International Journal of Emerging Research in Engineering and Technology
Pearl Blue Research Group | Volume 7 Issue 1 PP 146-153, 2026
ISSN: 3050-922X | https://doi.org/10.63282/3050-922X.IJERET-V7I1P120

Original Article

Deep Learning-Based Threat Intelligence Framework for Proactive Cyberattack Detection and Mitigation

Ashay Mohile
Technical Program Manager, Infrastructure Security, IEEE senior Member.

Received On: 31/12/2025 ***Revised On: 02/02/2026*** ***Accepted On: 09/02/2026*** ***Published On: 13/02/2026***

Abstract - *The use of cybersecurity threat detection systems that were previously effective is becoming a thing of the past as a result of the spread and complexity of cyberattacks. This study suggests the CNN-LSTM architecture and the CIC-IDS2017 dataset as the foundation of the hybrid deep learning threat detection model. The extensive data pretreatment that is practiced by the offered technique to address the problem of severe imbalance between classes is covered by data cleaning, feature extraction, normalization, label encoding, and class balancing based on the Synthetic Minority Over-sampling Technique (SMOTE). After the 80: 20 split of the processed data into training and testing samples, the performance of the model is evaluated on standard indicators, such as as accuracy (ACC) and precision (PRE) and recall (REC), F1-score (F1) and ROC-AUC. With a 99.6% ACC rate, 97.5% PRE, 97.0% REC, 98.0% F1, and 0.99% ROC-AUC, the suggested CNN-LSTM model outperforms the state-of-the-art. The hybrid architecture has been effectively compared to other models due to its flexibility to large as well as real-time network intrusion detection systems.*

Keywords - *Deep Learning, Threat Detection, Cybersecurity, CNN-LSTM, Smote.*

1. Introduction

Digital infrastructure has made life easier, however it has also shown many inadequacies. Malevolent actors and nation-state actors as well as cybercriminals have shifted their interest to the critical infrastructure, such as energy, transportation, healthcare, banking, and government. The attack surface has expanded significantly with the rapid technology advancement with the help of the IoT and cloud computing [1][2]. In this study, Explore how behavioural analytics can transform cyber threat intelligence (CTI), into a preventative defensive [3][4]. The cybersecurity environment is dynamic and thus it associates significantly with the nature and intensity of threats that are suffered by organizations. With the growth of the digital space and its interconnection, cyber threats have evolved into sophisticated forms, and their impact on classic reactive strategies is not enough [5][6]. Conventional methods of network security, though indispensable, are not withstanding the emergent and new threats. This is where the specialization in the direction of preventing security measures rather than reactive measures is relevant to prevent the occurrence of risks before they can develop into serious threats [7]. The new direction of the research is to improve network security through machine learning-based threat intelligence[8]. This is aimed at identifying suspicious activity pattern that may be harbingers of cyber threats before turning into attacks[9].

The spread of cyber threats has led to the creation of game changing technologies such as AI and ML that can be used to complement traditional security with proactive threat intelligence, predictive analytics, and automated response systems [10]. This is because AI driven cybersecurity solutions provide a paradigm shift in terms of combating cyber threats by organisations by relying on adaptive learning, pattern recognition, and real time data analysis[11][12]. Finding new threats, such as a zero-day vulnerability that regular signature-based security systems cannot detect, is done through behavioural analysis and anomaly detection by artificial intelligence (AI)[13].

The AI application in cybersecurity is not confined to the detection and prevention of threats. Utilising NLP, cutting-edge AI-powered solutions examine threat intelligence reports, identify harmful messages, and detect phishing attempts [14][15][16]. By automatically detecting suspicious activity and responding to potential dangers before they may cause damage, deep learning systems improve network security. Biometric authentication, fraud detection, and risk assessment are a few other ways AI can be utilised to strengthen security measures in many areas.

1.1. Significance of the Study

This work is important as it helps to improve the network intrusion detection by overcoming the complexity and disbalance of the real traffic on the network. The suggested framework outperforms other threat detection methods based on a hybrid CNNLSTM design that is capable of identifying the spatial and temporal features of network flows in a single network thereby yielding high-ACC and dependable threat detection. The minority attack detection is greatly enhanced by the use of massive data preprocessing and class balancing using SMOTE, and the number of false negatives is minimized, which is a severe security risk. The high ACC and ROC-AUC have proven the practicality of the model as a system used to detect intrusions in real-time and at scale hence it is a useful contribution to enhancing the resilience of

current cybersecurity infrastructures against more advanced forms of cyber threats.

1.2. Contributions of this study

This research has made the following key contributions:

- The CIC-IDS2017 data is heavily preprocessed, with data cleaning, feature extraction, normalization, label encoding.
- The model enhances detecting ACC by merging spatial features learnt by CNN with temporal dependencies learnt by LSTM.
- Improved the model's capacity to learn minority attack patterns by using SMOTE to rectify the imbalance between attack and normal traffic classes.
- PRE, ACC, REC, F1, and ROC-AUC were the usual performance metrics used to conduct the experimental evaluation.

1.3. Justification and Novelty of Paper

The proposed approach is supported because there is a requirement for more accurate and efficient intrusion detection systems that can handle the complex and highly unbalanced data that is connected with network traffic. The geographical and temporal properties of network flows are often not embodied by conventional ML and individual deep learning models, leading to an increase in false alarms and missed attacks. What makes this work novel is that CNN models with LSTM models are effectively used with thorough data preprocessing and class balancing based on SMOTE using a large dataset of CIC-IDS2017 to learn both local and long-term correlations. The hybrid architecture leads to better detection capability and generalization which make it a powerful and viable solution to the current network security environment.

1.4. Organization of the Paper

The paper structure is as follows: Section II reviews related work on threat detection systems. Section III details the data, data preprocessing process and the proposed structure. Findings of the experiments, performance comparisons, drawbacks, and future plans are all outlined in Section IV. Section V finally concludes the study.

2. Literature Review

In this section, the authors note current advances in intrusion detection with the help of ML with reference to the following approaches: oversampling, stacked feature embedding, and feature extraction to handle large, imbalanced datasets, enhance the overall work of the system, reduce false alarms, and improve detection efficiency. Among the latest and most influential works in this field are:

Alkharabsheh et al. (2025) brings a new AI-focused cybersecurity system, shifting the defense strategy to the proactive mode. The system identify, classify, and estimate cyber threats in real time based on models such as LR, RF and custom risk score models. This system was simulated using Scikitlearn and TensorFlow and worked well in various evaluation measures: ACC 91.011 percent, PRE 92.1 percent and F1 90.9 percent. [17].

Seetharaman and Yadav (2025) This research introduces machine learning based approach to identifying and mitigating cyber threats in IoT scenarios with the focus on categorizing cyberattacks with the help of the ResNet model. In a comparison of the framework based on the CICDS 2019 data, ResNet model results in a 99.5% ACC and a 93.3% AUC, which are higher than more traditional machine learning models such as FFNN, SVM, and GRU[18].

Dorothy et al. (2024) offers an artificial intelligence initiative to address the flaws of existing systems, including non-dynamic rule-based frameworks. The combination of AD and ML methods provides system adaptability to the emerging security threats. The threat detection (95% ACC) and anomaly detection (93% ACC) performance metrics of the system are highly boosted due to the real-time monitoring and reaction. The proposed method is better as it has an improvement over the existing method of 95% ACC, 93% PRE, and 96% REC[19].

Vadisetty and Polamarasetti (2024) proposes a very modern experience of preprocessing data prior to applying a DNN to detect network intrusion in a live environment, as well as an in-depth evaluation of the traditional machine learning models. The proposed DNN model helped a lot in enhancing detection abilities with an AUC of 1.00, ACC of 99.50, and the least misclassification rate among all the evaluation parameters[20].

Sridevi et al. (2023) suggest a mixed-model approach that draws from both deep neural networks—which excel at capturing nuanced behavior—and feature-engineered patterns—which can reveal unusual insider activities. In order to detect unusual insider actions, this model would be employed. At 96.3%, model was very accurate in its detection [21].

Malik and Singh Saini (2023) propose the use of Adversarial/Multi Agent Reinforcement Learning in conjunction with Deep Q Learning (AE-DQN). Evaluate recommendations on two datasets: NSL-KDD and KDDTest+. The difficulty of reducing an infinite number of possibilities to a manageable five groups is the subject of this essay. As a whole, approach achieved an F1 of 79% and an ACC rate of 80% [22].

Table I presents a comparative overview of recent studies on threat detection using machine and deep learning approaches for large and imbalanced datasets, detailing methodologies, datasets, performance metrics, and limitations to highlight research gaps and future directions.

Research gap: There are still many cybersecurity knowledge gaps, despite the fact that current research shows that deep learning and machine learning substantially improve intrusion detection and cybersecurity. Works that are currently available either make use of the conventional machine learning models or individual deep learning models that restrict their capability to jointly obtain spatial and temporal properties of network traffic. Although certain

methods are very accurate, they value specific datasets (e.g., CICIDS2019, NSL-KDD) or specific settings (e.g., IoT) lowering their generalizability. Also, such issues as excessive class imbalance, false negative minority attack classes, and the lack of evaluation of hybrid deep learning models are not thoroughly discussed. Not many studies combine thorough preprocessing, class balancing, and an all-encompassing CNNLSTM model on the CIC-IDS2017 data.

Table 1: Comparative Analysis of AI-Driven Cybersecurity Research with Future Work Directions

Author(s) & Year	Focus Area	Models	Dataset	Key Performance Results	Future Work
Alkharabsheh et al. (2025)	Proactive AI-based cybersecurity threat detection and forecasting	Logistic Regression, Random Forest, Custom Risk Scoring Functions	Scikit-learn, TensorFlow	Accuracy > 91%, Precision 92.1%, F1-score 90.9%	Extend the framework to incorporate deep learning and reinforcement learning models for adaptive threat mitigation and deployment in large-scale real-world environments.
Seetharaman & Yadav (2025)	Cyberattack classification in IoT environments	ResNet (Deep Learning), FFNN, SVM, GRU	CICIDS 2019	Accuracy 99.5%, AUC 93.3%	Discover deep learning models that are both energy-efficient and lightweight, making them ideal for deployment at the edge in real-time and Internet of Things devices with limited resources.
Dorothy et al. (2024)	Adaptive AI-driven cybersecurity using anomaly detection	Anomaly Detection + Machine Learning	Real-time Monitoring Framework	Accuracy 95%, Precision 93%, Recall 96%	Incorporate XAI approaches to enhance the dependability and transparency of anomaly detection conclusions.
Vadisetty & Polamarasetti (2024)	Real-time network intrusion detection	Traditional ML Models, DNN	Network Intrusion Datasets	Accuracy 99.5%, AUC 1.00, Lowest misclassification rate	Investigate hybrid deep learning architectures and online learning mechanisms to handle evolving attack patterns.
Sridevi et al. (2023)	Insider threat and anomalous behavior detection	Hybrid Deep Neural Networks with Feature Engineering	Insider Threat Datasets	Detection Accuracy 96.3%	Extend the model to multi-domain insider threat detection and incorporate temporal behavior modeling for early threat prediction.
Malik & Singh Saini (2023)	Adversarial network detection with reinforcement learning	Artificial Enemy-Demon Q-Network, AE-DQN	NSL-KDD, KDDTest+	Accuracy 80%, F1-score 79%	Improve classification performance by integrating deep ensemble learning and expanding the approach to modern intrusion datasets.

3. Methodology

The threat detection approach that proposed, based on the CIC-IDS 2017 dataset, starts with the extensive data preprocessing, includes data cleaning to eliminate noise and inconsistency, feature extraction to determine the relevant traffic characteristics, and normalization to scale features to equal levels. Label encoding and SMOTE is used to reduce the class imbalance and enhance the number of minority attack classes. The processed data is then divided to training (80%), and testing (20%). The training data is processed using a hybrid CNNLSTM model whereby the CNN model is used to extract spatial information about network traffic and the LSTM is used to learn temporal relationships to achieve a higher detection ACC. Lastly, the ACC, PRE, REC, and F1 are assessed on the test data and the results are utilized to categorize the network traffic as an attack or normal one. Fig. 1 shows the flowchart of this methodology.

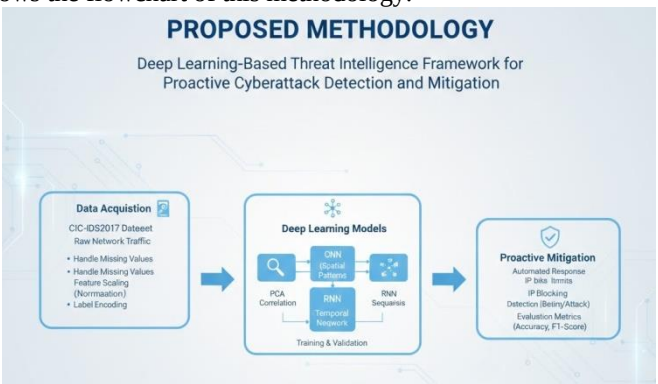

Fig 1 : Proposed Methodology For Threat Detection Using CIC-IDS2017 Data

3.1. Data Collection

The CICIDS2017 dataset, which includes entire packet payloads and categorised network inputs, was used for the tests. Eight separate files containing attack traffic data and five regular days of Canadian Institute of Cybersecurity data made up the CICIDS2017 dataset.

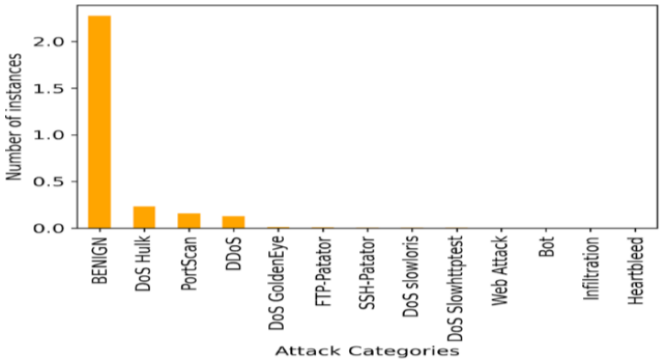

Fig 2 : CICIDS2017 Dataset Distribution By Attack Category

Fig 2 indicates that BENIGN traffic has the highest number of two million instances in the dataset. The categories of the attacks include DoS Hulk, PortScan, and DDoS each with several hundred thousand samples. On the contrary, such attacks as DoS GoldenEye, FTP-Patator and Web Attacks are represented in significantly lower numbers, showing a high-class imbalance towards benign traffic.

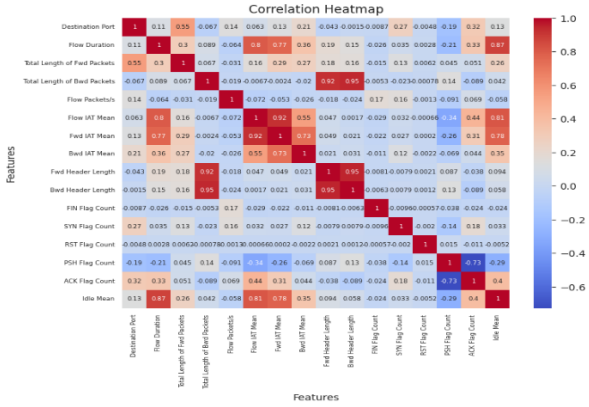

Fig 3 : Correlation Heatmap Of CICIDS2017 Dataset

The heatmap in Fig 3 offers the correlation between the network traffic characteristic in the CICIDS2017 dataset. The color range is between blue (negative correlation) and red (positive correlation) which show patterns and dependencies of features. Attributes like the flow duration, the length of packet and the number of flags are strongly correlated and assist in guiding the selection of features that are used to model intrusion detection effectively.

3.2. Data Preprocessing

Data collected from the real world is often imperfect, noisy, and missing or duplicated values. An essential part of machine learning is the data preprocessing phase. This step is essential for cleaning and preparing the initial data set for the ML model. It is a process, which is used to apply methods to the original dataset, aiming at simplifying it, removing characteristics, which do not matter, are incorrect, or otherwise unnecessary.

- Data cleaning: These records were eliminated in the further processing; the missing values were addressed through imputation techniques; and the outliers were addressed with the help of IQR approach.
- Feature extraction: Converted raw data into useful features by examining network statistics, system logs using n-gram analysis, and malware samples for behavioral characteristics.
- Data normalization: Addressed the issue of min-max scaling by standardizing numerical data types so that they can be scaled together. Equation (1) is used to derive it:

$$\times = \frac{X - x_{min}}{x_{max} - x_{min}}$$

3.3. Label Encoding

The process of label encoding [23] can be used with the model of ML to use numeric values based on the categorical class labels. As the algorithms used to learn are numerically-based, categorical labels have to be encoded into integers when training. Label encoding is a technique in which a unique class is represented by an integer between 0 and n-1 in which n is the number of unique classes. As an illustration, in case the data has 11 classes, they are coded with the help of integer numbers 0-10.

3.4. Class Balancing using SMOTE

The imbalance in the training data is corrected by the SMOTE [24]. To make the distribution of classes more fair, SMOTE generates synthetic samples by extending the existing examples of under-represented ones rather than random oversampling. Given its ability to enhance model learning while decreasing the risk of overfitting due to simple duplication, this method shines when used to datasets that are extremely imbalanced.

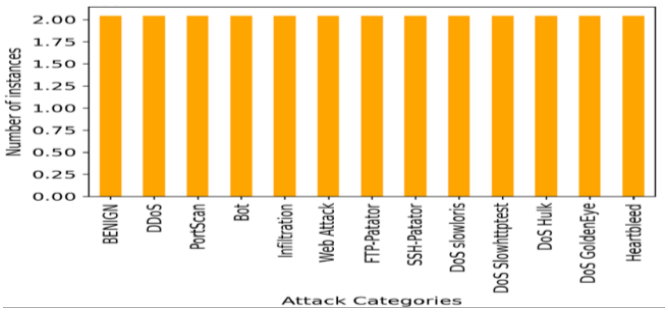

Fig 4 : Balanced Distribution Of Dataset By Attack Category

As shown in Fig 4, all attack categories, including BENIGN, DDoS, PortScan, and DoS Hulk, exhibit nearly equal numbers of instances, each approaching two million. This balanced distribution indicates the effectiveness of SMOTE in mitigating class imbalance and supporting robust model training.

3.5. Data Splitting

There is an 80:20 split between the pre-processed dataset's training and testing sets.

3.6. Proposed CNN-LSTM Model

The data is also transformed such that the 1D convolutional layer can use it as input. There are 64 neurones in a convolutional layer with a 10-neuron kernel [25][26]. Three hidden layers, a convolutional layer with thirty-two input values, and a dense layer with seven layers make up the CNN+LSTM model. The dense layer uses Relu as its activation function and takes 78 input values, which represent the dataset's features. The feature extraction and feature discarding processes are carried out by means of a Maxpool layer and can feed 64 values into the LSTM layer. The use of a dropout layer, which removes nodes at random intervals (every weight update cycle with a chance of 20%), helps to avoid overfitting. A thick coating appears at last. Incorporated all of the hidden layers by using the Relu activation function. The final step of the output layer is to use the sigmoid activation function.

3.7. Performance Metrics

The model made use of four popular confusion-matrix-based metrics for evaluating information retrieval: the ratio of correctly categorised attack flows (TP) to all classified flows (TP+CF) and the PRE value (Pr), often called the positive predictive value (PPV) [27][28]. The number of correctly categorised attack flows (TP) divided by the total number of flows created for all tests (TP+FN) is called REC (Rc). A mixture of the Pr and Rc, the F-measure (F1) combines the two into a single metric. Using (2-6) one can determine the ACC, also known as the percentage of correct classification (ACC):

$$Precision(Pr) = \frac{TP}{TP + CF}$$

$$Recall(Rc) = \frac{TP}{TP + FN}$$

$$F1 = \frac{2}{\frac{1}{Pr} + \frac{1}{Rc}}$$

$$ACC = \frac{TP + TN}{TP + FP + FN + TN}$$

The variables TP, TN, FP, and FN stand for various counts: TP for regularly classified instances, TN for intrusions, FP for normal intrusions, and FN for attacks on normally classified cases.

4. Result Analysis and Discussion

The studies were carried out in a state-of-the-art computing environment using a 2X-large virtual machine that had 64 GB of RAM, 40 GB of disc space, and 8 CPU cores. The development and experimentation were carried out using Jupyter Notebook accessed through Anaconda Navigator. The implementation was developed in Python, leveraging widely used libraries including TensorFlow, Keras, Scikit-learn, Pandas, NumPy, Seaborn, and Matplotlib. The suggested CNN-LSTM model had a ROC-AUC score of 0.99, a REC of 97.5%, a PRE of 97.0%, and an F1 of 98.0%, as shown in Table II. A whopping 99.6% adhered. These results demonstrate that the Hybrid model successfully distinguishes between malicious and benign network traffic while maintaining a balanced detection sensitivity and false-alarm rates.

Table 2 : Evaluation Of CNN-LSTM Model For Threat Detection On CICIDS-2017 Dataset

Metrics	CNN-LSTM
Accuracy	99.6
Precision	97.5
Recall	97
F1-score	98
ROC-AUC	0.99

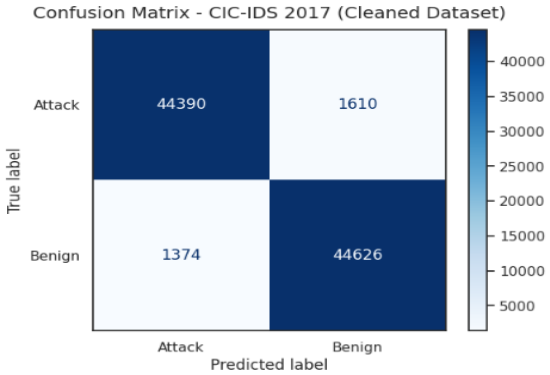

Fig 5: Confusion Matrix Of CNN-LSTM Model For Network Intrusion Detection

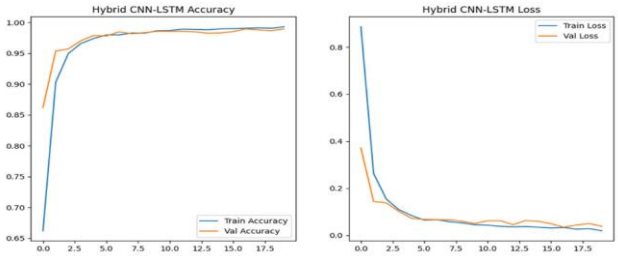

Fig 6 : Accuracy And Loss Curve Graph Of CNN-LSTM Model

Fig 5 shows the confusion matrix of CNN-LSTM model when the model is tested on the cleaned CIC-IDS 2017 dataset to detect network intrusion. The model had a high detection rate of both the attack and benign classes, with 44,390 and 44,626 attack and benign respectively being correctly classified as either an attack or a benign attack. Nevertheless, the number of attack samples that were incorrectly labeled as benign (false negatives) was 1,610, which is vital in terms of security because they are the untreated attacks. Also, 1,374 benign cases were wrongly identified as attacks (FP), which could result in unnecessary alerts.

The training and validation ACC and loss curves shown in Fig 6 show that the hybrid CNN-LSTM model's ACC goes up quickly at first but then levels off as the number of epochs goes up. Both the training and validation ACC are close to 99, which proves that the model learns very well and also works

well in other situations. At the same time, the loss curves are sharp in the beginning and slightly stabilize at very low losses with little difference between training and validation losses, indicating that the optimization is efficient and is not overfitting.

4.1. Comparative Analysis

This section Table III provides a comparative performance evaluation of the available threat detection models in dissimilar benchmark data sets. The LSTM model when tested on the CICIDS2017 dataset is able to achieve a high ACC of 97.67 showing its ability to capture temporal based attack patterns, but the CNN model on the CICIDS 2020 dataset achieves a relatively lower ACC of 88.6 showing its failure to generalize to complex traffic patterns. Based on the results of the testing of the ANN model on the KDD-CUP 99 data, the ACC of 93.99 and comparatively lower values of PRE, REC, and the F1 are indicative of the difficulties in the correct identification of the attack and benign traffic. On the contrary, the suggested hybrid CNN-LSTM model is much more effective with the highest ACC of 99.6 and the best PRE (97.5), REC (97.0), and F1 (98.0) and thus the power and efficiency of the model in threat detection by considering both spatial and temporal features learning.

Table 3 : Performance Comparison of Existing Models For Threat Detection

Model	Accuracy	Precision	Recall	F1- Score
CICIDS2017				
LSTM[29]	97.67	94.96	95	93.55
CICIDS 2020				
CNN[30]	88.6	86.7	89.2	87.9
KDD-CUP 99				
ANN[31]	93.99	81.99	81.99	81.99
Proposed				
CNN-LSTM	99.6	97.5	97.0	98.0

CNNs are good at extracting spatial characteristics, while LSTM networks are good at learning temporal sequences; together, they form a hybrid model that should provide better threat identification. The model manages to detect much better and minimize false positives and false negativity because it successfully captures local traffic trends and long-term dependencies in the network data. It has a higher ACC, PRE, REC and F1 indicating a higher generalization, convergence speed and reliability than the traditional single-model solution, which is why it is a well-suited solution to real-time and large-scale IDS.

4.2. Limitations and Future Work

Although the suggested CNN-LSTM-based threat detection framework performs rather well, some limitations can still be identified. The model was trained and tested only on the CIC-IDS2017 dataset, which, despite its exhaustiveness, does not necessarily reflect the changing real-world network traffic patterns and zero-day attack cases, which might constitute a limitation to the generalization. Moreover, the model proposed has high computational demands during the training phase due to which it might not be able to be deployed on resource-limited or edge-based systems. The next steps in work include the validation of the framework on various and more recent intrusion detection datasets, and real-time traffic streams to increase the resilience and flexibility. The inclusion of online or incremental learning methods may allow dynamism in model changes to new threats. Moreover, the XAI techniques would enhance the model transparency and credibility, whereas the model optimization and lightweight models would support the efficient implementation in real-time and large-scale network security systems.

5. Conclusion

The use of AI in cybersecurity threat detection opens up new avenues for enhancing detection efficiency and ACC.This paper proposed a successful hybrid CNNLSTM-based network intrusion threat detection model utilizing the CIC-IDS2017 dataset to ensure the ever-increasing intrusion complexity of networks. The proposed approach provided high-quality and balanced input data to train the model since it involved a lot of data preprocessing, such as data cleaning, feature extraction, normalization, label encoding, and SMOTE-based class balancing. With a 99.6% success rate, good PRE and REC, an F1, and a ROC-AUC of 0.99, the suggested CNNLSTM model outperformed conventional models in the experiments. The training. validation curves and the confusion matrix also enabled the affirmation of the robustness of the model, high capabilities of generalizations, and low risks of overfitting. All in all, the suggested model is a stable and scalable model in detecting intrusions in real-time and in large scopes and provides a better security to the current networks.

References

[1] M. Ashraf, R. Paudel, and B. Maskey, “Advanced Cybersecurity Strategies Leveraging Neural Networks for Protecting Critical Infrastructure against Evolving Digital Threats through Proactive Risk Management and Threat Intelligence,” *ICCK Trans. Neural Comput.*, vol. 1, no. 1, 2024, doi: 10.62762/TNC.2025.737491.

[2] Henry Cyril, “Ai-Driven Anomaly Detection , Outage Prediction , And Self- Healing In Telecom Provisioning Systems,” *Int. J. Appl. Math.*, vol. 38, no. 12s, pp. 2817–2832, Dec. 2025, doi: 10.12732/ijam.v38i12s.1589.

[3] S. Narang and A. Gogineni, “Zero-Trust Security in Intrusion Detection Networks: An AI-Powered Threat Detection in Cloud Environment,” *Int. J. Sci. Res. Mod. Technol.*, vol. 4, no. 5, pp. 60–70, Jun. 2025, doi: 10.38124/ijsrmt.v4i5.542.

[4] V. Shah, “Traffic Intelligence In Iot And Cloud Networks: Tools For Monitoring, Security, And Optimization,” *Int. J. Recent Technol. Sci. Manag.*, vol. 9, no. 5, 2024, doi: 10.10206/IJRTSM.2025894735.

[5] Md Abubokor Siam *et al.*, “AI-Driven Cyber Threat Intelligence Systems: A National Framework for Proactive Defense Against Evolving Digital Warfare,” *Int. J. Comput. Exp. Sci. Eng.*, vol. 11, no. 3, pp. 6126–6140, 2025, doi: 10.22399/ijcesen.3793.

[6] L. Ogbidi and B. Oteh, “Advances in Hybrid Machine Learning and Physics-Based Models for Enhanced Reservoir Simulation,” *Int. J. Sci. Res. Comput. Sci.*

Eng. Inf. Technol., vol. 10, no. 6, pp. 2533–2543, Dec. 2024, doi: 10.32628/IJSRCSEIT.

[7] H. Kapadia and K. C. Chittoor, "Quantum Computing Threats to Web Encryption in Banking," *Int. J. Nov. Trends Innov.*, vol. 2, no. 12, pp. a197–a204, 2024.

[8] M. Barbhaya, P. R. Dasari, S. K. Damarla, R. Srinivasan, and B. Huang, "A deep learning framework for cyberattack detection and classification in Industrial Control Systems," *Comput. Chem. Eng.*, vol. 202, p. 109278, Nov. 2025, doi: 10.1016/j.compchemeng.2025.109278.

[9] P. Nutalapati, J. R. Vummadi, S. Dodda, and N. Kamuni, "Advancing Network Intrusion Detection: A Comparative Study of Clustering and Classification on NSL-KDD Data," in *2025 International Conference on Data Science and Its Applications (ICoDSA)*, IEEE, Jul. 2025, pp. 880–885. doi: 10.1109/ICoDSA67155.2025.11157595.

[10] S. Chatterjee, "Risk Management in Advanced Persistent Threats (APTs) for Critical Infrastructure in the Utility Industry," *Int. J. Multidiscip. Res.*, vol. 3, no. 4, Aug. 2021, doi: 10.36948/ijfmr.2021.v03i04.34396.

[11] R. Muppalaneni, A. C. Inaganti, and N. Ravichandran, "AI-Driven Threat Intelligence: Enhancing Cyber Defense with Machine Learning," *J. Comput. Innov. Appl.*, vol. 2, no. 1, pp. 1–11, 2024, doi: 10.63575/.

[12] V. Shewale, "Beyond EDR: Exploring the rise of XDR for unified threat detection and response," *World J. Adv. Eng. Technol. Sci.*, vol. 15, no. 2, pp. 380–386, May 2025, doi: 10.30574/wjaets.2025.15.2.0551.

[13] A. R. Bilipelli, "AI-Driven Intrusion Detection Systems for Large- Scale Cybersecurity Networks Data Analysis : A Comparative Study," *TIJER – Int. Res. J.*, vol. 11, no. 12, pp. 922–928, 2024.

[14] A. Zedan and N. H. El-Farra, "A machine-learning approach for identification and mitigation of cyberattacks in networked process control systems," *Chem. Eng. Res. Des.*, 2021, doi: 10.1016/j.cherd.2021.09.016.

[15] S. Kumara, "AI-Driven Threat Identification and Response: Implications for Secure and Scalable Telecom Infrastructure," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 4, p. 559, Dec. 2025, doi: 10.48175/IJARSCT-30567.

[16] S. Thangavel, "AI Enhanced Image Processing System For Cyber Security Threat Analysis," 2024.

[17] A. R. Alkharabsheh, F. H. Alhosani, M. H. Alameri, A. B. Alrashdi, F. M. Almenhali, and A. A. Alzaabi, "AI-Driven Proactive Framework for Cybersecurity Threat Prediction, Detection, and Attack Classification," in *2025 International Conference on Computer Science, Technology and Engineering (ICCSTE)*, IEEE, Jun. 2025, pp. 12–17. doi: 10.1109/ICCSTE65902.2025.11138235.

[18] K. M. R. Seetharaman and P. Yadav, "A Machine Learning Framework for Detecting and Mitigation of Cyber Threats in IoT Environments," in *2025 3rd International Conference on Inventive Computing and Informatics (ICICI)*, IEEE, Jun. 2025, pp. 1112–1119. doi: 10.1109/ICICI65870.2025.11069697.

[19] A. B. Dorothy, B. Madhavidevi, B. Nachiappan, G. Manikandan, P. K. Patjoshi, and M. Sindhuja, "AI-Driven Threat Intelligence in Cloud Computing Detecting and Responding to Cyber Attacks," in *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)*, IEEE, Aug. 2024, pp. 1–6. doi: 10.1109/IACIS61494.2024.10721888.

[20] R. Vadisetty and A. Polamarasetti, "Enhancing Intrusion Detection Systems with Deep Learning and Machine Learning Algorithms for Real-Time Threat Classification," in *2024 Asian Conference on Intelligent Technologies (ACOIT)*, IEEE, Sep. 2024, pp. 1–6. doi: 10.1109/ACOIT62457.2024.10939322.

[21] D. Sridevi, L. Kannagi, G. Vivekanandan, and S. Revathi, "Detecting Insider Threats in Cybersecurity Using Machine Learning and Deep Learning Techniques," in *2023 International Conference on Communication, Security and Artificial Intelligence, ICCSAI 2023*, 2023. doi: 10.1109/ICCSAI59793.2023.10421133.

[22] M. Malik and K. Singh Saini, "Network Intrusion Detection System using Reinforcement learning," in *2023 4th International Conference for Emerging Technology (INCET)*, 2023, pp. 1–4. doi: 10.1109/INCET57972.2023.10170630.

[23] S. Amrale, "Anomaly Identification in Real-Time for Predictive Analytics in IoT Sensor Networks using Deep," *Int. J. Curr. Eng. Technol.*, vol. 14, no. 6, pp. 526–532, 2024, doi: 10.14741/ijcet/v.14.6.15.

[24] G. Sarraf, "Behavioral Analytics for Continuous Insider Threat Detection in Zero-Trust Architectures," *Int. J. Res. Anal. Rev.*, vol. 8, no. 4, pp. 596–602, 2021.

[25] O. Elnakib, E. Shaaban, M. Mahmoud, and K. Emara, "EIDM: deep learning model for IoT intrusion detection systems," *J. Supercomput.*, vol. 79, no. 12, pp. 13241–13261, Aug. 2023, doi: 10.1007/s11227-023-05197-0.

[26] V. Prajapati, "Enhancing Threat Intelligence and Cyber Defense through Big Data Analytics: A Review Study," *J. Glob. Res. Math. Arch.*, vol. 12, no. 4, 2025.

[27] A. S. Jaradat, M. M. Barhoush, and R. B. Easa, "Network intrusion detection system: Machine learning approach," *Indones. J. Electr. Eng. Comput. Sci.*, 2022, doi: 10.11591/ijeecs.v25.i2.pp1151-1158.

[28] N. K. Prajapati, "Federated Learning for Privacy-Preserving Cybersecurity: A Review on Secure Threat Detection," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 4, pp. 520–528, Apr. 2025, doi: 10.48175/IJARSCT-25168.

[29] J. Jose and D. V. Jose, "Deep learning algorithms for intrusion detection systems in internet of things using CIC-IDS 2017 dataset," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 1, p. 1134, Feb. 2023, doi: 10.11591/ijece.v13i1.pp1134-1141.

[30] K. N. I. Ara, T. Mithila, M. M. A. Rony, and I. Sarkar, "Engineering of AI-Powered Cyber Defense Tools to Protect Immigration Databases, Biometric Identity Systems, and Border-Control Infrastructure from Nation-State Attacks," *J. Comput. Sci. Inf. Technol.*, vol. 2, no. 2, pp. 47–58, Nov. 2025, doi:

10.61424/jcsit.v2i2.573.
[31] N. Omer, A. Samak, A. I. Taloba, and R. M. A. El-Aziz, "Cybersecurity Threats Detection Using Optimized Machine Learning Frameworks," *Comput. Syst. Sci. Eng.*, vol. 48, no. 1, pp. 77–95, 2024, doi: 10.32604/csse.2023.039265.