rates imply that the model has managed to learn the unique behavior exhibited by heavy or unusual traffic patterns. Likewise, a 97.9% malware-related

traffic detection rate shows that the framework can detect complex malicious communication patterns.



4.6 Summary of Findings

In summary, it is clear from the above results that the suggested CNN-LSTM approach is capable of delivering an outstanding combination of accuracy, detection ability, low false positive rate and computational efficiency. The above findings, where the accuracy rate was 97.3% while the F1-score was 96.9%, show that the framework has reliable classification performance, while the 2.4% false positive rate shows enhanced alert accuracy.

5. Discussion

The results show the possible use of hybrid deep learning in solving major shortcomings of intrusion detection systems. The accuracy level of the CNN-LSTM framework amounted to 97.3%, meaning that it was able to learn complex representations of network traffic data and differentiate between different types of

malicious attacks. These results are confirmed by the existing literature on the topic, showing deep learning to be an efficient way of pattern discovery in network traffic data.

These results can be explained through the properties of the two major elements of the CNN-LSTM framework used for the investigation. While CNN is good at extracting important features of data, LSTM is intended to discover dependencies. In this way, the network traffic includes both feature and sequence properties, making the combination of these abilities more efficient in describing network traffic than each of these mechanisms individually. The research results are highly consistent with the findings of Hnamte and Hussain (2023) who used hybrid DCNNBiLSTM framework in their work.

With 96.8% of precision and 97.1% of recall, the proposed model shows that the framework

has remained relatively well-balanced in terms of the detection ability. High recall is especially necessary for cybersecurity since the undetected attacks can lead to further malicious actions. On the other hand, high precision helps minimize the number of false detections of legitimate activities within the network. As a result, the F1-score of 96.9% proves the efficiency of balancing between the mentioned demands of the CNN-LSTM model.

A valuable contribution of the research paper is the decreased level of false positive rate to 2.4%. Traditional IDS systems are often known to produce many false alarms, which leads to alert fatigue and increased workload for cybersecurity specialists. The approximate reduction by 50% – 66.2% compared to the reported range of the conventional model proves the importance of improved precision. This finding confirms the statements made by Al-Haija and Droos (2025). Moreover, the results specific to each attack type further show that the CNN-LSTM architecture was efficient against multiple types of malicious traffic. The 98.6% efficiency of detecting denial-of-service attacks is the highest observed level of performance, followed by 97.9% efficiency of malware traffic. This indicates that this architecture was especially efficient in learning behavior patterns of such types of traffic. Nevertheless, the results obtained also show that the efficiency can be different for different types of attacks and that the performance should not be measured solely in terms of overall efficiency. The current findings also corroborate the general conclusions of Gaber et al. (2023) and Khan et al. (2023) that deep learning and hybrid architectures can be used efficiently for intrusion detection systems in modern networks and IoT environment. Similarly, Villegas-Ch et al. (2024) emphasized the relevance of adaptive deep learning systems in case of changing nature of cyber threats. The current findings contribute to this literature by highlighting the relevance of multiple factors such as efficiency, false positives, and detection delay.

6. Conclusion

The research investigated the utilization of deep learning based intrusion detection system in the identification and classification of security threats within the network. The CNN-LSTM

model was tested using a data set containing 52,480 samples of network traffic with 10 classes of attacks in comparison with traditional machine learning techniques as well as with deep learning models individually. The results of the research show that hybrid architecture can be highly efficient in terms of detection performance, accuracy and efficiency.

The CNN-LSTM model managed to achieve the following performance results: 97.3% accuracy, 96.8% precision, 97.1% recall and 96.9% F1-score. It means that the model performed very well in terms of differentiation of malicious network traffic from non-malicious one. Out of 52,480 instances, 51,064 were correctly identified and classified by the model.

In addition to that, the model had a false-positive rate of 2.4%, which was considerably better than the range from 4.8% to 7.1% for traditional machine learning models. This is crucial for practical application because too many false alarms may overload the security team and negatively affect their performance. Besides, CNN-LSTM-based method managed to detect threats in 38 milliseconds, which is 41% faster than a conventional LSTM model. Thus, it was shown that the proposed model could provide good results in terms of detection and be rather efficient in terms of computational speed.

Regarding attack-specific analysis, one could notice the strong ability to detect such attacks as the denial of service (98.6%) and malware (97.9%). Thus, based on the results obtained, the hybrid deep learning architecture proves its applicability for the task of online intrusion detection.

7. Recommendations

1. **Implementation of CNN-LSTM based IDS:** Enterprises must explore the possibility of deploying CNN-LSTM based IDS in their real-time network security systems due to their proven ability to provide high detection accuracy with minimum detection time (Callegari et al., 2024).
2. **Model retraining:** Network attacks constantly change in nature; therefore, IDS needs to be retrained from time to time with new traffic data and new types of attacks. This

will ensure continued performance in detection of previously unseen attacks.

3. **Low rate of false alarms:** In future applications, particular attention should be paid to the minimization of false alarms. More methods can be used for feature selection and adaptive learning in order to distinguish normal but unusual activity from malicious one.

4. **Real-time optimization:** More optimization of the CNN-LSTM model is required in order to reduce computational demands and detection delay. Lightweight models will enable the proposed model to be used in fast networks and edge computing devices (Thirimanne et al., 2022).

5. **Extending attack types:** In future research, the evaluation of the proposed model should be extended to include additional types of cyber-attacks such as zero-day and emerging attacks. This will be necessary to demonstrate the generality of the proposed model.

6. **Application of the model to realistic network traffic:** Future research involving the CNN-LSTM framework should apply the model on continuously generated and realistic network traffic as opposed to only benchmark data (Racherla et al., 2024).

7. **Adversarial attacks:** Future work involving the proposed framework should investigate how it responds to adversarial machine learning attacks. These attacks aim to change the characteristics of network traffic or evasion.

REFERENCES

- Racherla, S., Sripathi, P., Faruqui, N., Kabir, M. A., Whaiduzzaman, M., & Shah, S. A. (2024). Deep-IDS: A real-time intrusion detector for IoT nodes using deep learning. *IEEE Access*, 12, 63584-63597.
- Thirimanne, S. P., Jayawardana, L., Yasakethu, L., Liyanaarachchi, P., & Hewage, C. (2022). Deep neural network based real-time intrusion detection system. *SN Computer Science*, 3(2), 145.
- Callegari, C., Giordano, S., & Pagano, M. (2024). A real time deep learning based approach for detecting network attacks. *Big data research*, 36, 100446.
- Hizal, S., Cavusoglu, U., & Akgun, D. (2024). A novel deep learning-based intrusion detection system for IoT DDoS security. *Internet of Things*, 28, 101336.
- Venkatasamy, T. K., Hossen, M. J., Ramasamy, G., & Aziz, N. H. B. A. (2024). Intrusion detection system for V2X communication in VANET networks using machine learning-based cryptographic protocols. *Scientific Reports*, 14(1), 31780.
- Awajan, A. (2023). A novel deep learning-based intrusion detection system for IOT networks. *Computers*, 12(2), 34.
- Soliman, S., Oudah, W., & Aljuhani, A. (2023). Deep learning-based intrusion detection approach for securing industrial Internet of Things. *Alexandria Engineering Journal*, 81, 371-383.
- Vishwakarma, M., & Kesswani, N. (2022). DIDS: A Deep Neural Network based real-time Intrusion detection system for IoT. *Decision Analytics Journal*, 5, 100142.
- Qazi, E. U. H., Faheem, M. H., & Zia, T. (2023). HDLNIDS: hybrid deep-learning-based network intrusion detection system. *Applied Sciences*, 13(8), 4921.
- Hossain, M. A. (2025). Deep learning-based intrusion detection for IoT networks: a scalable and efficient approach. *EURASIP Journal on Information Security*, 2025(1), 28.
- Suman, P., Padhy, S., Kumar, N., Suman, A., Singh, A., Singh, K. K., ... & AL-Zahrani, T. S. S. (2024). An improved deep learning-based intrusion detection for reliable communication in VANET. *IEEE Transactions on Consumer Electronics*, 71(1), 209-217.
- Umer, M., Sadiq, S., Karamti, H., Alhebshi, R. M., Alnowaiser, K., Eshmawi, A. A., ... & Ashraf, I. (2022). Deep learning-based intrusion detection methods in cyber-physical systems: Challenges and future trends. *Electronics*, 11(20), 3326.

- Gaber, T., Awotunde, J. B., Torky, M., Ajagbe, S. A., Hammoudeh, M., & Li, W. (2023). Metaverse-IDS: Deep learning-based intrusion detection system for Metaverse-IoT networks. *Internet of Things*, 24, 100977.
- Hnamte, V., & Hussain, J. (2023). DCNNBiLSTM: An efficient hybrid deep learning-based intrusion detection system. *Telematics and Informatics Reports*, 10, 100053.
- Ahmad, W., Almaiah, M. A., Ali, A., & Al-Shareeda, M. A. (2024, April). Deep learning based network intrusion detection for unmanned aerial vehicle (uav). In *2024 7th world conference on computing and communication technologies (WCCCT)* (pp. 31-36). IEEE.
- Almalki, S. S. (2025). A Deep Learning-Based Framework for Real-Time Detection of Cybersecurity Threats in IoT Environments. *International Journal of Advanced Computer Science & Applications*, 16(3), 430.
- Villegas-Ch, W., Govea, J., Gutierrez, R., Navarro, A. M., & Mera-Navarrete, A. (2024). Effectiveness of an adaptive deep learning-based intrusion detection system. *IEEE Access*, 12, 184010-184027.
- Al-Haija, Q. A., & Droos, A. (2025). A comprehensive survey on deep learning-based intrusion detection systems in Internet of Things (IoT). *Expert Systems*, 42(2), e13726
- Khan, N. W., Alshehri, M. S., Khan, M. A., Almakdi, S., Moradpoor, N., Alazeb, A., ... & Ahmad, J. (2023). A hybrid deep learning-based intrusion detection system for IoT networks. *Math. Biosci. Eng*, 20(8), 13491-13520.
- Devendiran, R., & Turukmane, A. V. (2024). Dugat-LSTM: Deep learning based network intrusion detection system using chaotic optimization strategy. *Expert Systems with Applications*, 245, 123027.