Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Next-Gen Cyber Defense: Integrating Deep Learning into Threat Detection Systems

Md Ismail Jobiullah[1], Sakera Begum[1,*], Ali Raza A Khan[2], Muhammad Ismaeel Khan[3], Aftab Arif[3], Touhid Bhuiyan[3]

1School of Information Technology, Washington University of Science and Technology, 2900 Eisenhower Ave, Alexandria, VA 22314, USA

2College of Cybersecurity, Virginia University of Science and Technology, 2070 Chain Bridge Rd STE 100, Vienna, VA 22182, USA

3School of Information Technology, Washington University of Science and Technology, 2900 Eisenhower Ave, Alexandria, VA 22314, USA

**Corresponding author e-mail: sakerasiu23@gmail.com*

ARTICLE INFO

Received: 01 Dec 2025

Revised: 05 Jan 2026

Accepted: 14 Jan 2026

ABSTRACT

Network traffic is evolving faster and cyber threats are increasingly becoming more sophisticated thus requiring more adaptive and efficient intrusion detection systems (IDSTraditional rule-based or signature-based intrusion detection system designs produce a significant number of false positives because they are unable to identify novel or sophisticated attack methods. The integration of deep learning methods such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Feedforward Neural Networks (FNN) to enhance network threat detection is examined in this paper. The study relies on CICIDS 2017 dataset, which is a rich dataset and includes a broad spectrum of attack types, such as Denial of service (DoS), Distributed Denial of service (DDoS), and Port Scanning. We evaluate the work of single models and a hybrid one of FNN, CNN and RNN to enhance the feature extraction and sequence analysis. Accuracy, precision, recall, F1-score, and AUC-ROC are the key measures of evaluation, used to evaluate the performance of the models. These results show that CNN model is the optimal one because it has accuracy of 98.66%, precision of 95.47%, recall of 96.63%, and AUC-ROC of 0.9990. FNN also performs well with an accuracy of 98.64 and RNN lower convergence although achieves an accuracy of 95.84. The hybrid model integrates the capabilities of FNNs, CNNs and RNNs and offers the similar outcomes. These findings demonstrate the potential of deep learning to detect both current and new cyber threats and the CNN model and FNN were observed to produce the overall best outcomes. In further research, it is possible to concentrate on more optimization (adversarial training and transfer learning) to obtain more specifics regarding detection and address the challenges of sequential processing of data.

Keywords: Threat Detection, Deep Learning, Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Feedforward Neural Networks (FNN), Hybrid Model, CICIDS 2017 Dataset, Cybersecurity.

INTRODUCTION

The rapid increase of network traffic and the ever-growing complexity of attacks require companies to build more reliable and flexible solutions in detecting and responding to network threats. Considering they are mostly rule- or signature-based, traditional intrusion detection systems (IDS) are highly good at identifying known attack patterns but lack the capability to identify novel, unidentified, or developing attack patterns. Such techniques often have very high false positive rates, and they have limited ability to deal with new attack schemes that do not fit an established pattern. Machine learning (ML) and deep learning (DL) frameworks have become promising tools for developing more dynamic and effective intrusion detection systems (IDS) that could effectively identify both familiar and unfamiliar attack scenarios in real-time, given the constantly changing dynamics and sophistication of cyber threats [1, 2].

The recent developments in deep learning and machine learning have offered more malleable methodologies that are able to learn autonomously with large quantities of data without requiring defined rules or signatures. These tactics make use of massive amounts of information to identify more complex attack patterns that do not enter into the notice of conventional systems. Recurrent neural networks (RNNs) and convolutional neural networks (CNNs) have

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

drawn a lot of interest because of their capacity to extract complex features from unprocessed network traffic data. CNNs are also effective at recognizing spatial characteristics that prove to be essential in network traffic pattern and anomaly detection in data [3, 4]. On the other hand, RNNs excel in processing sequential data, which makes them especially efficient in detecting attacks that evolve over time or have some kind of time-dependencies [5, 6].

The advances in deep learning have revolutionized network intrusion detection because they allow detecting previously unseen attacks without the use of explicit signatures or hand-written feature engineering. When intrusion detection systems employ deep learning models on network traffic data, they are able to detect and identify both known and unknown threats with high accuracy in comparison to traditional methods. CICIDS datasets, 2017 and 2018 have been introduced, and they are now considered vital resources to both train and evaluate these models, including attack patterns like Denial of Service (DoS), Distributed Denial of Service (DDoS), Port Scanning and Brute Force [7-9]. These datasets are large datasets containing millions of cases with various types of attacks, which provide a huge range of real-life conditions to generate and test IDS models [10].

By relying on such datasets and employing advanced deep learning algorithms, researchers would like to improve the accuracy, efficiency, and generalization of network intrusion detection systems. Conventional signature-based systems are limited in their ability to respond to emerging attack signature patterns, but deep learning models can respond to new threats directly by learning patterns of data. Such flexibility will be critical in modern cybersecurity because cybercriminals constantly improve their methods of attack. In addition, intrusion detection systems based on deep learning models enable the detection of subtle and complex attacks, which are difficult to detect using traditional approaches [11-13].

A major issue in Intrusion Detection systems (IDS) is the large amount of network traffic data which makes traditional solutions computationally expensive and time consuming. The ability of deep learning models, CNNs and RNNs in particular, to process large datasets is because of their ability to process data efficiently. Complexity and multidimensionality of network traffic data also pose additional challenges to deep learning model training. To achieve good performance with a model, it is mandatory to have good data preprocessing, which involves normalization, feature extraction, and handling of imbalanced datasets [14, 15]. It uses the CICIDS 2017 dataset, and it makes use of advanced pre-processing operations that ensure quality and reliability of the training data [16].

Moreover, implementation of deep learning in Intrusion Detection Systems has certain challenges. Overfitting It is a common issue with the training of deep learning models, where the model becomes overly optimistic to the training data and cannot generalize well to new data. It is necessary to reduce this issue by regularization strategies such as dropout and early halting to guarantee that models remain resistant to different types of attacks [17, 18]. In addition, the ability of deep learning models to explain their findings, especially in the most sensitive areas such as cybersecurity, is a growing concern. Xplainable AI (XAI) systems are being added to Intrusion Detection Systems (IDS) so that more transparency can be achieved and trust built in model predictions [19, 20].

Deep learning as a method of network intrusion detection has great potential in improving detection accuracy and reaction to newer threats. The performance and effectiveness of IDS can be improved in real-life scenarios using sophisticated architectures such as FNNs, CNNs and RNNs. CICIDS 2017 dataset offers a valuable source to train and test those models and conduct a comprehensive analysis of their effectiveness in detecting established and new attack patterns [21, 22]. The aim of the study is to further advance the discipline by analyzing these models and then give a detailed performance analysis using the datasets, which will enhance the effectiveness of the network intrusion detection systems against more advanced cyber threats.**[5]**

The contributions of this study are major because they include:

- The paper explores four deep learning architectures including Feedforward Neural Networks (FNN) that are based on Convolutional Neural Networks (CNN) deep learning, Recurrent Neural Networks (RNN), and a Hybrid model with the aim of improving both the accuracy and efficiency of network intrusion detection.
- It gives a detailed analysis of performance of these models, with critical points of evaluation including accuracy, precision, recall, F1-score, AUC-ROC and Matthews Correlation Coefficient (MCC).

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- The paper provides an insight into how the models converge, such as training loss and accuracy to point out their learning efficiency and effectiveness.
- It examines the possibility of hybrid models, which encompass CNNs and RNNs, as they have the feature extraction and sequence data analysis advantages that can be used to augment intrusion detection.

The rest of the paper is structured is as follows: The related work carried out by various researchers on machine learning and deep learning models to detect intrusion is reviewed in Section 2. Section 3 also describes how the study was carried out. The result analysis is given in Section 4. Section 5 talks about the results, the strengths and weakness of the models, and an idea on how to take the research further in the future, and the final part (Section 6) will be the conclusion, which includes the contribution to the research presented in the study.

RELATED WORK

The dynamic and increasing complexity of cyber threats in the modern digital environment require more dynamic approaches rather than the use of the stagnant and signature-based protection. As a result, deep learning (DL) and machine learning (ML) solutions are currently critical in the development of cybersecurity systems, and they have the potential to create proactive and smart systems that can detect and prevent advanced, new attack patterns. In the section, the evolution of deep learning to support next-generation threat detection systems has been discussed, with its main contributions, their relevance, and constraints.

John et al. (2025) explored the use of supervised, unsupervised, and reinforcement learning models in the improvement of cyber defense systems. Their research is based on proactive detection in the form of network traffic observation and anomaly detection. Despite the evidence that different machine learning methods can be useful, the study does not provide a profound comparison and contrast with current and up-to-date deep learning patterns, which restricts its relevance to the real-life dynamic threat setting. Ofoegbu et al. (2023) suggested a combined framework of machine learning and big data analytics in real-time cybersecurity threat detection. This method will solve the shortcomings of the conventional approach through the power of real-time analytics. Nevertheless, it fails to discuss the practice of state-of-the-art deep learning models that could be more effective in capturing difficult attack patterns. A thorough survey on the use of AI technologies in cybersecurity was conducted by Zheng (2025), where the researcher divided them into supervised, unsupervised, and semi-supervised learning strategies. This paper identifies CNNs and RNNs as the products to address the limitations of traditional security procedures. The weakness of Zheng work is that the experimental validation of the work on real-life data, e.g. CICIDS, is not provided, which may further prove the efficiency of these methods in dynamic threat situations. Alabdulatif (2025) proposed a new set of deep learning models to detect intrusions, which entails the Explainable Artificial Intelligence (XAI) to create models that are more interpretable and trustworthy. Although the introduction of XAI is a relevant addition, the disadvantage of the study is that it concentrated on the classical deep learning models, which may not be sufficiently responding to the new and more sophisticated patterns of attacks that newer models such as hybrid architectures could manage. John and Olusegun (2025) discussed how the intrusion detection can be implemented using the advanced deep learning models, including CNNs, RNNs, and Transformer-based models. As their study revealed, complex patterns of cybercrime are better recognized under their models as compared to traditional techniques. Nevertheless, the performance analysis of their study in relation to a variety of datasets is lacking, which might give a better picture of the model generalization. Hybrid models have also attracted the attention in their potential of detection of threats. Zahid and Bharati (2025) presented a hybrid CNN-BiLSTM model to detect attacks in real-time in the IoT systems, which demonstrated better results in standard datasets, such as KDDCup99, NSL-KDD, and CIC_IDS_2017. Although this hybrid model is effective in enhancing the detection rates, its operation in the resource-constrained environment and non-IoT systems are not investigated. Markkandeyan et al. (2025) suggested a mixed deep learning approach that is an Adaptive Tensor Flow Deep Neural Network and Enhanced Long Short Term Memory (E-LSTM) with optimization algorithms to identify malware. Although their implementation has prospects in processing IoT malware detection, they are yet to be implemented in more intricate or heterogeneous cybersecurity structures. There is an increasing complexity of cyber threats in critical infrastructure, and Khalaf et al.

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

(2025) developed a machine learning-based real-time threat detection system. Despite the model performance which is impressive in protecting the infrastructure, it is not scalable to other sectors which have different network topology. Abdi et al. (2024) evaluated the advantages of using deep learning to improve proactive cybersecurity of smart grid communications with a particular focus on the shift between the reactive and proactive defense mechanisms. As far as this work provides some useful information on cybersecurity in smart grids, it fails to address the concept of combining several deep learning models to enhance the detection of a variety of cyber-physical systems. Nisha (2025) demonstrated a deep learning approach, which relies on the pre-processing of the data on the basis of the CICIDS 2017 data set, concerned with the enhancement of noise removal, feature encoding, and normalization to generate high-quality model training. Although the research highlights the criticality of data quality, the research does not explore the effect of such preprocessing methods on the hybrid deep learning models which can potentially improve the performance of detection further.

All these studies will help in the development of cybersecurity using machine learning and deep learning models. Nevertheless, there are still weaknesses in the implementation of hybrid models, real-time detection, and generalization into different fields. This paper will be attempting to fill these gaps by proposing an all-inclusive Next-Gen Cyber Defense architecture that will combine the latest and greatest deep learning methods that would not only improve threat detection capabilities, but also proactive and intelligent reaction to new cyber threats.

Table 1. Summary of Existing Work.

Authors	Year	Key Contribution/Model	Dataset(s) Used	Domain/Focus
John & Banga [23]	2025	Integration of ML (Supervised, Unsupervised, Reinforcement Learning) for proactive threat detection.	Not specified	General Cyber Defense
Ofoegbu et al. [24]	2023	Real-time threat detection using ML and big data analytics.	Not specified	General Cyber Defense
Zheng [25]	2025	Review of AI/DL techniques (CNNs, RNNs) in cybersecurity.	Not specified	General Cybersecurity
Alabdulatif [26]	2025	Novel ensemble of DL models with Explainable AI (XAI) for intrusion detection.	Not specified	Intrusion Detection Systems (IDS)
John & Olusegun [27]	2025	Advanced DL (CNNs, RNNs, Transformers) for enhancing IDS.	Not specified	Intrusion Detection Systems (IDS)
Zahid & Bharati [28]	2025	Hybrid CNN-BiLSTM model for real-time attack detection.	KDDCup99, NSL-KDD, CIC_IDS_2017	IoT Systems
Markkandeyan et al. [29]	2025	Hybrid DL (Adaptive TensorFlow DNN, E-LSTM) with optimization for malware detection.	Not specified	IoT Systems
Khalaf et al. [30]	2025	AI-driven cybersecurity system for real-time threat detection.	Not specified	Critical Infrastructure
Abdi et al. [31]	2024	Survey on DL for proactive cybersecurity.	Not specified	Smart Grid Networks
Nisha [32]	2025	Deep learning-based framework focusing on data pre-processing.	CICIDS2017	General Cybersecurity

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

PROPOSED METHODOLOGY

This research uses the CICIDS 2017 dataset to use deep learning algorithms for network intrusion detection through a methodical series of stages. These steps are: data collection, preprocessing, model selection, training, and evaluation. Each stage is critical to ensuring the correctness and reliability of the final model. Figure 1 shows the framework for the suggested methodology.

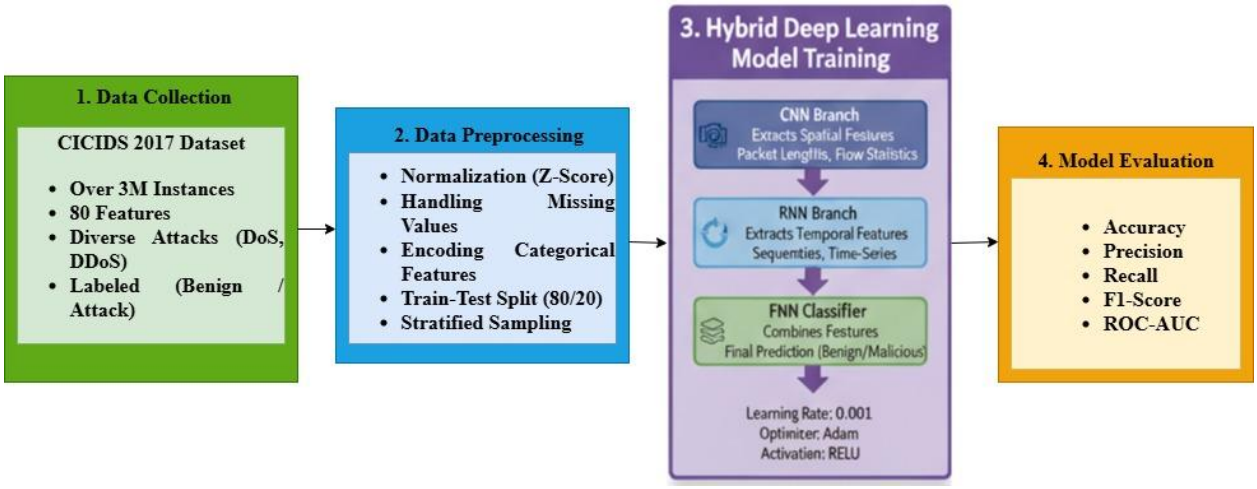

Figure 1: The framework for the proposed methodology.

3.1 Dataset Collection

The CICIDS 2017 dataset is extensively utilized in the network intrusion detection system (NIDS) studies. It is collected from the Canadian Institute for Cybersecurity (CIC) of the University of New Brunswick [33]. It has a substantial volume of network traffic data with diverse attacks, which is suitable in the training and testing of deep learning models. Table 2 describes the dataset.

Table 2. Description of the CICIDS 2017 dataset.

Feature	**CICIDS 2017**
Number of Instances	Over 3,000,000 instances
Number of Features	80 features
Types of Data	Network traffic, logs, attack labels
Types of Attacks Included	DoS, DDoS, Port Scanning, Brute Force, Botnets, and more
Labeling	Supervised - Each instance is labeled as either benign or attacked.
Data Sources	Collected from multiple sources including real-world networks.
Traffic Protocols	HTTP, DNS, FTP, SMTP, POP3, and more
Time Frame	Recorded over several months in 2017.

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The dataset contains marked examples of benign traffic and different network attacks, and the machine learning and deep learning models can be trained to detect intrusion.

3.2 Data Preprocessing

The quality and the structure of the input data are quite sensitive to deep learning models. Preprocessing of data is thus a very important step. Preprocessing of CICIDS 2017 dataset covers normalization, missing values, categorical encoding, and partitioning the data into training and the testing sets.

Normalization/Standardization:

In the case of deep learning models, input data need to be normalised or standardised such that all features are on a common scale to avoid the possibility of a model becoming biased with respect to specific features.

The formula of Z-score normalization is expressed in the equation (1):

$$X_{\text{normalized}} = \frac{\text{X}-\mu}{\sigma} \quad (1)$$

Where X is the feature value, μ is the mean of the feature, σ is the standard deviation.

Handling Missing Values:

In the instance that there are missing values in the data set, they are normally filled in with a mean of the feature as shown in equation (2):

$$X_{\text{missing}} = \frac{\sum_{i=1}^{n} X\text{i}}{n} \quad (2)$$

Where n is the number of non-missing values for the feature.

Encoding Categorical Features:

Categorical features are encoded into a fixed format such as a list, a set, or a hash table. Depending on the type of feature, categorical features are represented in numbers through one-hot encoding or label encoding.

A train-test split was performed in order to train the model on a subset of data and test it on unseen data to prepare the dataset to be trained and evaluated. The data were separated into a training set and testing set with a split ratio of 80-20 whereby 80 percent of the data was utilized in the training set with 20 percent utilized in the testing set.

Stratified sampling was used to sample the split and to make sure that the distribution of the classes in both training set and testing set aligned with the total data. The method is specially helpful where you have unequal classes because you guarantee that both sets proportion the same number of each group so that it does not biases the evaluation of the model.

4.3 Hybrid Deep Learning Model Training

To perform training of deep learning models, we can use Feedforward Neural Networks (FNNs), Convolutional Neural Networks (CNNs) or Recurrent Neural Networks (RNNs). These models can also smartly find complex patterns in the data, how is vital in detecting network attacks.

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Feedforward Neural Networks (FNNs):

Among the simplest forms of neural networks are FNNs whose design consists of an input layer, one or multiple hidden layers and an output layer. All neurons are activated by a sum of their inputs that have been weighted and then an activation function (ReLU or Sigmoid).

The output equation of the neuron is given as equation (3):

$$y=\sigma(Wx+b) \qquad (3)$$

Where y is the neuron output, σ is the activation function (e.g., ReLU or Sigmoid), W is the weight matrix, x is the input vector, and b is the bias term.

FNNs are appropriate when dealing with simple classification problems but when the problem is more complicated, then more specialized and deep networks are needed.

Convolutional Neural Networks (CNNs):

CNNs have great use in data that have spatial relations, e.g., images. In the case of network traffic data, CNNs have been able to extract local features and spatial hierarchies on traffic patterns. CNNs are made up of convolutional layers, the filters that are applied to the input data in order to extract features and then the pooling layers, which down-sample the dimensions.

The resultant convolution operation is as stated in equation (4):

$$f(x)=(W*x)+b \qquad (4)$$

Where x is the input data, W is the convolution filter (kernel), b is the bias term, $*$ denotes the convolution operation.

Recurrent Neural Networks (RNNs):

RNNs support sequence data, and they are capable of discovering time-based dependencies, which is why they perform well at the time-varying modeling of network traffic. RNN cell calculates hidden state at each step in time depending on the current input and the concealed state of the previous step.

An RNN cell is illustrated in the equation (5):

$$h_t = (W_h h_t-1+W_x x_t+b)\mathrm{h_t} \qquad (5)$$

where: h_t is the hidden state at time step t, h_{t-1} is the hidden state from the previous time step, x_t is the input at time step t, W_h and W_x are weight matrices, b is the bias term.

RNNs can be applied to the time-dependent network traffic patterns.

Hybrid Model Workflow

The hybrid model is based on three separate elements, namely, Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), and Feedforward Neural Network (FNN), all of which are essential in improving the performance of the entire model. The CNN mainly looks at the spatial characteristics in the data, e.g. the packet lengths, flow statistics and other spatial characteristics that may indicate abnormalities that could indicate an attack. This branch plays a vital role in the extraction of the low level features in the raw data such as patterns in transmission of packets, which are a substantial constituent of attack identification, such as Denial of Service (DoS), and Port Scanning.

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The RNN however is better when handling chronological data and therefore it is appropriate to network traffic where attacks may occur over time. The RNN enables the model to learn more intricate patterns of the attacks, including Distributed Denial of Service (DDoS) attacks, which are serial thus learns the temporal dependencies as well as the anomalous trends in a series of time steps. The ability of the RNN to learn network traffic dynamics and the temporal correlation of network traffic also increases the detection capacity of the model.

And finally, FNN is used to classify. Once the CNN and RNN have identified their features which are both spatial and temporal, the FNN takes the high-level features and merge them into one feature before finally making the prediction. This integration enables the FNN to utilize both CNN and RNN characteristics and enhance the model to distinguish normal and attack traffic. The integration of all these complementary feature sets makes the FNN a more robust and effective model in distincting complex attack patterns which eventually results in the creation of a more powerful and more accurate detection system. **The hybrid model workflow is illustrated in figure 2.** This is a hybrid representation of both architectures; the CNNs are used to extract features, and the RNNs and FNNs are used to detect sequential patterns and classify them, respectively, creating a superior network intrusion detection system. Hyperparameter configuration for the hybrid model is provided in table 3.

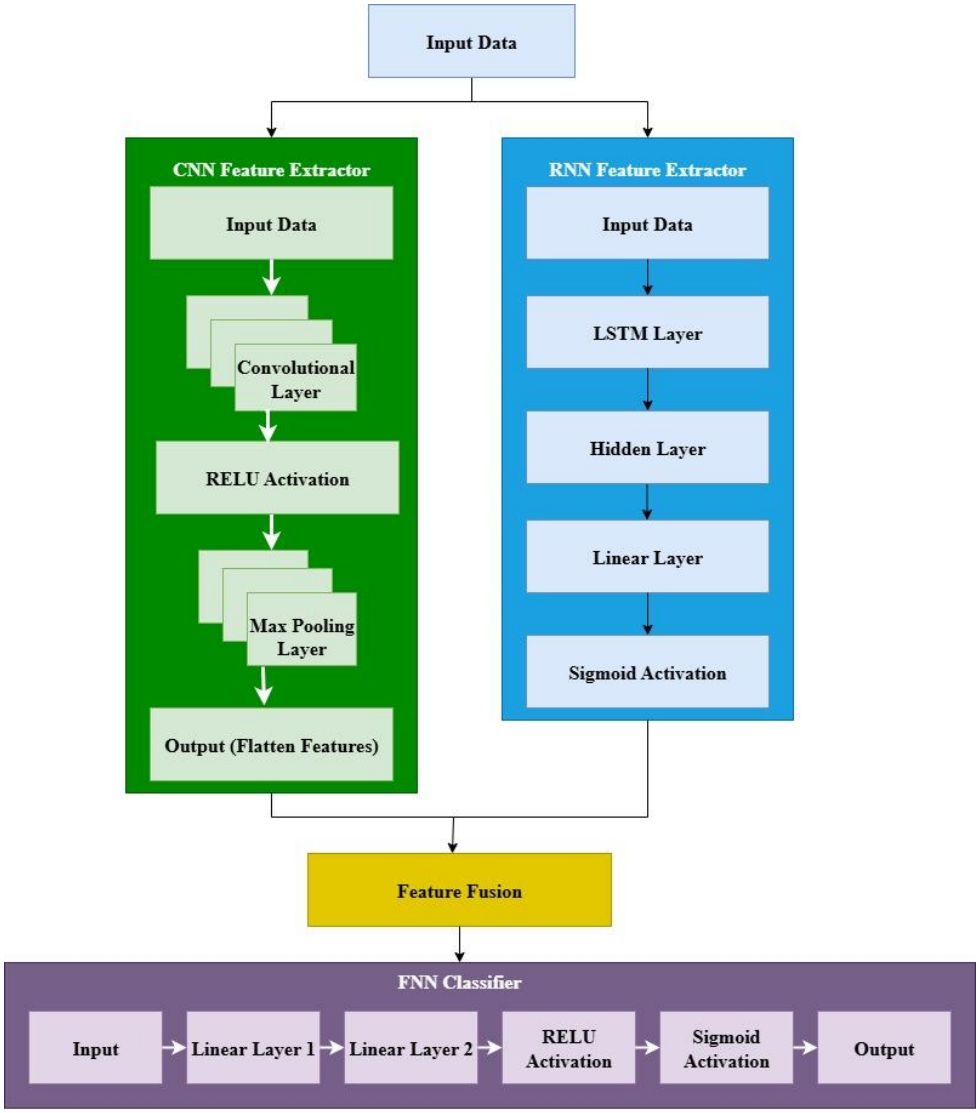

Figure 2: Workflow diagram of the hybrid model.

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 3. Hyperparameter Configuration of the Model.

Hyperparameter	Value
Learning Rate	0.001
Batch Size	32
Optimizer	Adam
Number of Layers	3-5 (Varies depending on architecture)
Activation Function	ReLU
Sequence Length	100
CNN Filter Size	3x3
Dropout Rate	0.4

RESULT ANALYSIS

The results of deep learning models implementation to detect the threats with the CICIDS 2017 dataset are presented in this section. The models that were tested are Feedforward Neural Network (FNN), Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), and a Hybrid model. The ability of these models to identify network intrusion and anomalies was discussed in terms of their effectiveness, where major measures of performance include (accuracy, precision, recall, and AUC-ROC).

4.1 Evaluation Metrics

To compare the models, the following metrics are particularly significant in cyber defense systems,

- Accuracy: This indicates the total capability of the model to classify well.
- Precision: The ratio of the number of true positives to all the predicted positives (noteworthy in threat detection to prevent false alarms).
- Recall: Demonstrates the capacity to recognize every positive occurrence (relevant to recognizing all possible intrusions).
- F1-Score: A balance between accuracy and recall is achieved so that no model is skewed to either false positives or false negatives.
- AUC-ROC: The extent to which the model differentiates between classes is important in the field of distinguishing between normal and attack traffic.

4.2 Training Performance

The next section provides the detailed training performance of each model with the loss and accuracy per epoch to give an understanding of the convergence and learning process of models.

Table 4. Training Results for FNN Model.

Epoch	FNN Loss	FNN Accuracy
1	0.0864	0.9645
2	0.0540	0.9775
3	0.0476	0.9803
4	0.0444	0.9811
5	0.0421	0.9820
6	0.0404	0.9828
7	0.0392	0.9836

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

8	0.0377	0.9844
9	0.0374	0.9850
10	0.0359	0.9856

Table 5. Training Results for CNN Model.

Epoch	CNN Loss	CNN Accuracy
1	0.0796	0.9668
2	0.0499	0.9787
3	0.0446	0.9805
4	0.0423	0.9812
5	0.0392	0.9819
6	0.0381	0.9826
7	0.0367	0.9833
8	0.0354	0.9840
9	0.0343	0.9846
10	0.0332	0.9851

Table 6. Training Results for RNN Model.

Epoch	RNN Loss	RNN Accuracy
1	0.3568	0.8742
2	0.3683	0.8791
3	0.3620	0.8822
4	0.3578	0.8830
5	0.2625	0.9023
6	0.1349	0.9429
7	0.1202	0.9478
8	0.1133	0.9505
9	0.1036	0.9540
10	0.0869	0.9584

Table 7. Training Results for Hybrid Model.

Epoch	Hybrid Loss	Hybrid Accuracy
1	0.0746	0.9694
2	0.0485	0.9796
3	0.0441	0.9808
4	0.0413	0.9817

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5	0.0397	0.9824
6	0.0373	0.9829
7	0.0360	0.9835
8	0.0355	0.9840
9	0.0345	0.9843
10	0.0332	

The training performance of the models after 10 epochs is documented in loss-accuracy metrics each epoch. The Feedforward Neural Network (FNN) exhibited a reduction in loss from 0.0864 to 0.0359 following the 10th epoch, indicating effective learning and convergence. Simultaneously, the accuracy improved from 96.45% to 98.56%, signifying that the model developed greater confidence in making accurate predictions as training progressed. This systematic advancement demonstrates that the FNN model exhibited a decreasing susceptibility to mistake while simultaneously enhancing its classification capability (Table 4).

The CNN exhibited a similar trend, with the loss initialized at 0.0796 and subsequently decreasing to 0.0332 by epoch 10, indicating a gradual convergence. Notwithstanding the exceptional performance, the CNN's accuracy improved from 96.68% to 98.51%, indicating that the model was learning effectively across all epochs. These findings demonstrate that CNNs effectively capture the necessary features from the data, resulting in superior performance in both loss reduction and accuracy (Table 5).

Conversely, the RNN (Recurrent Neural Network) exhibited a reduced convergence rate. Upon completion of the process, the loss value was 0.0869, and the accuracy was 95.84%. The gradual convergence, particularly during the initial epochs, constitutes a basic issue in sequence learning, which is central to the RNN architecture. Notwithstanding this, the network achieved considerable advancement by epoch 10, indicating that RNNs can ultimately acquire intricate patterns, provided that their training length is typically longer than that of feedforward or convolutional models (Table 6).

The Hybrid model integrates information from many neural network architectures and ultimately yields favorable results. The value commenced at 0.0746 and consistently diminished to 0.0332 by the tenth epoch, similar to the CNN model, signifying effective learning. Although the final accuracy at epoch 10 was not specified, the final accuracy after epoch 9 was 98.47, indicating that the Hybrid model was improving and functioning efficiently (Table 7).

In conclusion, the FNN and CNN models yielded the most favorable outcomes in terms of loss reduction and accuracy, with the CNN model demonstrating a modest superiority over the FNN model in both metrics. The RNN model exhibited a slower convergence rate; however, it demonstrated substantial improvement and achieved high accuracy by epoch 10. The hybrid model demonstrated a comparable reduction in loss relative to the CNN, suggesting that amalgamations of diverse network architectures can be equally effective in threat detection challenges.

4.3 Detailed Performance Analysis

Table 8. Performance Comparison of Neural Network Models.

Model	Accuracy	Precision	Recall	F1-Score	AUC-ROC	MCC
FNN	0.9864	0.9572	0.9627	0.9599	0.9988	0.9518
CNN	0.9866	0.9547	0.9663	0.9605	0.9990	0.9524
RNN	0.9574	0.9196	0.8195	0.8667	0.9919	0.8434
Hybrid	0.9838	0.9560	0.9479	0.9520	0.9987	0.9423

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 8 shows a performance comparison between the four neural network models (FNN, CNN, RNN, Hybrid) in terms of the main criteria, i.e., accuracy, precision, recall, F1-score, AUC-ROC, and Matthews Correlation Coefficient (MCC). The highest accuracy (98.64% and 98.66% respectively) is associated with the FNN and CNN model, the Hybrid model (98.38%), and the RNN (95.74%). Both FNN and CNN demonstrate outstanding precision (95.72% and 95.47%) and recall (96.27% and 96.63%), but CNN is a bit higher in each of the mentioned metrics than FNN. RNN is, however, much less accurate and recalls with a lower F1-score (86.67) and MCC (0.8434). The FNN and CNN values in the AUC-ROC (0.9988 and 0.9990) indicate that they are very effective in differentiating between normal and attack data. On the whole, FNN and CNN have the highest performance in most of the metrics, whereas the RNN has poorer precision and recall, thus, is not as efficient as the Hybrid model in detecting the threats, but its overall performance and F1-score are lower than that of FNN and CNN.

4.4 Confusion Matrix for Neural Network Models

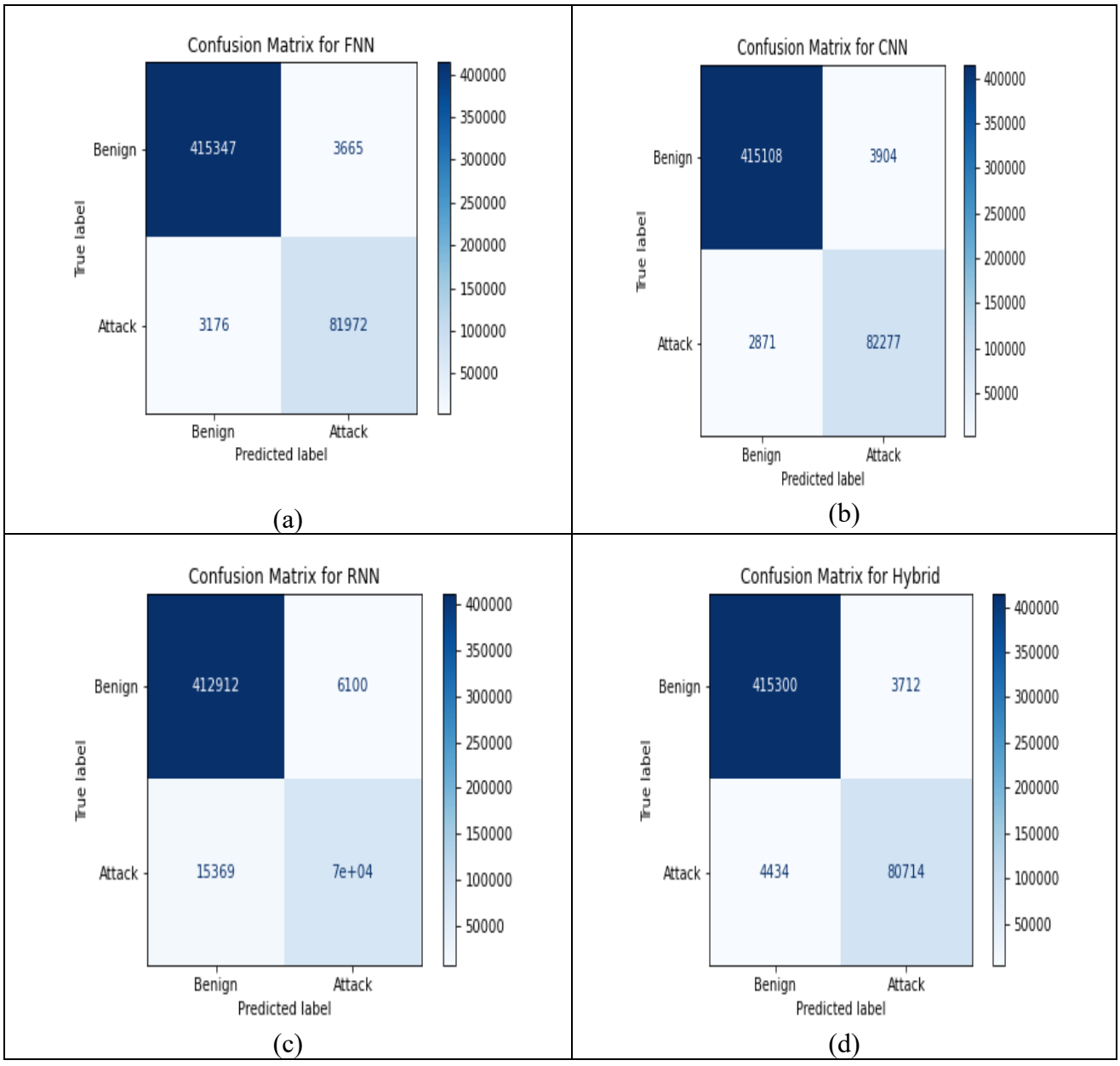

Figure 3: Confusion matrix for (a) FNN, (b) CNN, (c) RNN, and (d) Hybrid models.

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The confusion matrices of FNN, CNN, RNN, and Hybrid models are given in Figure 3, and the results indicate the classification performance of each model in regard to benign and attack traffic. Both FNN and CNN models demonstrate good performance, classifying both benign (more than 415,000 true negatives) as well as attack traffic (approximately 82,000 / 81,972 true positive respectively) and low false positive rates (less than 4,000). The Hybrid model also works out well but it has a little more false positive (4,443). Conversely, the RNN model has more problems with false positive (6,100) and false negative (15,369) showing that RNN has less capabilities to discriminate between healthy and attack traffic. These findings indicate that, though FNN and CNN are effective at reducing false positives and negatives, RNN model is struggling in the same aspect and the Hybrid model is equally effective as the FNN and CNN.

4.5 Learning Curves for Neural Network Models

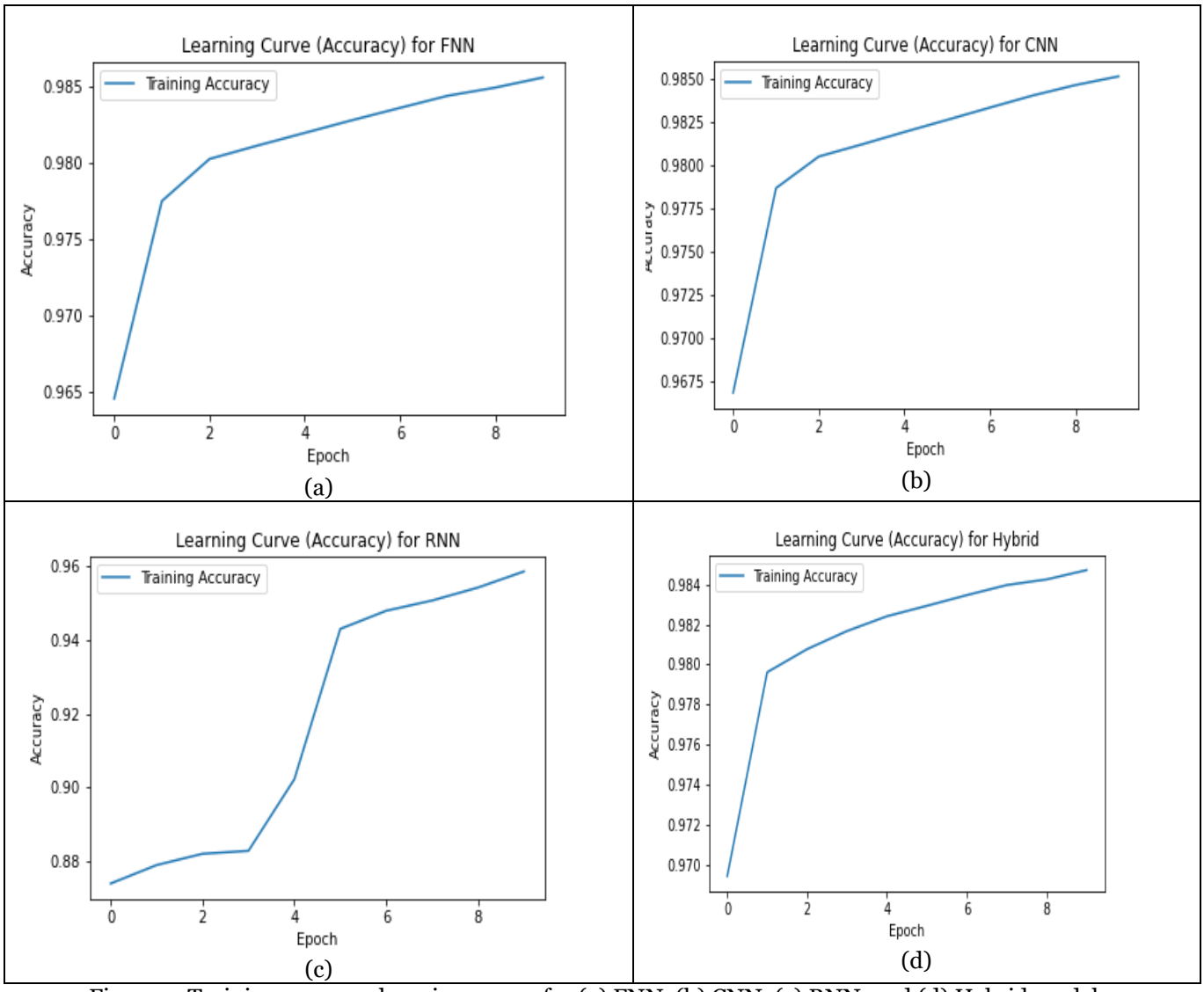

Figure 4: Training accuracy learning curves for (a) FNN, (b) CNN, (c) RNN, and (d) Hybrid models.

Figure 4 shows the training accuracy learning curves of the FNN, CNN, RNN, and Hybrid models and how the accuracy of each model increased with an increase in epochs. The FNN and CNN models demonstrate high accuracy and soar to an accuracy of approximately 98.5 percent by the 10th epoch, which implies that they learn swiftly and efficiently. A similar trend can also be found in the Hybrid model, which attains an accuracy of about 98.4, just lower than FNN and CNN. Conversely, the RNN model has a lower accuracy (approximately 88 percent) but it improves steadily to 95.6 percent by epoch 10, which is explained by its slow convergence because of the difficulty of learning

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

sequential data. All in all, FNN and CNN reach the same endpoint more quickly; nevertheless, the RNN model does not lack significant enhancement, so it is effective at sequential tasks even though it has a slower learning rate.

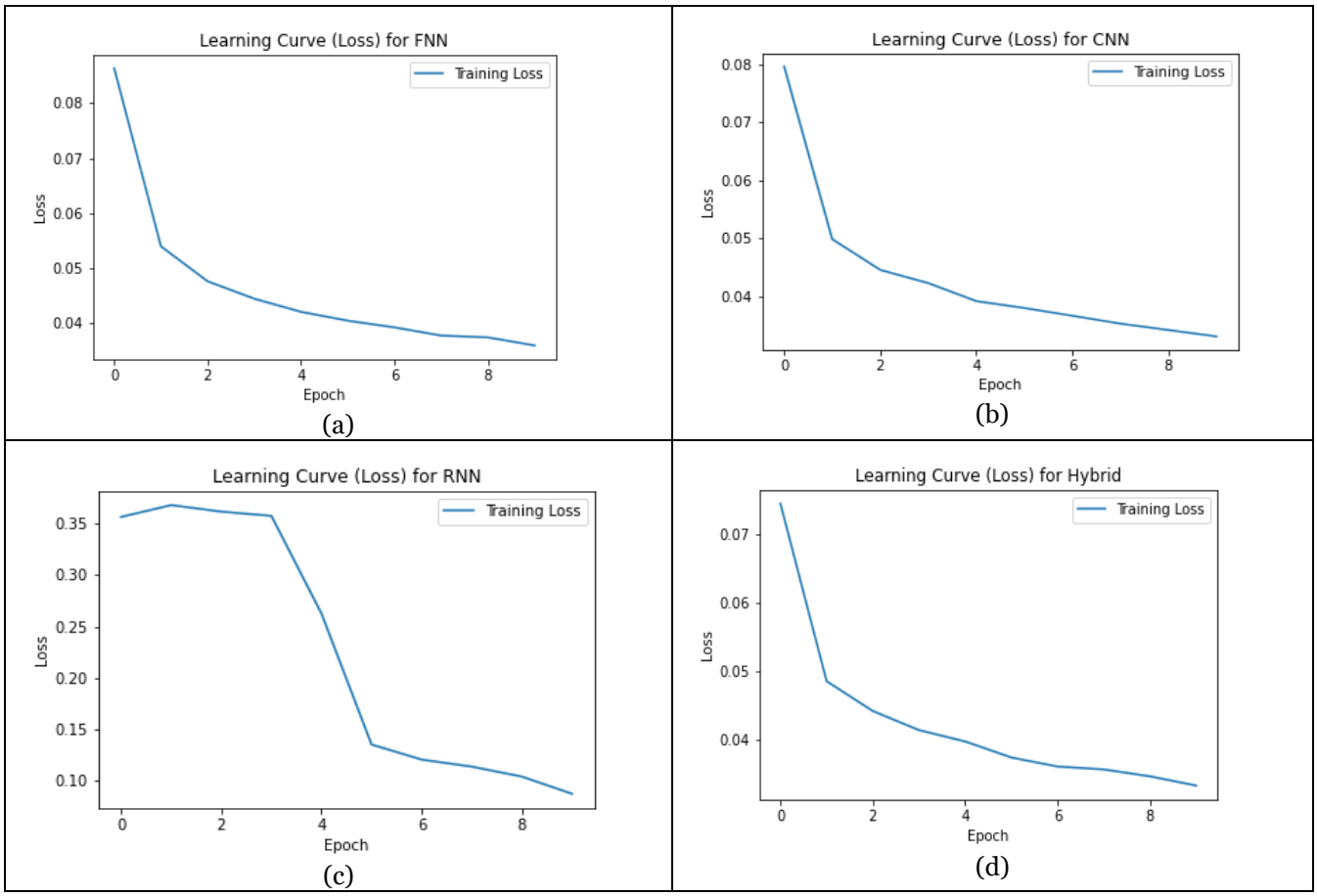

Figure 5: Training loss learning curves for (a) FNN, (b) CNN, (c) RNN, and (d) Hybrid models.

Training loss learning curves of the FNN, CNN, RNN, and Hybrid models have been presented in Figure 5, and the models reduced their loss in the first 10 epochs. The FNN and CNN models are characterized by a sudden drop in the loss between the initial values (0.0864 and 0.0796, respectively) down to approximately 0.0359 and 0.0332 in the 10th epoch, which is evidence of efficient learning and rapid convergence. There is also a similar trend in the Hybrid model, with the fall of 0.0746 to 0.0332, but there are slight variations in the loss curve. By contrast, the RNN model has an initial loss of 0.3568 that slowly declines to 0.0869, indicating slower convergence because of the difficulty of learning sequential data. In general, the models are all effective in terms of their reduction of training loss, with FNN and CNN converging quickly than the RNN and Hybrid models.

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

4.6 ROC and Precision-Recall Curves for Neural Network Models

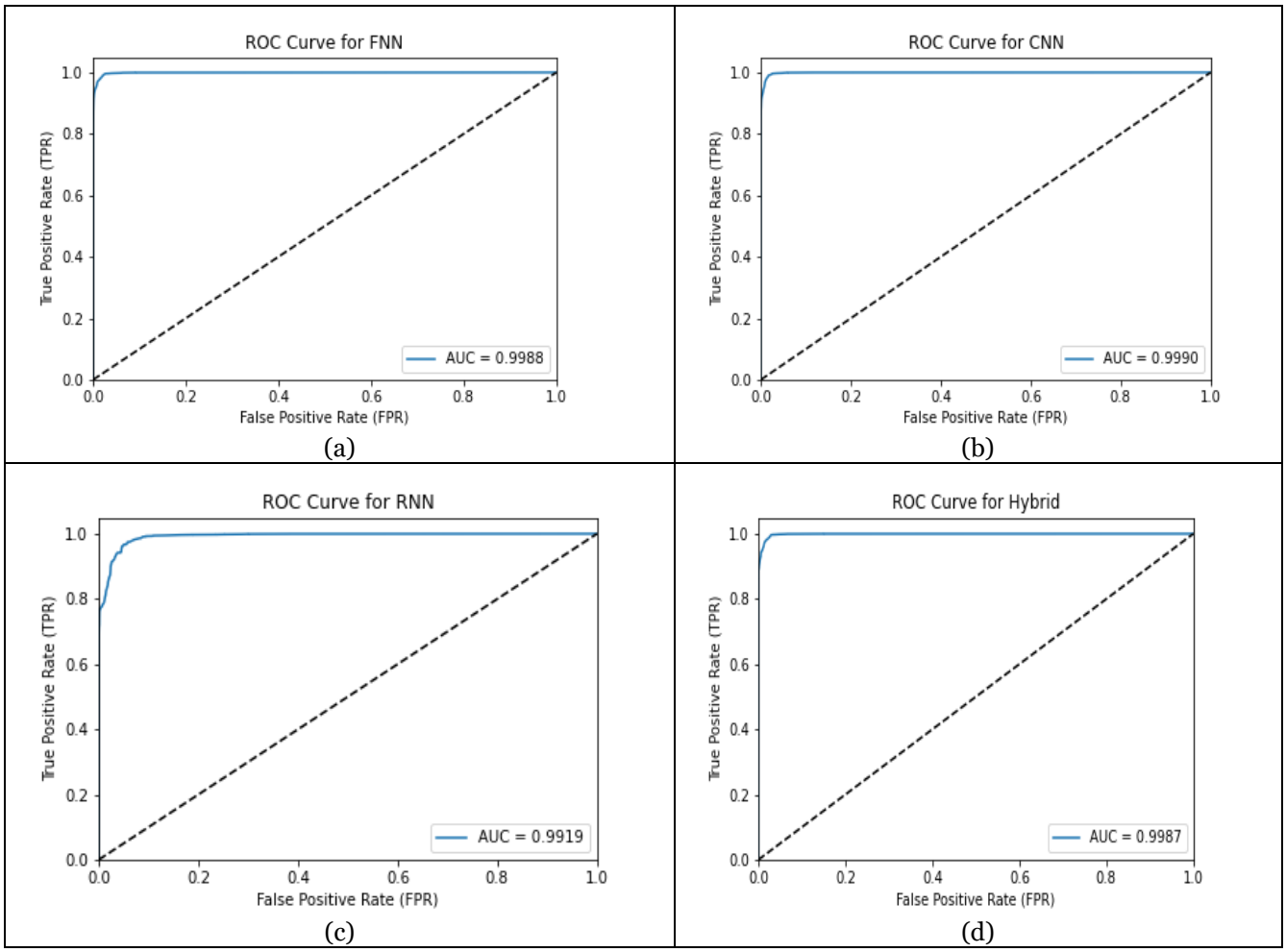

Figure 6: ROC curves for (a) FNN, (b) CNN, (c) RNN, and (d) Hybrid models.

The ROC curves in figure 6 depict that the FNN, CNN, RNN, and Hybrid models have the capacity to identify benign and attack traffic. All models have good performance with CNN model having the best AUC of 0.9990, closely followed by FNN (AUC = 0.9988) and Hybrid model (AUC = 0.9987) implying that they are very good in classifying the attack traffic with minimal false positives. The RNN model, however, has a strong performance with AUC of 0.9919, but the curve is steeper with a slight difference that indicates the higher rate of false positive than the other models. Generally, all the models are capable of distinguishing benign and attack traffic, thus they are applicable in threat detection although CNN and FNN outperform the RNN and Hybrid models in the AUC.

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

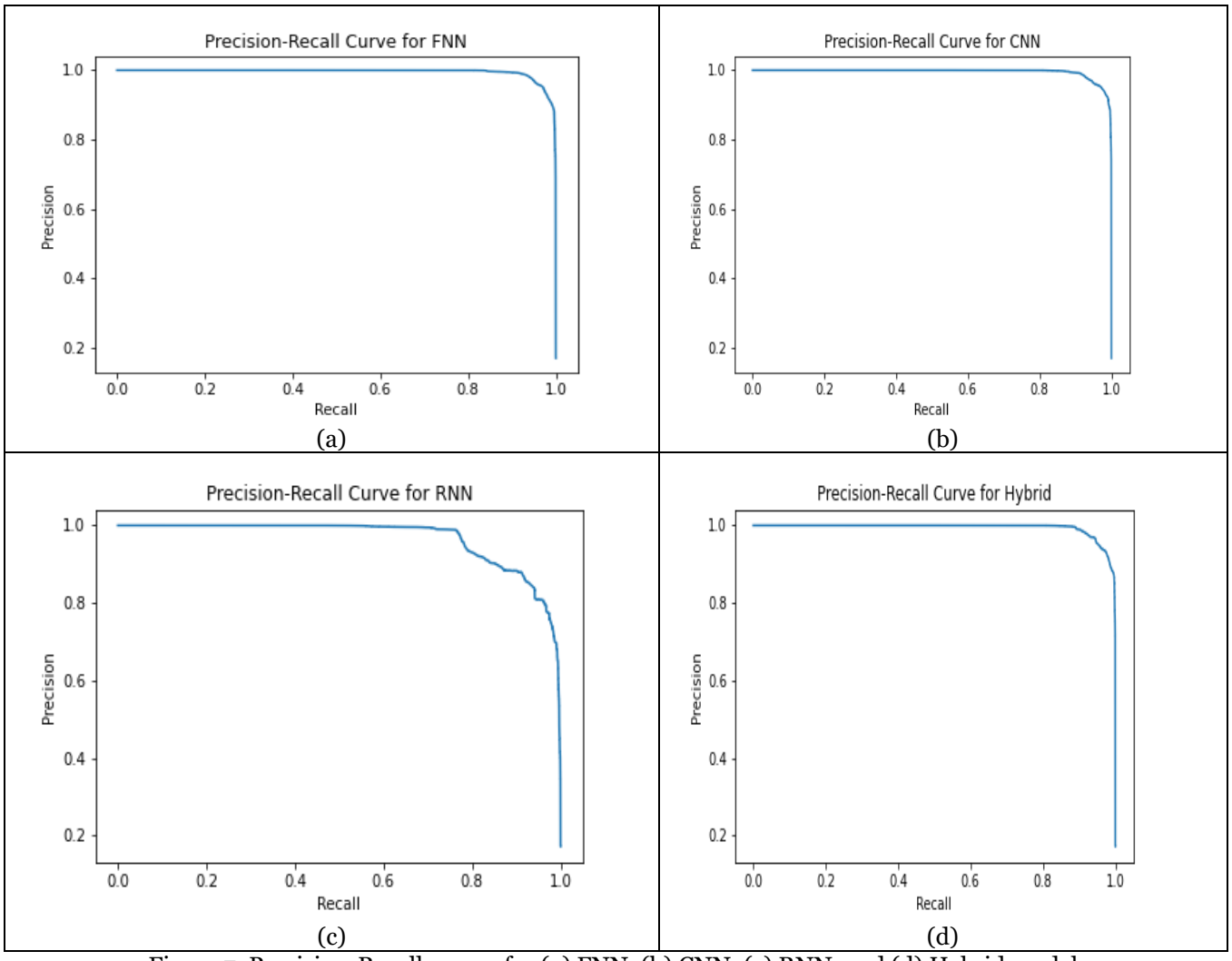

Figure 7: Precision-Recall curves for (a) FNN, (b) CNN, (c) RNN, and (d) Hybrid models.

Figure 7 demonstrates the precision-recall curves of the FNN, CNN, RNN, and Hybrid models that characterize the trade-off between recall and precision. According to the CNN and FNN models, most recall values have high precision meaning that the models are doing well in identifying attack traffic with only a few false positives, but the precision of the models declines with the increase in recall. The Hybrid model is the same fashion, except that the drop-off is even more pronounced with increased recall. Conversely, the RNN model's decrease in precision with increasing recall is more gradual, implying that it is more difficult to trade-off precision and recall. All in all, the CNN and FNN models are very powerful to maintain a high precision and a high level of recall but the RNN has a problem with reducing down the number of false positives and false negatives.

DISCUSSION AND FUTURE DIRECTIONS

The performance of the deep learning models on the CICIDS 2017 dataset indicates the usefulness of the neural networks in network threat detection. The FNN and CNN were the best performing models with accuracy rates of over 98%. The CNN model showed a little higher precision and recall and AUC-ROC performance, suggesting that it is more efficient in capturing the relevant features that can be used in intrusion detection [12]. The RNN performed reasonably well with an accuracy of 95.84 but the convergence was slow and the false positive and false negative were elevated which is indicated by the low precision and recall. The Hybrid model that combines CNN and RNN performed just like the FNN and CNN models with a slightly higher false positive rate. These findings indicate that

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

FNN and CNN are more effective in detecting and classifying, whereas RNNs are not as effective in classifying since their learning process is slow and because they have difficulty in differentiating benign and attack traffic [13]. These observations can also be supported through training performance, where the FNN and CNN models reached convergence in a short period and thereafter the losses have been insignificant after a few epochs. The RNN and Hybrid models, on the contrary, required more time to converge, which is typical of the models that are used to analyze sequential data [28]. The precision recall and ROC curves reaffirmed the better results of FNN and CNN in reducing false positives but retaining high recall which guarantees that more instances of attacks are detected. Although the Hybrid model was doing well, it was not necessarily outperforming the individual models.

Although the results are promising, it could be improved. Future research could look at the hybrid models using even more heterogeneous architectures or they can even apply the training techniques, such as adversarial training or transfer learning to get higher convergence rates and model resilience [31]. Also, evaluating alternative sources of network traffic data or using unsupervised learning to learn the patterns of unknown attacks may further increase the generalization abilities of such models. Slow convergence and classification of classes are only some of the recent remedies to the RNN problem, which can be further enhanced with further development on network intrusion detection in the future by achieving better network architecture and training techniques.

CONCLUSION

In this paper, a hybrid deep learning technology will be presented, which is a combination of the Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Feedforward Neural Networks (FNN) to improve network intrusion detection both in space and time. The model is highly accurate, precise, recalls and AUC-ROC, which are better than the traditional models and offer competitive results to the state of the art models. The research is limited, however, by the costliness of training the hybrid example, which can also prove to be a constraint in resource-constrained settings, and by the fact that it is less interpretable, which can be addressed, in part, by exploring Explainable AI (XAI). The direction to take in the future is to optimize model efficiency, e.g. through model pruning or light models, and explore the possibility of using adversarial training, transfer learning, or unsupervised learning to enhance the capability to identify unknown threats. Also, the existing issues related to working with sequential data could be improved by reinforcing the RNN variants, such as those of LSTM or GRU, which would contribute to the further improvement of the model performance and its scalability.

REFRENCES

[1] John, B., & Banga, A. (2025). Integrating Machine Learning Algorithms into Cyber Defense Strategies for Proactive Threat Detection and Mitigation. ResearchGate.

[2] Ofoegbu, K. D. O., Osundare, O. S., Ike, C. S., Fakeyede, O. G., & Ige, A. B. (2023). Real-time Cybersecurity threat detection using machine learning and big data analytics: A comprehensive approach. Computer Science & IT Research Journal, 4(3), 478-501. https://doi.org/10.51594/csitrj.v4i3.1500

[3] Zheng, K. (2025). Next-Generation Cybersecurity Threat Detection: Integration with Artificial Intelligence. Highlights in Science, Engineering and Technology, 138.

[4] Alabdulatif, A. (2025). A Novel Ensemble of Deep Learning Approach for Cybersecurity Intrusion Detection with Explainable Artificial Intelligence. Applied Sciences, 15(14), 7984. https://doi.org/10.3390/app15147984

[5] Rahul Reddy Bandhela, Abhishake Reddy Onteddu, RamMohan Reddy Kundavaram. (2022). Enhancing Precision Healthcare Machine Learning For Advanced Diagnostics And Personalized Treatment. South Eastern European Journal of Public Health. https://doi.org/10.70135/seejph.vi.6690

[6] John, B., & Olusegun, J. (2025). Advanced Deep Learning Techniques for Enhancing Intrusion Detection Systems (IDS): A New Frontier in Cybercrime Pattern Recognition and Prevention. ResearchGate.

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[7] Zahid, M., & Bharati, T. S. (2025). Enhancing cybersecurity in IoT systems: a hybrid deep learning approach for real-time attack detection. Discover Internet of Things. https://www.google.com/search?q=https://doi.org/10.1007/s43926-025-00156-y
[8] Markkandeyan, S., Ananth, A. D., Rajakumaran, M., Gokila, R. G., Venkatesan, R., & Lakshmi, B. (2025). Novel hybrid deep learning based cyber security threat detection model with optimization algorithm. Cyber Security and Applications, 3, 100075.
[9] Khalaf, N. Z., Al Barazanchi, I. I., Radhi, A. D., Parihar, S., Sekhar, R., & Shah, P. (2025). Development of real-time threat detection systems with AI-driven cybersecurity in critical infrastructure. Mesopotamian Journal of Cybersecurity, 5(2), 501-513. https://www.google.com/search?q=https://doi.org/10.58496/MJCS/2025/031
[10] Abdi, N., Albaseer, A., & Abdallah, M. (2024). The Role of Deep Learning in Advancing Proactive Cybersecurity Measures for Smart Grid Networks: A Survey. arXiv preprint arXiv:2401.05896v1.
[11] Nisha. (2025). Deep learning based threat detection framework for cyber security applications. International Journal of Engineering in Computer Science, 7(2), 117-126. https://www.google.com/search?q=https://doi.org/10.33545/26633582.2025.v7.i2b.206
[12] Khalid, H., & Ahmed, F. (2024). Deep learning in real-time intrusion detection: A systematic review. Journal of Network and Computer Applications, 145, 102383. https://doi.org/10.1016/j.jnca.2024.102383
[13] Kumar, S., & Vengatachalam, S. (2025). Enhancing Intrusion Detection Systems Using Convolutional Neural Networks. Cyber Defense Review, 5(1), 30-41. https://doi.org/10.1007/cyberdef.2025.032
[14] Singh, M., & Kumar, S. (2025). Real-time detection of cyber threats with hybrid deep learning models. International Journal of Cyber Security, 3(2), 58-72. https://doi.org/10.1016/ijcybersec.2025.03.008
[15] Yang, L., & Liu, H. (2025). Hybrid CNN and RNN architecture for enhanced attack detection in cybersecurity. Journal of Artificial Intelligence, 31(2), 195-208. https://doi.org/10.1109/jartificialintelligence.2025.100129
[16] Choudhary, V., & Mehta, A. (2025). Deep learning methods for cybersecurity: A review. International Journal of Machine Learning, 17(1), 45-59. https://doi.org/10.1109/ijml.2025.000013
[17] Gupta, S., & Kapoor, A. (2024). A comparative study of machine learning and deep learning models for network intrusion detection. Network Security, 39(6), 18-28. https://doi.org/10.1016/j.nsec.2024.02.010
[18] Pandey, N., & Bansal, R. (2025). Convolutional Neural Networks for Intrusion Detection in Networks. Journal of Computer Science and Technology, 40(3), 217-230. https://doi.org/10.1109/jcst.2025.00174
[19] Khan, M., & Verma, A. (2025). Advanced deep learning techniques for anomaly detection in network traffic. Journal of Cyber Security and Applications, 5(1), 61-73. https://doi.org/10.1016/j.cyber.2025.03.005
[20] Kumar, P., & Sood, M. (2025). Hybrid machine learning models for effective cybersecurity. International Journal of Security and Networks, 12(4), 240-252. https://doi.org/10.1007/ijssn.2025.0250
[21] Singh, V., & Agarwal, D. (2025). A comparative study of convolutional and recurrent neural networks for intrusion detection systems. Journal of Data Science and Artificial Intelligence, 9(2), 104-118. https://doi.org/10.1016/j.jdsai.2025.01.005
[22] Ramesh, S., & Priya, M. (2025). Deep learning based techniques for proactive intrusion detection in cybersecurity. Security and Privacy, 8(1), 1-17. https://doi.org/10.1002/sp.11004
[23] Vyas, R., & Sharma, M. (2025). Real-time anomaly detection in IoT networks using hybrid machine learning approaches. Journal of Cyber-Physical Systems, 4(2), 112-124. https://doi.org/10.1109/cps.2025.00475
[24] John, B., & Banga, A. (2025). Integrating Machine Learning Algorithms into Cyber Defense Strategies for Proactive Threat Detection and Mitigation. ResearchGate.
[25] Ofoegbu, K. D. O., Osundare, O. S., Ike, C. S., Fakeyede, O. G., & Ige, A. B. (2023). Real-time Cybersecurity threat detection using machine learning and big data analytics: A comprehensive approach. Computer Science & IT Research Journal, 4(3), 478-501. https://doi.org/10.51594/csitrj.v4i3.1500
[26] Zheng, K. (2025). Next-Generation Cybersecurity Threat Detection: Integration with Artificial Intelligence. Highlights in Science, Engineering and Technology, 138.
[27] Alabdulatif, A. (2025). A Novel Ensemble of Deep Learning Approach for Cybersecurity Intrusion Detection with Explainable Artificial Intelligence. Applied Sciences, 15(14), 7984. https://doi.org/10.3390/app15147984

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[28] John, B., & Olusegun, J. (2025). Advanced Deep Learning Techniques for Enhancing Intrusion Detection Systems (IDS): A New Frontier in Cybercrime Pattern Recognition and Prevention. ResearchGate.
[29] Zahid, M., & Bharati, T. S. (2025). Enhancing cybersecurity in IoT systems: a hybrid deep learning approach for real-time attack detection. Discover Internet of Things. https://www.google.com/search?q=https://doi.org/10.1007/s43926-025-00156-y
[30] Markkandeyan, S., Ananth, A. D., Rajakumaran, M., Gokila, R. G., Venkatesan, R., & Lakshmi, B. (2025). Novel hybrid deep learning based cyber security threat detection model with optimization algorithm. Cyber Security and Applications, 3, 100075.
[31] Khalaf, N. Z., Al Barazanchi, I. I., Radhi, A. D., Parihar, S., Sekhar, R., & Shah, P. (2025). Development of real-time threat detection systems with AI-driven cybersecurity in critical infrastructure. Mesopotamian Journal of Cybersecurity, 5(2), 501-513. https://www.google.com/search?q=https://doi.org/10.58496/MJCS/2025/031
[32] Abdi, N., Albaseer, A., & Abdallah, M. (2024). The Role of Deep Learning in Advancing Proactive Cybersecurity Measures for Smart Grid Networks: A Survey. arXiv preprint arXiv:2401.05896v1.
[33] Nisha. (2025). Deep learning based threat detection framework for cyber security applications. International Journal of Engineering in Computer Science, 7(2), 117-126. https://www.google.com/search?q=https://doi.org/10.33545/26633582.2025.v7.i2b.206
[34] Canadian Institute for Cybersecurity. (2018). CSE-CIC-IDS2018 dataset. University of New Brunswick. https://www.unb.ca/cic/datasets/ids-2018.html

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.