International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

An Intelligent Unified Framework for Network Security in Threat Identification using Deep Learning Methods

Dr. Manish Jain*

Associate Professor, Department of Electronics and Communications, Mandsaur University, Mandsaur (M.P.), India

Received 01 Dec 2025, Accepted 20 Dec 2025, Available online 21 Dec 2025, **Vol.15, No.6 (Nov/Dec 2025)**

Abstract

An integrated threat analysis and mitigation system that enhances network security with the help of deep learning. Policies, technology and monitoring systems are important in the protection of infrastructures against dynamic threats. The detection and mitigation systems of cyber threats (particularly botnets) are becoming increasingly more complex and require intelligent and adaptable systems that are capable of detecting and mitigating them in real-time. The presented paper presents a deep learning network that integrates the use of SMOTE data balancing, GA feature optimization, and RNN trained on the CTU-13 dataset. The proposed RNN outperformed the traditional counterparts in terms of sequential traffic patterns that are critical to intrusion detection with a high accuracy (ACC) of 99.25, precision (PRE) of 98.30, recall (REC) of 99.25, and F1-score (F1) of 98.75. Studies revealed that RNN performed better than the baseline models, e.g. Hidden Markov Model (HMM) (94.80% accuracy), Convolutional Neural Network (CNN) (97.21% accuracy), and Support Vector Machine (SVM) (92% accuracy). The fact that the RNN could model temporal dependencies minimized misclassifications, and the network was also more resilient. The above results indicate the promise of RNNs in future-generation cybersecurity, which provides scalable, proactive threat detection in dynamic networks, including network descriptions facilitated by clouds and supported by IoT, which is essential to ensure the security of critical systems.

Keywords: *Network Security, Deep Learning, Recurrent Neural Network (RNN), Botnet Detection, CTU-13 Dataset, Machine learning.*

1. Introduction

Cybersecurity is a critical component of the modern digitized world that protects confidential data, valuable infrastructures, and company resources against bad actors [1]. The capacity of interconnected devices, cloud computing and Internet of Things is rising at an exponential rate exposing the digital attack surface and making it susceptible to attacks by malicious forces [2]. Traditional security systems despite their efficiency over a short period of time cannot be effective in dealing with more dynamic, intelligent and dynamic cyber threats that grow by leaps and bounds in scale and intensity [3].

The threat landscapes are necessary to protect the digital infrastructures [4][5]. Threat analysis can be used to identify, classify, and analyze a number of malicious acts. These are sophisticated persistent threats, phishing, malware distribution, distributed denial of service (DDoS) attacks and spyware [6][7][8]. However, the heterogenization of network environments (they are becoming heterogeneous) and the complexity of attack methods of aggressors are a challenge to the conventional intrusion detection platforms (IDS) [9].

*Corresponding author's ORCID ID: 0000-0000-0000-0000
DOI: https://doi.org/10.14741/ijcet/v.15.6.5

False alarm rates cripple the functioning of such systems, low latency and set an extremely low threshold of being able to extrapolate to new attacks that the system has no previous experience with [10][11][12]. This raises to mind the spectacular necessity to come up with adaptive and scale-up capabilities which can monitor the situation in real-time and be pro-anticipatory on the defensive [13].

Risk assessment is not enough without proper countermeasures that could reduce the effects of attacks. Defense on the network should go beyond detection to encompass fast reaction systems to contain infected network elements and halt horizontal mobility of attacks and to restore system equilibrium [14], [15]. This can be quite complex to develop due to centralized issues of scaling, computation, and due to heterogeneity of data traffic that exists in IOST-enabled/Cloud-driven environments [16][17][18]. To achieve cyberattack resilience, the combined use of detection, prediction, and mitigation is to be brought into one framework to further enhance defence and post-attack recovery measures.

Machine learning systems to detect threats take advanced approaches to identifying potential threats such as anomaly detection, behavioural analysis, and

predictive modelling to recognize potential threats before they evolve into actual problems [19][20]. The ML and DL algorithms have been employed to detect abnormalities in networks, intrusion and prevention, automated feature extraction, anomaly detection and predictive modelling [21][22][23]. In contrast to traditional ML methods, network flows taught by CNNs, RNNs, or blends of the two can learn intricate patterns with time-varying dependencies. Such features make it more accurate, minimize false alarms and help to initiate counteracting measures in advance [24][25][26]. By embedding the analysis of threats provided by DL into intelligent mitigation combinators it is feasible to create a holistic platform that provides scalable, dynamic, and real-time network security.

Motivation with contribution

Cyber dangers, especially botnets, which can bypass conventional security measures, are becoming more sophisticated and common, which is why this study is necessary. The rapid expansion of networked technology and the IOT has created an immediate demand for intelligent, automated systems that can identify and avert dangerous acts in real-time. To develop a threat detection system that is more precise, dynamic, and scalable, must resort to the methods of ML and DL since the conventional signature-based detection approach is not always capable of identifying new or evolving threats. The project results in improved cybersecurity frameworks through the more effective utilization of the CTU-13 dataset and the enhancement of model inputs. The area of Network Security Improvement is one of the areas where the current study contributes greatly in several critical aspects:

- Applied the CTU-13 data, a popular standard in botnet detection; it is a collection of labelled network traffic in thirteen real botnet cases.
- Applied a full data pre-processing process such as missing data treatment, outlier treatment, min-max normalization as well as class balancing with the SMOTE tool to enhance data quality and model ACC.
- Reduced dimensionality and improved model efficiency with the use of GA to choose the most relevant features, all while maintaining ACC.
- Presented a solid approach that integrates data pre-processing, feature optimization, and DL to facilitate the immediate and precise identification and elimination of network threats.
- Developed and deployed a specialized RNN model, capitalizing on its ability to detect patterns in network data that vary over time.
- REC, ROC, F1, and PRE were among the ACC metrics used to conduct a thorough evaluation of the model's performance.
- Scalability and Adaptability the pipeline to support IoT and cloud, ensuring applicability to evolving digital ecosystems.

A. Justification and Novelity

This study is justified by the fact that there is a great urgency in intelligence and adaptive approach to detecting threats that can put up with the changing face of cyber-attacks, especially those that are brought about by botnets. Traditional detection systems have a low capability of detecting a new and enhanced threat since they rely on the existing and unchanging fingerprints. To contribute to the development of the innovative approach, the given research combines an optimized pre-processing pipeline with the advanced feature selection based on the use of the Genetic Algorithm (GA) and a RNN model that is perfectly adapted to process sequential network traffic patterns. Indeed, the combination of GA-inspired feature selection and temporal learning of RNNs, when used on the CTU-13 dataset, a control ground not often studied with such a methodological integration, underlines the novelty of the work. It could be described as a scalable and efficient way of real-time network threat mitigation. This approach enhances the detection ACC and model efficiency.

B. Structure of paper

The outline of the paper is as follows: Section II is the literature review of the topic of network security, Section III is the description of the approach which was followed in each of the stages of system designing, Section IV is the comparison and evaluation of the results of the proposed models, and Section V is the conclusion of this work and the discussion of the possible directions of future research.

2. Literature Review

The literature overview on DL and AI approaches to efficient and accurate threat detection in network security settings is covered in this section. A synopsis of the evaluated research and its effects on improving intrusion detection and mitigation is presented in Table I.

Numpradit, Boonyopakorn and Charoensawat (2025) prioritize the investigation and detection of malware by employing DL approaches through FCNN in order to improve detection ACC while decreasing false alarm rates. The study emphasizes developing a model capable of efficiently detecting malware attacks in complex network environments. Protocol, Source Port, Packet Size, Source IP, and Destination IP are some of the features used by the model for prediction. The potential of DL technology in cybersecurity threat prevention and handling complex attacks is demonstrated experimentally by the high performance of the FCNN model in data classification, with results of 91.49% ACC, 95.45% PRE, 87.50% REC, and 91.18% F1. This allows for effective and timely responses to emerging attack patterns [27].

Tang (2025) deep learning (DL) based network information security situational awareness and prediction model, which combines the advantages of CNN and LSTM, aiming to achieve real-time situational awareness of the network environment and accurate prediction of future security threats situation network security situation by learning the time series law of historical situation data. The experimental results show that the model achieves 92.5% situational awareness ACC on the test set, especially in identifying high-level security threats such as high consumption of computing resources and low ACC of long-term prediction, model optimization and data set for building an intelligent and efficient network security protection system [28].

G et al. (2024) proposed framework captures multiple perspectives of malware behavior, including system calls, memory access patterns, and network activities, to create a comprehensive representation of malicious activities. The MVCNN architecture leverages these diverse views to enhance classification ACC, addressing the limitations of single-view analysis. The dynamic execution of malware in sandboxed environment produces behavior logs which are preprocessed and mapped into multi-dimensional feature maps that are then used to feed into the MVCNN. The model is then designed to extract high-level capabilities across multiple views, to provide robust classification and automatically create unique malware signatures. The experimental validation of the suggested method proves its effectiveness as the classification ACC exceeds 98% on benchmarks. Also, the generated signatures are highly precise and recall in distinguishing malware variations [29].

Ali et al. (2024) Cybersecurity analysis is being provided to SMGs through the strategy of integrating current and voltage data characteristics and training a comprehensive deep-learning model. This model covers attacks at the component level and develops defence mechanisms for detection, mitigation, and prevention. Additionally, it provides a sufficient rate of detection. In addition, as compared to the conventional machine learning approach, the fine-tuned, deep ANN with optimal hyperparameters is able to successfully avoid cyberattacks while boasting an improved ACC level of 97.51% and a modest loss of 0.101% [30].

Sadia et al. (2024) The proposal laid out a strategy using CNNs to improve WSN intrusion detection and prevention in setting where there are multiple classes of data. Research aims to compare the model to CNN, Deep Neural Network (DNN), and enhance detection ACC while decreasing loss value and false alarm rate (5). REC, PRE, support, F, and macro-average are some of the measures used to evaluate the research findings. The remarkable outcomes produced by the CNN model are evidence of the hard work put in: an ACC rate of 97%, a loss measurement of 0.14, and an exceptionally low False Alarm Rate. This greatly improves the ACC of IDS while simultaneously decreasing false alarms, and this, in turn, strengthens the security of WSNs against the elevated cyber threats [31]

Abuali, Nissirat and Al-Samawi (2023) Access to the internet and related networks has put most companies at risk of cybercrime. Security for organisational networks relies heavily on intrusion detection systems (IDSs). Additionally, security researchers have created intrusion detection systems (IDSs) utilising a variety of cutting-edge methodologies, including AI techniques, to combat the ever-evolving amount and quality of viruses and harmful attacks. Hope to present a deep learning system that uses support vector machines (SVMs) to categorise server data in order to identify intrusion instances. The CSE-CIC-IDS 2018 dataset underwent multiple pre-training procedures. A sample dataset consisting of 100,000 instances has been used to implement the proposed model. The results showed a 96% success rate when considering the ACC, PRE, specificity, FP REC, and F1 [32].

Haricharan, Govind and Kumar (2023) The performance is assessed by using supervised machine learning techniques, including SVM and ANN, for the task of network traffic classification on the NSL-KDD dataset. The suggested model surpassed its rivals in terms of intrusion detection, according to research after study. In order to detect and lessen the impact of malicious cyberattacks on hosts and communities, attack detection systems that use ML methods are widely used. Therefore, it is necessary to create a reliable method of identification. Results from the simulation show that the dataset may achieve an extremely high ACC rate of up to 97.52% on many occasions [33].

Recent studies highlight the growing role of AI and DL in strengthening network security. FCNN-based approaches have improved malware detection while reducing false alarms, and hybrid CNN-LSTM models have been applied for real-time situational awareness and threat prediction. Multi-view CNN models can be used to collect the various behavioural features (system calls, memory usage, and network activity) that allow a complete analysis of malware. The ANN- and CNN-based models have already been utilized in such areas as smart microgrids and wireless sensor networks to improve resilience and minimize false alarms. Deep learning in the form of SVMs and classical ML models, like SVMs and ANNs, has been demonstrated to work on benchmark data also. All in all, these show great potential for intrusion detection and mitigation of threats, but when it comes to scalability, flexibility, and real-time implementation.

Table 1 Comparative Analysis of Recent Studies on network security in threat analysis using Machine Learning

Author(s)	Dataset	Key Findings	Performance	Challenges	Future Work
Numpradit, Boonyopakorn & Charoensawat (2025)	Some of the features of network traffic include protocol, port number, packet size, source IP address, and destination IP address.	Proposed FCNN for malware detection with reduced false alarms	Accuracy: 91.49%, Precision: 95.45%, Recall: 87.50%, F1: 91.18%	Handling complex attack scenarios	Extend to larger datasets and real-time detection
Tang (2025)	Historical network security data	Hybrid CNN-LSTM for situational awareness and threat prediction	92.5% situational awareness accuracy	High resource consumption, long-term prediction accuracy	Model optimization and larger dataset integration
G et al. (2024)	Malware behavior logs (sandbox execution)	MVCNN to capture system calls, memory, and network activities	>98% classification accuracy	Single-view limitations in malware analysis	Expand to real-world datasets, signature generation
Ali et al. (2024)	Smart Microgrid (SMG) current & voltage data	Deep ANN for cyberattack detection in SMGs	Accuracy: 97.51%, Loss: 0.101%	Complex component-level attack detection	Enhance resilience and real-time deployment
Sadia et al. (2024)	Wireless Sensor Networks (WSN) traffic data	CNN-based IDS for multiclass classification	Accuracy: 97%, Loss: 0.14	False alarm reduction	Extend to large-scale IoT networks
Abuali, Nissirat & Al-Samawi (2023)	CSE-CIC-IDS 2018	SVM-based DL IDS for intrusion classification	Accuracy: 96%	High evolving malware patterns	Further refinement for adaptive IDS
Haricharan, Govind & Kumar (2023)	NSL-KDD	Comparative study using SVM & ANN	Accuracy: 97.52%	Limited generalization	Apply hybrid ML-DL models

3. Methodology

Modern cyberattacks demand advanced techniques capable of analyzing sequential traffic patterns in real time. The proposed framework integrates deep learning with systematic pre-processing and feature optimization for robust threat detection. The whole process is illustrated in Figure 1. The proposed process of botnet detection uses a systematic approach starting with the CTU-13, a benchmark data set that has all 13 unique botnet scenarios with labeled network traffic. Raw data was initially processed by merging, cleansing and extracting features. The models were made more robust by handling missing values and eliminating outliers. Feature values were standardized to a range of 1-0 using min-max normalization. SMOTE was used in case of class imbalance to oversample minority class samples to make learning balanced. The feature selection was performed through Genetic Algorithm (GA), i.e., the algorithm that optimized the input feature space and retained only those attributes that are most significant, so the dimensionality problem was reduced, and computational efficiency increased. The cleaned data was then separated into training (70%) and testing (30%). Last, a RNN model was applied because it performs well in the recognition of sequential dependence in network traffic patterns, a criterion that makes the model very appropriate in identifying time-dependent patterns in the nature of botnet activities. The model's PRE, REC, ACC, F1, and ROC curves were utilized to assess its efficacy in enhancing network security through threat prediction, classification, and mitigation.

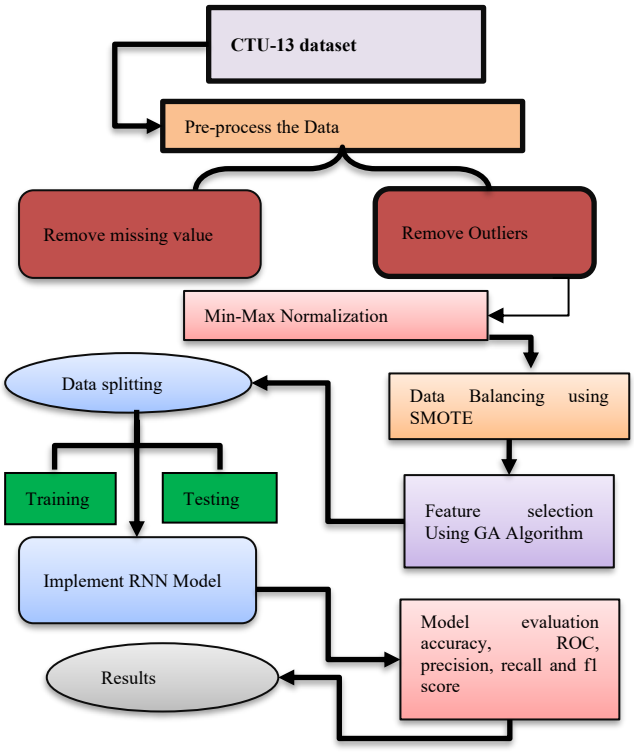

Fig.1 Flowchart for Network Security and Threat Analysis Using Machine Learning

Data collection

The CTU-13 dataset is widely used as a benchmark by researchers in botnet identification. Comprised 25,677 instances that were categorised as either botnet or

normal traffic. It mimics various botnet behaviours, including spam, distributed denial of service, and click fraud, using tagged traffic data from thirteen real-world cases. Protocol type, source and destination addresses, port numbers, flow time, byte count, and packet count are all part of each flow record in the dataset. The following are examples of some of the visuals:

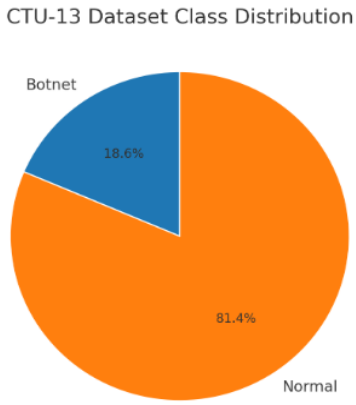

Fig.2 Class Distributions of pie chart

The count distribution of classes in the CTU-13 data, which shows the large lopsided distribution in Figure 2, with regular network traffic occupying 81.4 percent of the samples and malicious botnet traffic occupying 18.6 percent, illustrates the natural condition of cybersecurity data sets, where anomalous patterns are naturally sparse, requiring an intensive classification method to achieve successful network intrusion detection.

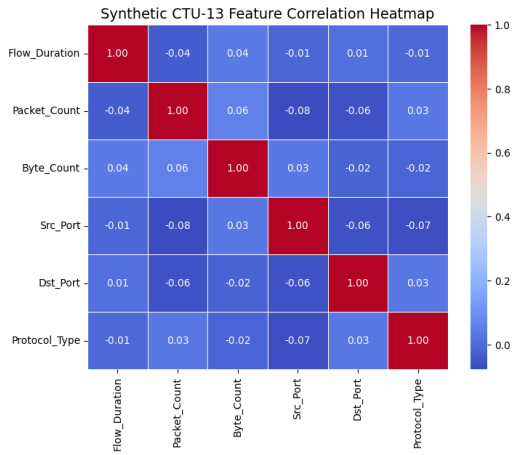

Fig.3 Distribution of Feature Correlation Heatmap

Figure 3, provides the feature correlation heatmap, which depicts the correlation value between network traffic features such as Flow Duration, Packet Count, Byte Count, Src Port, Dst Port, and Protocol Type and has Pearson correlation coefficients ranging between -0.08 to 1.00, indicating there is limited inter-feature dependencies that are inherent to the effective network security anomaly detection and intrusion classification systems.

Data Preprocessing

Data preparation involved collecting the CTU-13 dataset, merging the data files, and performing data cleansing to extract relevant features. Data transformation and normalization, addressing missing values, and outlier removal were all part of the pre-processing stages. The key steps of the pre-processing process are outlined below. Key steps in data pre-processing include:

Remove missing value: One simple approach to cleaning up a data frame is to use the dropna () function to eliminate any observations or features that have missing values. Some methods are listed below. In an attempt to clean up a dataset, one of three things could happen: When using dropna (), all rows with empty values are removed.

Remove Outliers: An integral aspect of data pre-processing, outlier reduction ensures that models and analytics are more accurate and consistent. Data points that are extremely out of the ordinary, or outliers, might distort the results and hurt the accuracy of the models used to analyze them.

Min Max Normalization

Records were normalized by limiting values to a range of 0 to 1 using the min-max approach. The goal in doing this was to make the classifiers work better and lessen the impact of extreme cases. The following mathematical formula was used to undertake the normalization process Equation (1):

$$X' = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (1)$$

X_{min} represents the minimum value, X_{max}stands for the maximum value, X' stands for the normalised value, and X is the beginning value of the feature.

Data Balancing using SMOTE

The term "data balancing" refers to the practice of correcting class imbalance by changing the distribution of classes in a dataset. SMOTE, is a way to even out datasets that are skewed in one direction or the other by adding fake data points from the minority group. Using linear interpolation, remove noisy samples from the minority (attack) class and add more to the normal (main) class, while decreasing the number of samples in the minority (attack) class. To fix the issue of machine learning models favouring the majority, this can be utilised to improve representation of minority groups.

Feature Selection Using GA Algorithm

The GA algorithm, a well-known evolutionary optimization technique, is used in the feature selection process. This process is a carbon copy of natural selection, in which the fittest individuals pass their

genes on to future generations. Feature selection programs employ Ga to find the best and most relevant features for predictive modelling, while also reducing the number of features that are unnecessary or redundant. This optimization enhances the model's computing performance while reducing the dataset without sacrificing ACC.

Data splitting

A training set and a test set were created from the dataset so that the model's performance could be accurately evaluated. Training used 70% of the data for parameter approximation and model training, while testing and performance evaluation only used 30%.

Classification Equation of Recurrent Neural Network (RNN) Model in Network Security

RNNs are a kind of DL model that was originally developed to handle sequential input. In order to process sequential data, Recurrent Neural Networks (RNNs) keep a secret state that stores details about their previous inputs [34]. Three layers make up the fundamental design: input, concealed, and output. Figure 4 shows that RNNs, in contrast to feedforward neural networks, feature recurrent connections, which enable data to circulate inside the networks.

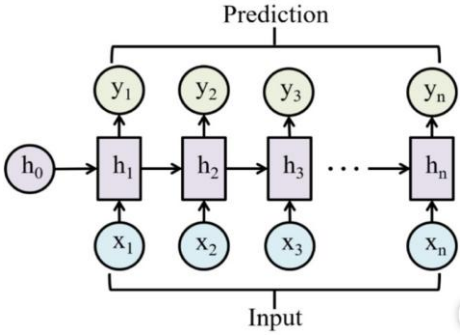

Fig.4 Structured of RNN Model

Every time step t rolls around, the RNN changes its hidden state **h***t* with an input vector **x***t* according to Equation (2).

$$h_t = \sigma_h(W_{xh}x_t + W_{hh}h_{t-1} + b_h) \quad (2)$$

$$y_t = \sigma_h(W_{hy}h_t + b_y) \quad (3)$$

The hidden and output layers are linked by the weight matrix W_{hy}, Which stands for by, the bias vector, and σy, the activation function for the output layer.

Performance Matrix

Several performance criteria were used to evaluate the efficacy of the suggested design. TP, FP, TN, and FN were found by comparing the model's predicted outputs with the real values. Please elaborate on the key evaluation criteria derived from these findings below reliability, specificity, memory, and F1-score:

Accuracy: A measure of how well the trained model predicted outcomes relative to the whole dataset (input samples). It is presented as Equation (4)-

$$Accuracy = \frac{\text{TP+TN}}{\text{TP+Fp+TN+FN}} \quad (4)$$

Precision: Precision measures how well a model predicts positive occurrences relative to all positive occurrences. Precision indicates. How good the classifier is in predicting the positive classes is expressed as Equation (5)-

$$Precision = \frac{\text{TP}}{\text{TP+FP}} \quad (5)$$

Recall: This metric, the ratio of events that were accurately predicted as positive to all instances that should have proved positive. In mathematical form it is given as Equation (6)-

$$Recall = \frac{\text{TP}}{TP+FN} \quad (6)$$

F1 score: It is a combination of the harmonic mean of REC and PRE, that is, it helps to balance REC and PRE. Its range is [0, 1]. Mathematically, it is given as Equation (7)-

$$F1 - score = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad (7)$$

Receiver Operating Characteristic Curve (ROC): The ROC plot shows the likelihood that a model correctly identifies positive cases and the likelihood that it incorrectly identifies negative examples. Whereas FPR (1-specificity), TPR (more commonly known as sensitivity or REC).

4. Results and Discussion

The Intelligent Recurrent Neural Network (RNN) model of network threat detection proposed has been experimentally performed in a GPU-accelerated environment of Google Colab to ensure an efficient processing and less time of convergence. It consisted of Python 3.10 and packages such as TensorFlow 2.x and Keras, 16 GB VRAM, and 12 GB RAM. The GPU was an NVIDIA Tesla T4. This model was developed, and it was tested and trained on CTU-13, a popular botnet and intrusion detection dataset. It is a dataset that spans a range of good and bad traffic trends. The performance was evaluated based on the criteria given in Table II, which are ACC, PRE, REC, and F1. The proposed RNN achieved excellent performance with 99.25% ACC, 98.30% PRE, 99.25% REC, and 98.75 F1. Regarding the steady ability to detect threats and a reasonable balance of the detection sensitivity and the detection ACC, these measures can testify to the fact that RNN is long-term. According to these results, RNN model is a very powerful tool that can be used to identify and prevent threats in dynamic network environments in real-time.

Table 2 Experiment Results of Proposed Models for Threat Analysis and Mitigation on CTU-13 Dataset

Performance matrix	Recurrent Neural Network (RNN) Model
Accuracy	99.25
Precision	98.30
Recall	99.25
F1-score	98.75

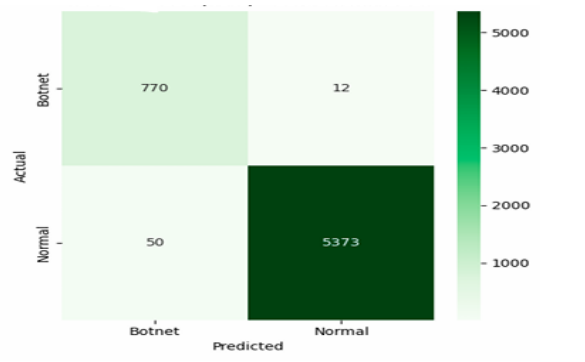

Fig.5 Confusion Matrix for the RNN Model

The confusion matrix of the proposed model based on classification is presented in Figure 5. It is shown that the model had a high level of ACC with 770 botnet instances and 5373 samples of the normal traffic being accurately identified. In addition, it showed strong discriminative effectiveness through the attainment of a minimum level of misclassification 12 false positives (non-botnet traffic samples labelled as botnet) and 50 false negatives (botnet samples labelled as normal).

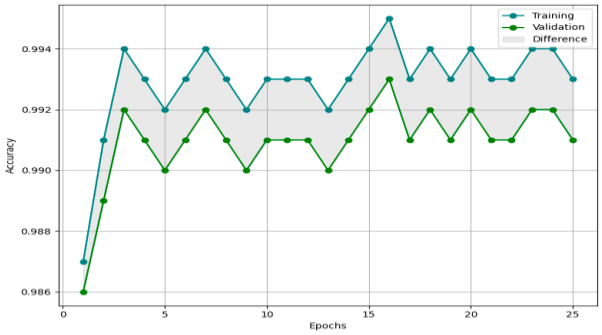

Fig.6 Accuracy Curves for the RNN Model

Figure 6 shows the training and validation accuracy curves with 25 epochs. The training ACC (blue line) is about 99.6% and the validation ACC (green line) is about 99.3% which shows that the model successfully converges without overfitting and has a steady performance in the intrusion detection of networks and other cybersecurity threats classification applications.

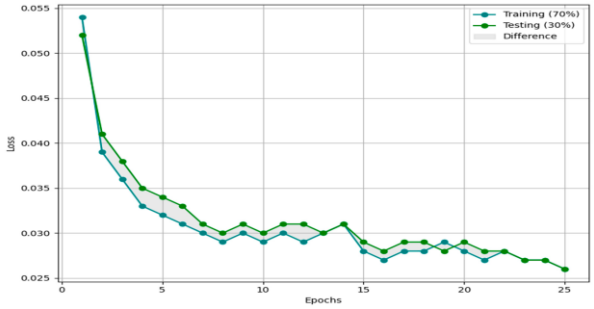

Fig.7 Loss curves for the RNN Model

Figure 7 shows training and testing loss convergence after 25 epochs with data split percentage 70%-30% where both curves decline fast at first to about 0.025 and convergence is stable with no significant variations in training and testing phases and is a good validation of effective model optimization in network security anomaly detection applications.

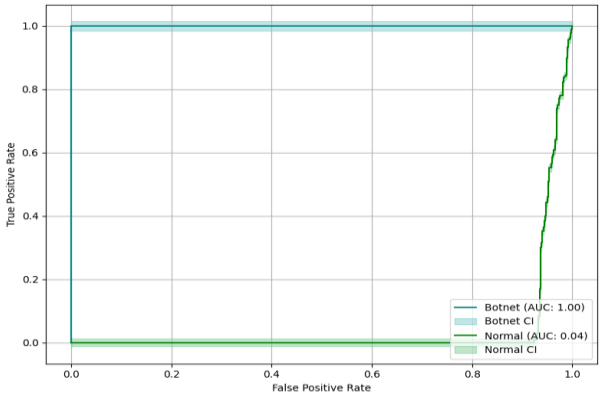

Fig.8 Curves for the RNN Model

Figure 8 illustrates the ROC curves of binary classification performance, which indicate that the detection of botnet in Figure 8 has an AUC of 1.00, and normal traffic classification has an AUC of 0.64, indicating excellent discriminative ability in detecting malicious traffic and acceptable performance in detecting normal network traffic in cybersecurity intrusion detection systems.

Discussion

The suggested RNN model has been demonstrated effective in terms of its ACC when compared to that of other existing models. Table III is a comparison of four types of neural networks RNNs, CNNs, SVMs, and HMMs using four metrics including REC, ACC, PRE, and F1. According to the data on the experiments, the proposed RNN model outperforms the baseline models significantly. ACC, PRE, REC, and F1 were 94.80%, 70.46%, 98.01% and 81.98% alias 97.21%, 96.84%, 96.59%, and 96.71% with HMM, CNN, and SVM, respectively. RNN is a powerful network security solution to implement in real-time and it is definitely superior compared to the other solutions in all the metrics of the evaluation. It was the most accurate (99.25%) and had a very good balance in terms of the capture of sequential dependencies to network traffic patterns, which was better in intrusion detection.

Table 3 Accuracy Comparison of Different Predictive Models of Threat Analysis and Mitigation for Enhancing Network Security using the CTU-13 Dataset

Models	Accuracy	precision	Recall	F1-score
HMM[35]	94.80	70.46	98.01	81.98
CNN[36]	97.21	96.84	96.59	96.71
SVM[37]	92	--	91.5	92
RNN	99.25	98.30	99.25	98.75

The suggested RNN model has important benefits regarding the threat analysis and mitigation

application as it is capable of processing sequential and time-dependent data effectively, which is important to analyze network traffic patterns. RNN, unlike conventional models where the data points are handled as discrete points, captures temporal relationships and changing behavior of the malicious activities, and hence more effective threat detection. The ACC of 99.25% on the CTU-13 data can be used to show its effectiveness and can be of great significance in terms of identifying sophisticated and delicate patterns of intrusion, thereby, enhancing a robust network security in dynamic and real-time conditions.
conclusion and future work

The threat identification, assessment, and prioritization process identifies potential system, network or information harm. Deep learning can be used to improve the security of the network to deal with the increased sophistication of cyber adversaries, especially botnet-based attacks. In this paper, a detailed model has been suggested to combine systematic pre-processing, feature optimization, and deep-learning steps in order to achieve effective detection and mitigation. Based on the CTU-13 dataset that consists of real-life botnet samples, pre-processing (min-max normalization, class balancing using SMOTE, and feature reduction using Genetic Algorithm (GA)) took place. The model uses RNN to learn sequential dependencies on network flows with the highest ACC of 99.25% compared to the baseline models, such as Hidden Markov Model (94.80%), Convolutional Neural Network (97.21%), and Support Vector Machine (92%). These findings indicate the effectiveness of a pre-processing/ optimization/temporal learning approach to scalable and precise threat detection. The RNN was found to be effective in real-time anomaly detection, which has high generalization and is stable in unstable environments.

Future research should be the application of the framework to other benchmark data sets to achieve greater generalizability, to other architectures such as LSTM and CNN-RNN hybrids, and to Explainable AI (XAI) with real-time streaming support that will make interpretability, scalability and deployment-readiness of next-generation cybersecurity achievable.

References

[1] H. Kali, "The Future Of Hr Cybersecurity: Ai-Enabled Anomaly Detection In Workday Security.," Int. J. Recent Technol. Sci. Manag., vol. 8, no. 6, 2023, doi: 10.10206/IJRTSM.2025803096.

[2] 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.

[3] V. Prajapati, "Role of Identity and Access Management in Zero Trust Architecture for Cloud Security : Challenges and Solutions," Int. J. Adv. Res. Sci. Commun. Technol., vol. 5, no. 3, pp. 6–18, 2025, doi: 10.48175/IJARSCT-23902.

[4] 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.

[5] V. M. L. G. Nerella, K. K. Sharma, S. Mahavratayajula, and H. Janardhanan, "A Machine Learning Framework for Cyber Risk Assessment in Cloud-Hosted Critical Data Infrastructure," J. Inf. Syst. Eng. Manag., vol. 10, no. 4, pp. 2409–2421, 2025, doi: 10.52783/jisem.v10i4.12804.

[6] D. Patel, "Leveraging Blockchain and AI Framework for Enhancing Intrusion Prevention and Detection in Cybersecurity," Tech. Int. J. Eng. Res., vol. 10, no. 6, pp. 853–858, 2023, doi: 10.56975/tijer.v10i6.158517.

[7] S. B. Shah, B. Boddu, N. Prajapati, and S. A. Pahune, "AI-Powered Advanced Intrusion Detection for Securing Cloud Environments Against Network Attacks," in 2025 Global Conference in Emerging Technology (GINOTECH), IEEE, May 2025, pp. 1–7. doi: 10.1109/GINOTECH63460.2025.11076673.

[8] 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.

[9] P. Chandrashekar and M. Kari, "Design Machine Learning-Based Zero-Trust Intrusion Identification Models for Securing Cloud Computing Systems," Int. J. Res. Anal. Rev., vol. 11, no. 4, pp. 901–907, 2024.

[10] A. Djenna, S. Harous, and D. E. Saidouni, "Internet of Things meets Internet of Threats: New Concerns Cyber Security Issues of Critical Cyber Infrastructure," Appl. Sci., 2021, doi: 10.3390/app11104580.

[11] 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.

[12] 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.

[13] V. Shewale, "Demystifying the MITRE ATT&CK Framework: A Practical Guide to Threat Modeling," J. Comput. Sci. Technol. Stud., vol. 7, no. 3, pp. 182–186, May 2025, doi: 10.32996/jcsts . 2025.7.3.20.

[14] S. B. Shah, "Machine Learning for Cyber Threat Detection and Prevention in Critical Infrastructure," Dep. Oper. Bus. Anal. Inf. Syst. (OBAIS, vol. 2, no. 2, 2025, doi: 10.5281/zenodo . 14955016.

[15] R. Patel, "Automated Threat Detection and Risk Mitigation for ICS (Industrial Control Systems) Employing Deep Learning in Cybersecurity Defence," Int. J. Curr. Eng. Technol., vol. 13, no. 06, pp. 584–591, 2023, doi: 10.14741/ijcet/v.13.6.11.

[16] Y. Lu and L. Da Xu, "Internet of Things (IoT) cybersecurity research: A review of current research topics," IEEE Internet Things J., 2019, doi: 10.1109/JIOT.2018.2869847.

[17] A. R. Khan, M. Kashif, R. H. Jhaveri, R. Raut, T. Saba, and S. A. Bahaj, "Deep Learning for Intrusion Detection and Security of Internet of Things (IoT): Current Analysis, Challenges, and Possible Solutions," 2022. doi: 10.1155/2022/4016073.

[18] S. Ayyalasomayajula, D. D. Rao, M. Goel, and S. Khan, "A Mathematical Real Analysis on 2D Connection Spaces for Network Cyber Threats : A SEIAR-Neural Network Approach A Mathematical Real Analysis on 2D Connection Spaces for Network Cyber Threats : A SEIAR-Neural Network Approach," Commun. Appl. Nonlinear Anal., vol. 31, no. September, pp. 178–198, 2024, doi: 10.52783/cana.v31.1474.

[19] R. Dattangire, R. Vaidya, D. Biradar, and A. Joon, "Exploring the Tangible Impact of Artificial Intelligence and

Machine Learning: Bridging the Gap between Hype and Reality," in 2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET), IEEE, 2024, pp. 1–6. doi: 10.1109/ACET61898.2024.10730334.

[20] 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.

[21] N. G. Polson and V. O. Sokolov, "Deep Learning - Nature Review," Nature, 2018.

[22] C. Nobles, "Offensive artificial intelligence in cybersecurity: Techniques, challenges, and ethical considerations," in Real-World Solutions for Diversity, Strategic Change, and Organizational Development: Perspectives in Healthcare, Education, Business, and Technology, 2023. doi: 10.4018/978-1-6684-8691-7.ch021.

[23] R. Q. Majumder, "Machine Learning for Predictive Analytics : Trends and Future Directions," Int. J. Innov. Sci. Res. Technol., vol. 10, no. 4, 2025.

[24] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?," IEEE Signal Process. Mag., 2018, doi: 10.1109/MSP.2018.2825478.

[25] D. Bhamare, T. Salman, M. Samaka, A. Erbad, and R. Jain, "Feasibility of Supervised Machine Learning for Cloud Security," in ICISS 2016 - 2016 International Conference on Information Science and Security, 2017. doi: 10.1109/ICISSEC.2016.7885853.

[26] S. A. Pahune, P. Matapurkar, S. Mathur, and H. Sinha, "Generative Adversarial Networks for Improving Detection of Network Intrusions in IoT Environments," 2025 4th Int. Conf. Distrib. Comput. Electr. Circuits Electron., pp. 1–6, 2025, doi: 10.1109/ICDCECE65353.2025.

[27] J. Numpradit, P. Boonyopakorn, and S. Charoensawat, "Malware Detection and Analysis Using Deep Learning Through Fully Connected Neural Network (FCNN)," in 2025 IEEE International Conference on Cybernetics and Innovations (ICCI), 2025, pp. 1–6. doi: 10.1109/ICCI64209.2025.10987292.

[28] Z. Tang, "Research on Network Information Security Situation Awareness and Prediction Model Based on Deep Learning," in 2025 International Conference on Electrical Drives, Power Electronics & Engineering (EDPEE), 2025, pp. 496–501. doi: 10.1109/EDPEE65754.2025.00091.

[29] S. P. K. G, S. G. Sanu, K. Saranya, T. V. R. Kanth, and M. S, "Dynamic Malware Classification and Signature Generation Using Multi-View Convolutional Neural Networks," in 2024 International Conference on Integrated Intelligence and Communication Systems (ICIICS), IEEE, Nov. 2024, pp. 1–7. doi: 10.1109/ICIICS63763.2024.10859526.

[30] Z. Ali, T. Hussain, C.-L. Su, A. D. Jurcut, S. Baloch, and M. Sadiq, "Cyber Attacks Detection using Deep Learning Methods for Resilient Operation in DC Shipboard Microgrids," in 2024 IEEE/IAS Industrial and Commercial Power System Asia (I&CPS Asia), 2024, pp. 120–125. doi: 10.1109/ICPSAsia61913.2024.10761631.

[31] H. Sadia et al., "Intrusion Detection System for Wireless Sensor Networks: A Machine Learning Based Approach," IEEE Access, 2024, doi: 10.1109/ACCESS.2024.3380014.

[32] K. M. Abuali, L. Nissirat, and A. Al-Samawi, "Advancing Network Security with AI: SVM-Based Deep Learning for Intrusion Detection," Sensors, vol. 23, no. 21, 2023, doi: 10.3390/s23218959.

[33] M. G. Haricharan, S. P. Govind, and C. N. S. V. Kumar, "An Enhanced Network Security using Machine Learning and Behavioral Analysis," in 2023 International Conference for Advancement in Technology, ICONAT 2023, 2023. doi: 10.1109/ICONAT57137.2023.10080157.

[34] 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.

[35] R. Mannikar and F. Di Troia, "Enhancing Botnet Detection in Network Security Using Profile Hidden Markov Models," Appl. Sci., vol. 14, no. 10, 2024, doi: 10.3390/app14104019.

[36] M. K, N. S, D. V, and D. S. Baskaran, "Botnet Attack Procrastination Using Deep Learning Algorithm," Int. J. Res. Appl. Sci. Eng. Technol., vol. 13, no. 4, pp. 3736–3641, 2025, doi: 10.22214/ijraset . 2025.69088.

[37] J. Chao and T. Xie, "Deep Learning-Based Network Security Threat Detection and Defense," Int. J. Adv. Comput. Sci. Appl., vol. 15, no. 11, pp. 669–679, 2024, doi: 10.14569/IJACSA.2024.0151164.