Indonesian Journal of Electrical Engineering and Computer Science
Vol. 43, No. 3, September 2026, pp. 792~807
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v43.i3.pp792-807

Network anomaly detection using hybrid deep learning framework

Razibul Islam Khan, Md. Imran Hossain, Hridoy Mohonto, Md. Asmaul Haque, Anwar Parvez Rony, Fazle Rabbi
Department of Computer Science and Engineering, Faculty of Science and Engineering, City University, Savar, Bangladesh

Article Info

Article history:

Received Feb 10, 2026
Revised Jun 22, 2026
Accepted Jun 29, 2026

Keywords:

Anomaly detection
Cybersecurity
Deep learning
Intrusion detection system
Neural networks

ABSTRACT

Network anomaly detection has become increasingly important as modern communication networks face sophisticated and evolving cyber threats that cannot be effectively identified using conventional signature-based intrusion detection systems. Deep learning has demonstrated significant potential for detecting complex attack patterns; however, individual architectures often exhibit limitations in capturing diverse characteristics of network traffic. This paper proposes TriFusion-Net, a hybrid deep learning framework that integrates convolutional neural networks (CNN), long short-term memory (LSTM)-based recurrent neural networks (RNN), and feedforward neural networks (FNN) to improve flow-based network anomaly detection. CNN is employed to extract local spatial patterns from network flow features, LSTM models sequential feature dependencies, and the FNN classifier performs nonlinear decision making for binary intrusion classification. The proposed framework is evaluated using the CIC-IDS-2018 benchmark dataset containing large-scale benign and malicious network traffic. A unified preprocessing pipeline, including data cleaning, feature selection, normalization, and class balancing, is adopted to ensure robust model training and evaluation. Experimental results demonstrate that TriFusion-Net achieves an overall accuracy of 95.66%, with 87.88% precision, 94.99% recall, 91.30% F1-score, and 97.75% receiver operating characteristic area under the curve (ROC-AUC), outperforming the individual deep learning models considered in this study. These results indicate that the proposed hybrid framework provides an effective and computationally efficient solution for real-time network anomaly detection in modern cybersecurity environments.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Razibul Islam Khan
Department of Computer Science and Engineering, Faculty of Science and Engineering
City University
Savar, Dhaka, Bangladesh
Email: razibislam28@gmail.com

1. INTRODUCTION

Deep learning has emerged as one of the most promising approaches for addressing the growing complexity of anomaly-based intrusion detection in modern communication networks. Unlike conventional machine learning methods that often rely on manually engineered features, deep learning models can automatically learn hierarchical feature representations from high-dimensional network traffic, enabling more effective detection of sophisticated and previously unseen cyberattacks. This capability is particularly important as network environments become increasingly heterogeneous and dynamic, rendering traditional

signature-based detection techniques less effective against evolving attack patterns. Recent advances in neural network architectures have demonstrated state-of-the-art performance across a wide range of large-scale classification and pattern recognition tasks [1]–[3], highlighting their potential for cybersecurity applications. In the context of network intrusion detection, flow-based traffic analysis has attracted considerable attention because it captures essential communication characteristics while reducing computational overhead and preserving user privacy compared with payload-based inspection [4]. Building upon these developments, this study investigates the effectiveness of hybrid deep learning models by exploring flow-based network features and evaluating multiple neural architectures within a unified experimental framework. The objective is to leverage the complementary strengths of different deep learning paradigms to improve anomaly detection performance, enhance generalization capability, and provide a robust solution for identifying malicious network activities under realistic operating conditions.

Despite their widespread deployment, conventional intrusion detection systems (IDSs) face several limitations that reduce their effectiveness in modern network environments. Signature-based IDSs are highly effective against previously identified threats but struggle to detect zero-day attacks and rapidly evolving intrusion patterns, whereas traditional anomaly-based approaches often suffer from high false-positive rates due to their reliance on predefined thresholds and handcrafted decision rules [5]–[10]. Excessive false alarms not only increase the workload of security analysts but also diminish operational trust in IDS recommendations, thereby limiting their practical deployment in real-world cybersecurity operations [11], [12]. Furthermore, contemporary network traffic exhibits highly nonlinear, heterogeneous, and high-dimensional characteristics, where malicious behaviors are frequently concealed within complex interactions among multiple flow features rather than individual attributes. Conventional machine learning techniques often have limited capability to capture these intricate feature dependencies, resulting in reduced detection accuracy when confronted with sophisticated or previously unseen attacks [13]-[18]. From an implementation perspective, practical IDS solutions must also satisfy stringent operational requirements, including scalability for high-volume network traffic, robust and reproducible preprocessing pipelines, computational efficiency, and low-latency inference suitable for real-time deployment in enterprise and cloud environments [19]-[21]. These challenges highlight the need for advanced deep learning frameworks that not only achieve high detection performance but also maintain an appropriate balance between precision and recall while remaining computationally efficient and operationally practical [22]-[23]. Accordingly, this study addresses the following research question: How can a hybrid neural network framework be designed and evaluated to achieve robust and accurate anomaly detection on modern flow-based network datasets while preserving operationally meaningful precision–recall trade-offs for practical intrusion detection systems?

To address the aforementioned challenges, this work proposes TriFusion-Net, a hybrid deep learning framework for flow-based network anomaly detection and evaluates its performance using the widely adopted CIC-IDS-2018 benchmark dataset [3]. To ensure a fair and comprehensive assessment, four neural network architectures are implemented and trained using an identical preprocessing pipeline, as illustrated in Figure 1.

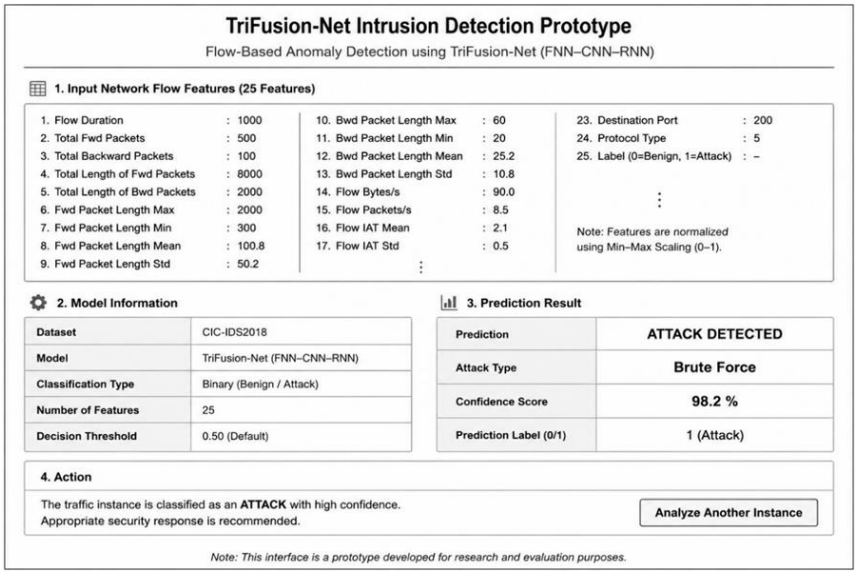


Figure 1. Solution workflow pipeline

The feedforward neural network (FNN) serves as the baseline model for learning nonlinear relationships among network flow features. A one-dimensional convolutional neural network (CNN) is employed to automatically extract discriminative local feature patterns and spatial correlations within the input feature vector through convolutional filtering. Long short-term memory (LSTM)-based recurrent neural networks (RNNs) are incorporated to capture sequential dependencies and long-range interactions among flow features by treating the feature vector as an ordered sequence, thereby exploiting the memory capability of LSTM cells to model complex feature relationships. Building upon the strengths of these individual architectures, the proposed TriFusion-Net integrates CNN, LSTM, and FNN into a unified hybrid framework that combines hierarchical feature extraction, sequential dependency learning, and nonlinear classification to improve anomaly detection performance. Beyond offline model evaluation, the trained framework is deployed within a lightweight Flask-based web application that accepts 25 network flow features as input and performs real-time inference to classify traffic as either benign or malicious. This deployment-oriented implementation demonstrates the practical applicability of the proposed framework for supporting intelligent and efficient network intrusion detection in operational cybersecurity environments.

This study aims to develop and evaluate a robust deep learning framework for flow-based network anomaly detection using neural network architectures and a standardized experimental pipeline. Specifically, the proposed framework is designed to provide a reproducible intrusion detection system based on network flow features while enabling a fair comparative analysis of four representative deep learning models, namely FNN, CNN, LSTM-based, RNN, and the proposed hybrid TriFusion-Net architecture. All models are trained and evaluated using an identical preprocessing strategy to ensure objective performance comparison. Their effectiveness is assessed using widely accepted intrusion detection metrics, including accuracy, precision, recall, F1-score, receiver operating characteristic area under the curve (ROC-AUC), and precision-recall AUC where applicable, together with an analysis of their strengths, limitations, computational characteristics, and deployment suitability. Unlike conventional signature-based intrusion detection systems, the proposed framework adopts an anomaly-based learning approach capable of recognizing previously unseen malicious behaviors by exploiting discriminative flow-level characteristics [4]. To enhance model robustness and reproducibility, a unified preprocessing pipeline incorporating feature selection, data normalization, and stable neural network training is employed using 25 representative network flow features. Furthermore, the practical applicability of the proposed approach is demonstrated through the development of a lightweight Flask-based web application that integrates the trained model with a user-friendly interface for real-time prediction, enabling automatic classification of network traffic as either benign or malicious. Collectively, these contributions establish a comprehensive and deployment-oriented framework for evaluating hybrid deep learning techniques in modern network anomaly detection systems.

2. BACKGROUND STUDY AND LITERATURE REVIEW

2.1. Intrusion detection system

An intrusion detection system (IDS) is a cybersecurity mechanism designed to monitor computer systems or network activities in order to identify unauthorized access, malicious behavior, policy violations, or other security threats. By continuously analyzing system events and network communications, an IDS provides early warning of potential attacks and assists security administrators in responding to cyber incidents before significant damage occurs. Depending on the deployment environment and monitoring scope, IDSs are generally categorized into host-based intrusion detection systems (HIDS) and network-based intrusion detection systems (NIDS). A HIDS operates at the individual host level by monitoring operating system logs, application events, file integrity, user activities, and system calls to detect suspicious behavior occurring within a single device. In contrast, a NIDS monitors network traffic traversing communication links, routers, or switches to identify abnormal communication patterns and malicious activities affecting multiple hosts simultaneously. Modern NIDS implementations increasingly rely on flow-level analysis rather than deep packet inspection because network flow records summarize essential communication characteristics while reducing computational overhead and preserving user privacy in encrypted network environments. Owing to its scalability, efficiency, and suitability for high-speed networks, flow-based intrusion detection has become an attractive approach for protecting contemporary enterprise, cloud, and internet-of-things (IoT) infrastructures. Accordingly, this study focuses on the development of a flow-based network intrusion detection system that utilizes deep learning techniques to identify malicious traffic from representative network flow features.

2.2. Proposed system overview

This study proposes TriFusion-Net, a hybrid deep learning framework designed to improve network anomaly detection by exploiting the complementary learning capabilities of multiple neural network

architectures. The proposed system adopts a supervised learning strategy using the CIC-IDS2018 benchmark dataset, one of the largest publicly available datasets for intrusion detection research, which contains diverse benign traffic and multiple categories of contemporary cyberattacks. Within the proposed framework, a one-dimensional CNN is employed to automatically extract discriminative local feature patterns from network flow data, while an LSTM-based RNN models the sequential dependencies and complex interactions among flow features. The learned representations are subsequently processed by a FNN that performs nonlinear classification to distinguish benign and malicious network traffic. By integrating spatial feature extraction, sequential dependency learning, and nonlinear decision making into a unified architecture, TriFusion-Net aims to improve detection robustness and generalization compared with individual deep learning models. The framework is trained and evaluated using 2,762,891 network flow instances, comprising 2,210,312 training samples and 552,579 testing samples, following a standardized preprocessing pipeline to ensure consistent model comparison and reproducible experimentation. Experimental evaluation demonstrates that the proposed framework achieves an overall binary classification accuracy of 95.66%, indicating its capability to effectively detect anomalous network behavior while maintaining computational efficiency suitable for practical network intrusion detection applications. Beyond achieving competitive predictive performance, the proposed system is intended as a deployable deep learning framework that can support intelligent, scalable, and real-time cybersecurity monitoring in modern network environments.

3. METHOD

3.1. Software environment

The proposed network anomaly detection framework was implemented using the Python programming language because of its comprehensive ecosystem for scientific computing, machine learning, and deep learning research. Numerical computation and matrix manipulation were performed using the NumPy library, while Pandas was employed for data loading, preprocessing, and efficient manipulation of large-scale network flow records. The Scikit-learn library provided essential utilities for feature normalization, dataset partitioning, class balancing, and performance evaluation, ensuring a standardized experimental workflow. Deep learning models, including the FNN, CNN, LSTM-based, RNN, and the proposed TriFusion-Net architecture, were developed and trained using the TensorFlow-Keras framework, which offers optimized computational performance and flexible model construction. Visualization of experimental results, including training convergence, confusion matrices, and receiver operating characteristic (ROC) curves, was carried out using Matplotlib and Seaborn. The integration of these software libraries provides a reproducible and scalable development environment suitable for implementing and evaluating deep learning-based intrusion detection systems on large network traffic datasets.

3.2. Overall system architecture

The overall framework of the proposed intrusion detection system consists of five sequential stages: data acquisition, data preprocessing, deep learning model development, performance evaluation, and deployment for real-time inference. The workflow begins with the acquisition of network flow records from the CIC-IDS2018 benchmark dataset, followed by a comprehensive preprocessing stage that includes data cleaning, feature selection, categorical encoding, normalization, dataset partitioning, and input reshaping. These preprocessing steps ensure data consistency and improve the stability of neural network training. Subsequently, four deep learning architectures, namely FNN, CNN, LSTM-based, RNN, and the proposed hybrid TriFusion-Net, are trained using the same preprocessed dataset to facilitate an objective comparison of their detection capabilities. The trained models are then evaluated using multiple intrusion detection performance metrics, including accuracy, precision, recall, F1-score, ROC-AUC, and precision-recall AUC. Finally, the best-performing model is integrated into a lightweight web-based application for real-time network traffic classification. The complete workflow of the proposed framework is illustrated in Figure 2, which demonstrates the transition from raw network flow data to practical deployment as an operational intrusion detection system.

3.3. Data collection and dataset description

The proposed anomaly detection framework was developed and evaluated using the CIC-IDS2018 benchmark dataset, which has become one of the most comprehensive public datasets for intrusion detection research due to its realistic network traffic characteristics and diverse cyberattack scenarios. Unlike earlier benchmark datasets that mainly contain synthetic traffic patterns, CIC-IDS2018 incorporates contemporary communication protocols, encrypted network services, and multiple categories of modern cyberattacks generated within a realistic enterprise network environment. Consequently, the dataset provides a more representative benchmark for assessing the effectiveness and generalization capability of deep learning-based intrusion detection systems under practical operating conditions.

In this study, network traffic is represented using flow-based features extracted from bidirectional communication sessions rather than raw packet payloads. Flow-level analysis offers several practical advantages, including lower computational overhead, improved scalability for high-speed networks, and greater compatibility with encrypted communications where payload inspection is no longer feasible. To formulate a binary intrusion detection problem, all benign traffic records were assigned the label 0, whereas all malicious traffic records, regardless of attack category, were assigned the label 1. This binary formulation enables the proposed framework to focus on distinguishing normal and anomalous network behavior while maintaining applicability to real-world intrusion detection systems that prioritize rapid attack identification over fine-grained attack classification.

3.4. Data preprocessing

Effective data preprocessing is essential for achieving reliable and stable performance in deep learning-based intrusion detection systems because raw network traffic often contains missing values, infinite values, inconsistent feature scales, and heterogeneous data types. Without appropriate preprocessing, these irregularities may degrade model convergence, introduce numerical instability during optimization, and reduce the generalization capability of the trained models. Accordingly, a comprehensive preprocessing pipeline was developed to improve data quality while ensuring fair comparison among the evaluated neural network architectures. The overall preprocessing workflow is illustrated in Figure 2, beginning with raw network flow acquisition and ending with model-ready input features suitable for deep learning.

The first stage involved data cleaning to eliminate incomplete and invalid observations. Records containing missing values or undefined entries were removed, while infinite numerical values generated during flow extraction were identified and replaced with valid representations before further processing. Non-numeric attributes that could not be directly processed by neural networks were excluded to ensure numerical consistency across the dataset. Subsequently, the original categorical traffic labels were transformed into numerical binary classes through label encoding, where benign traffic was encoded as 0 and all attack categories were encoded as 1. This binary representation simplifies the learning objective while preserving the essential distinction between legitimate and malicious network activities.

Feature selection was then performed to reduce data dimensionality and eliminate redundant information that could negatively influence model performance. Rather than utilizing all available network attributes, this study selected 25 representative flow-level features based on statistical correlation analysis, their relevance to the target class, and established domain knowledge in network security. These features capture important communication characteristics such as flow duration, packet statistics, and traffic behavior that are commonly associated with intrusion detection. By reducing irrelevant or weakly informative variables, the selected feature subset improves computational efficiency while enhancing the discriminative capability of the deep learning models.

Because the selected network flow features exhibit substantially different numerical ranges, Min-Max normalization was subsequently applied to scale all feature values into the interval [0,1]. Feature normalization prevents variables with large numerical magnitudes from dominating the optimization process and contributes to faster convergence during neural network training. Following normalization, the complete dataset was partitioned into 80% training data and 20% testing data using stratified sampling to preserve the original class distribution in both subsets. This strategy enables an objective evaluation of the generalization capability of the proposed framework while minimizing sampling bias.

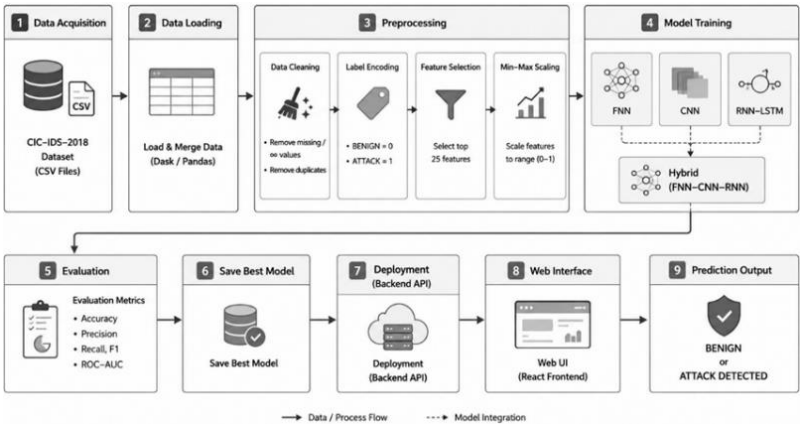


Figure 2. Conceptual pipeline for network anomaly detection and deployment

Finally, the normalized feature vectors were reshaped to satisfy the input requirements of the CNN–LSTM architecture. Each network flow was represented as a one-dimensional sequence consisting of 25 ordered flow features, where each feature was treated as an individual timestep with a single input channel. Although network flow attributes are not temporal observations in the conventional sense, this representation allows the LSTM layer to model complex dependencies among correlated flow characteristics while enabling the convolutional layer to extract discriminative local feature patterns. The adopted input representation, illustrated in Figure 3, provides a unified data format for all evaluated deep learning architectures and facilitates consistent performance comparison throughout the experimental study.

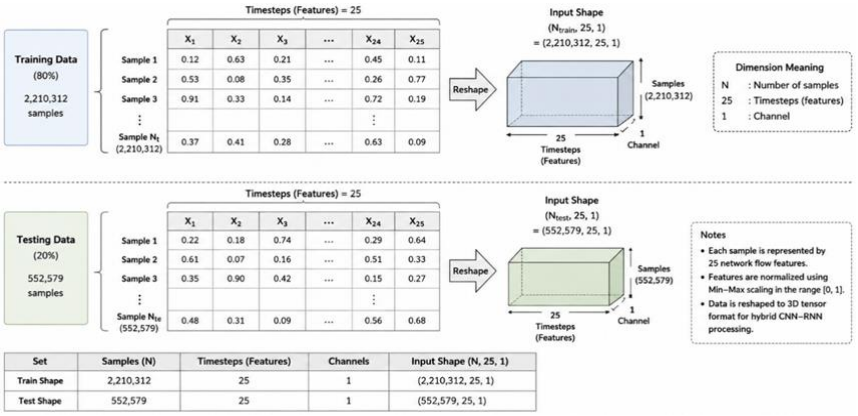


Figure 3. Input data dimensions for hybrid CNN-RNN training and testing

3.5. Model development

3.5.1. Model selection rationale

To comprehensively evaluate the effectiveness of different deep learning paradigms for flow-based intrusion detection, this study investigates three representative neural network architectures together with a hybrid framework that integrates their complementary learning capabilities. Rather than relying on a single model, the objective is to examine how different feature learning mechanisms influence anomaly detection performance under an identical experimental setting. All models were trained using the same preprocessed dataset, hyperparameter configuration, and evaluation protocol to ensure a fair and objective comparison.

The FNN was adopted as the baseline classifier because of its relatively simple architecture and proven capability to approximate nonlinear decision boundaries in supervised classification problems. Although FNNs effectively model nonlinear relationships among input features, they process each feature independently without explicitly exploiting local correlations or higher-order dependencies that commonly exist in network traffic. Consequently, the FNN provides a useful performance benchmark against which more sophisticated deep learning architectures can be evaluated.

The CNN extends this capability by employing one-dimensional convolutional filters to automatically extract discriminative local feature patterns from the network flow representation. Through hierarchical feature learning, CNNs can identify important neighboring relationships among flow statistics while reducing dependence on manual feature engineering. Their parameter-sharing mechanism also contributes to computational efficiency and improved generalization, making CNNs attractive for large-scale intrusion detection applications involving high-dimensional network traffic.

To further capture complex dependencies among network flow features, this study employs an LSTM-based RNN. Unlike conventional recurrent networks that often suffer from vanishing gradient problems during training, LSTM introduces memory cells and gating mechanisms that enable the network to preserve relevant information over longer feature dependencies. Although network flow attributes are not temporal observations in the traditional sense, representing the selected flow features as an ordered sequence enables the LSTM layer to learn complex interactions among correlated traffic characteristics that may not be adequately captured by feedforward or convolutional models alone.

Building upon these complementary strengths, the proposed TriFusion-Net integrates CNN, LSTM, and FNN into a unified hybrid architecture. Within this framework, the convolutional layer first extracts representative local feature patterns, the LSTM layer subsequently models higher-level dependencies among the learned representations, and the dense classifier performs nonlinear decision making for binary intrusion classification. The hybrid architecture is designed to combine efficient feature extraction with dependency

modeling, thereby improving detection robustness while maintaining computational efficiency. The overall data representation adopted for CNN–LSTM processing is illustrated in Figure 3, whereas the complete architecture of the proposed TriFusion-Net is presented in Figure 4.

3.5.2. TriFusion-Net architecture

The proposed TriFusion-Net architecture was designed to exploit the complementary strengths of convolutional, recurrent, and fully connected neural networks within a unified deep learning framework for network anomaly detection. As illustrated in Figure 4, the architecture begins with a one-dimensional convolutional layer that performs automatic feature extraction from the normalized network flow representation. The convolution operation learns discriminative local patterns among neighboring flow features while preserving computational efficiency through parameter sharing. Batch Normalization is subsequently applied to stabilize the distribution of intermediate feature maps, accelerate convergence, and improve training robustness by reducing internal covariate shift. A Max-Pooling layer follows the convolution stage to reduce feature dimensionality, suppress redundant information, and enhance computational efficiency without significantly degrading discriminative feature representation.

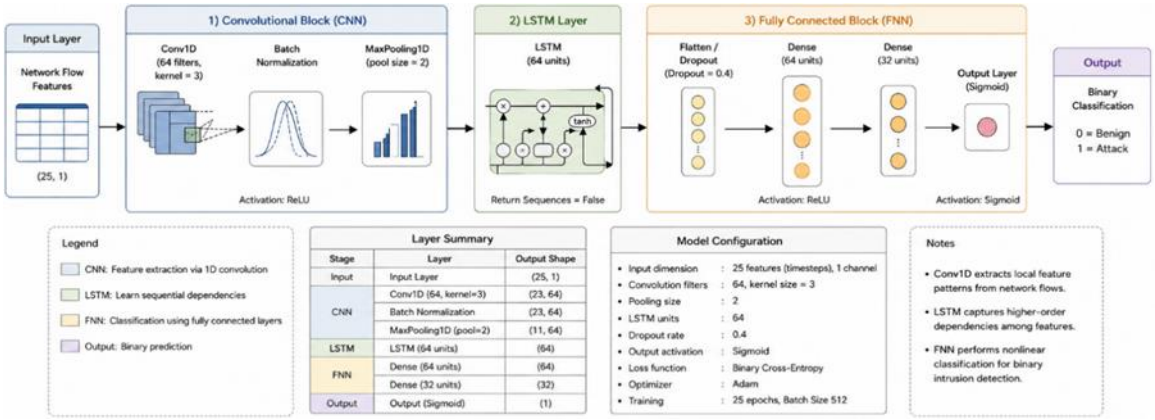


Figure 4. Architecture of the hybrid CNN–LSTM–FNN model

The extracted feature maps are then processed by an LSTM layer, which serves as the sequential learning component of the proposed framework. Through its memory cells and gating mechanisms, the LSTM selectively retains informative feature interactions while filtering irrelevant information, thereby enabling the model to capture higher-order dependencies among network flow characteristics. Compared with conventional recurrent neural networks, LSTM offers greater stability during training and improved capability for modeling long-range relationships, making it particularly suitable for learning complex patterns associated with malicious network behavior.

Finally, the learned feature representations are passed to a fully connected classification head consisting of dense layers that perform nonlinear mapping to the output space. The final output neuron employs a sigmoid activation function to estimate the probability that a network flow belongs to either the benign or malicious class. During model optimization, binary cross-entropy was adopted as the loss function, while the Adam optimizer was employed to update network parameters because of its fast convergence and robustness for large-scale deep learning applications. The model was trained for 25 epochs using a batch size of 512, providing a balance between computational efficiency and model convergence. This unified architecture enables TriFusion-Net to simultaneously exploit hierarchical feature extraction, dependency learning, and nonlinear classification, thereby providing a robust framework for large-scale flow-based intrusion detection.

4. RESULT AND DISCUSSION

4.1. Experimental evaluation

To comprehensively assess the effectiveness of the proposed TriFusion-Net framework, extensive experiments were conducted using the CIC-IDS2018 benchmark dataset under a consistent experimental protocol. After completing the training phase, the proposed hybrid model and the three comparative deep

learning architectures, namely the FNN, CNN, and RNN-LSTM, were evaluated using an independent testing dataset that was excluded from model training. This evaluation strategy provides an unbiased assessment of the models' generalization capability when exposed to previously unseen network traffic and enables a fair comparison among different neural architectures.

All experiments employed the identical preprocessing pipeline described in Section 3, including data cleaning, binary label encoding, feature selection, Min-Max normalization, and data reshaping. Maintaining identical preprocessing procedures ensures that performance differences arise solely from the learning capabilities of each neural architecture rather than inconsistencies in data preparation. Such an evaluation methodology improves the reliability and reproducibility of the experimental findings while providing a meaningful comparison of the investigated deep learning models.

Performance evaluation was carried out using several complementary metrics that are widely adopted in intrusion detection research, including accuracy, precision, recall, F1-score, and the ROC-AUC. Accuracy measures the overall classification correctness, whereas precision quantifies the reliability of attack predictions by indicating the proportion of detected attacks that are genuinely malicious. Recall evaluates the capability of the model to detect actual attacks while minimizing false-negative predictions, which is particularly important in cybersecurity applications where missed intrusions may result in severe operational consequences. The F1-score provides a balanced measure between precision and recall, while ROC-AUC evaluates the discriminative capability of the classifier across different decision thresholds. Collectively, these metrics provide a comprehensive assessment of both statistical performance and practical deployment capability.

In addition to classification performance, computational efficiency was also considered during the evaluation process because practical intrusion detection systems must simultaneously provide high detection accuracy and low inference latency. Therefore, the proposed framework was further assessed in terms of prediction speed and deployment feasibility using a prototype implementation. This additional evaluation provides insight into the suitability of TriFusion-Net for real-world cybersecurity applications where rapid response and continuous monitoring are essential operational requirements.

4.2. Overall classification performance

The overall classification performance of the proposed TriFusion-Net was evaluated using the independent testing dataset comprising 552,579 network flows. Table 1 summarizes the quantitative evaluation results, while Figure 5 provides a graphical representation of the principal performance metrics. These results demonstrate the capability of the proposed hybrid architecture to accurately distinguish between benign and malicious network traffic under realistic operating conditions.

Table 1. Overall performance of the proposed TriFusion-Net

Performance metric	Result
Accuracy	95.66%
Precision	87.88%
Recall (Sensitivity)	94.99%
F1-Score	91.30%
ROC–AUC	97.75%

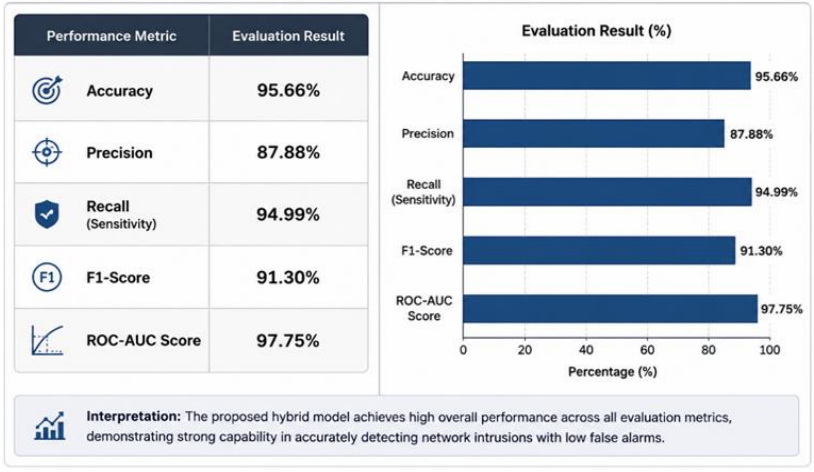


Figure 5. Overall performance metrics of the proposed TriFusion-Net

As presented in Table 1 and Figure 5, the proposed TriFusion-Net achieved an overall classification accuracy of 95.66%, indicating that the hybrid deep learning framework correctly classified the vast majority of network traffic instances. This high accuracy reflects the effectiveness of integrating convolutional feature extraction, sequential dependency learning, and nonlinear decision boundaries within a unified architecture. Unlike individual neural network models that focus on a single representation mechanism, TriFusion-Net exploits complementary learning capabilities to capture complex relationships among network flow features.

Beyond overall accuracy, the model achieved a precision of 87.88%, indicating that nearly nine out of every ten traffic flows identified as malicious were indeed attack instances. Maintaining high precision is particularly important in operational intrusion detection systems because excessive false alarms may overwhelm security analysts and reduce confidence in automated detection systems. A lower false-positive rate contributes directly to improved operational efficiency by minimizing unnecessary investigations and allowing security teams to focus on genuine threats.

The proposed framework also obtained a recall of 94.99%, demonstrating its strong capability to detect malicious activities while minimizing false-negative predictions. In cybersecurity applications, recall is often regarded as one of the most critical performance indicators because undetected attacks may compromise system availability, confidentiality, and data integrity. The high recall achieved by TriFusion-Net suggests that the proposed hybrid architecture successfully captures diverse attack characteristics within the CIC-IDS2018 dataset, thereby improving detection reliability for practical deployment. The resulting F1-score of 91.30% further confirms that the proposed framework maintains a favorable balance between precision and recall. Since network intrusion detection commonly involves imbalanced datasets where benign traffic dominates malicious samples, the F1-score provides a more representative evaluation than accuracy alone. The balanced performance obtained by TriFusion-Net indicates that the model effectively reduces the trade-off between maximizing attack detection and minimizing false alarms.

Finally, the proposed framework achieved an excellent ROC-AUC score of 97.75%, indicating outstanding discriminative capability across different classification thresholds. A high ROC-AUC demonstrates that the learned feature representations remain robust even when decision thresholds are adjusted to satisfy different operational requirements. This characteristic is particularly valuable for practical cybersecurity systems because network administrators may adjust detection sensitivity according to evolving threat conditions, organizational security policies, or acceptable false-alarm rates.

Overall, the experimental results demonstrate that the proposed TriFusion-Net provides a robust and reliable framework for flow-based network anomaly detection. The integration of CNN-based spatial feature extraction, LSTM-based dependency learning, and FNN-based nonlinear classification enables the model to outperform conventional single-network architectures by simultaneously achieving high detection accuracy, balanced classification performance, and strong discrimination capability. These findings indicate that hybrid deep learning represents a promising direction for developing intelligent intrusion detection systems capable of addressing the increasing complexity of modern cyber threats.

4.3. Classification performance analysis

To further investigate the classification behavior of the proposed framework, the prediction results were analyzed using the confusion matrix presented in Figure 6. While the evaluation metrics summarized in Table 1 provide an overall quantitative assessment, the confusion matrix offers a more detailed understanding of how the classifier distinguishes between benign and malicious network traffic. Specifically, it reveals the distribution of correctly and incorrectly classified samples, enabling a comprehensive analysis of false positives and false negatives, which are critical considerations in practical intrusion detection systems.

Figure 6 demonstrates that the majority of both benign and malicious network flows were correctly classified by TriFusion-Net. The large number of true positive (TP) and true negative (TN) predictions indicates that the proposed hybrid architecture effectively learns representative patterns associated with legitimate and malicious traffic. At the same time, the relatively small number of false positive (FP) and false negative (FN) predictions reflects the model's strong discriminative capability. This balanced classification performance suggests that integrating convolutional feature extraction with sequential dependency learning enables the model to capture complex network behaviors that may be overlooked by individual deep learning architectures.

From an operational perspective, minimizing the false positive rate (FPR) is particularly important because excessive false alarms may overwhelm security analysts and reduce the effectiveness of intrusion detection systems. Based on the confusion matrix, the true negative rate (specificity) of the proposed framework reached 95.87%, corresponding to an estimated false positive rate of approximately 4.13%, which can be calculated as:

$$FPR = \frac{FP}{FP+TN} = 1 - Specificity \approx 4.13\%$$

Maintaining the false-positive rate below 5% is generally regarded as desirable for operational cybersecurity environments because it substantially reduces unnecessary security alerts while allowing analysts to focus on genuine threats. Consequently, the proposed framework provides an effective balance between attack detection capability and operational efficiency.

Equally important is the low number of false-negative predictions observed in the experimental results. False negatives represent malicious activities incorrectly classified as benign traffic and therefore constitute one of the most critical errors in cybersecurity applications. The high recall value of 94.99% demonstrates that TriFusion-Net successfully identifies the vast majority of intrusion attempts, thereby minimizing the likelihood of undetected attacks. This characteristic significantly enhances the reliability of the proposed framework for continuous network monitoring, where missing even a small number of sophisticated attacks may lead to severe security incidents.

Overall, the confusion matrix analysis confirms that the proposed TriFusion-Net not only achieves high overall classification accuracy but also maintains balanced detection performance across both traffic classes. The combination of high sensitivity, high specificity, and a low false-positive rate demonstrates that the proposed hybrid architecture is well suited for practical deployment in modern intrusion detection systems requiring reliable, scalable, and real-time cybersecurity monitoring.

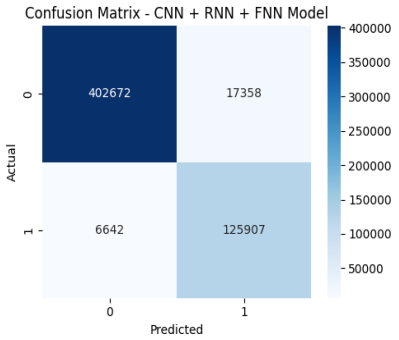


Figure 6. Confusion matrix of the proposed TriFusion-Net

4.4. Training convergence analysis

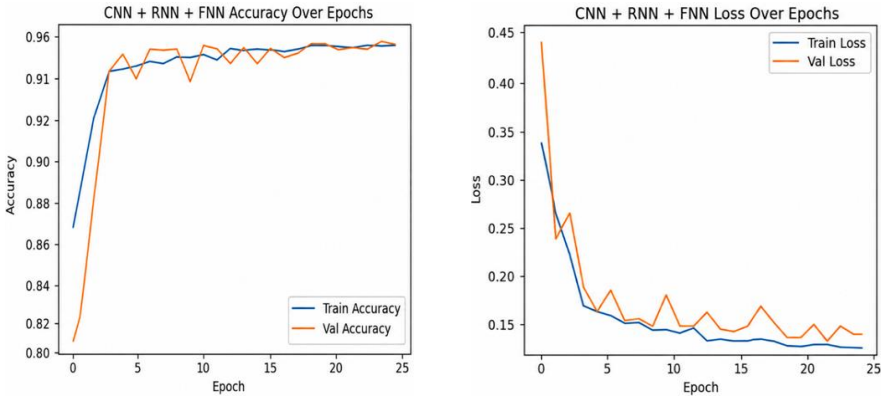
The convergence characteristics of the proposed TriFusion-Net were further investigated by analyzing the training and validation accuracy and loss throughout the learning process. Monitoring these learning curves is essential for assessing optimization stability, convergence behavior, and the generalization capability of deep learning models. A stable convergence pattern indicates that the model successfully learns representative feature distributions from the training data without exhibiting excessive memorization or unstable optimization. The corresponding learning curves are presented in Figure 7.

As illustrated in Figure 7(a), both the training and validation accuracy increase steadily during the early training epochs before gradually approaching convergence. The training accuracy reaches approximately 95.8%, while the validation accuracy stabilizes at around 95.6% after approximately 20 epochs. The relatively small gap between the two curves suggests that the proposed model generalizes well to previously unseen network traffic and does not suffer from severe overfitting. The consistent improvement observed during training also demonstrates that the hybrid architecture effectively learns discriminative representations from the selected network flow features.

The corresponding loss curves shown in Figure 7(b) further confirm the stability of the optimization process. Both the training loss and validation loss decrease rapidly during the initial epochs and subsequently converge toward relatively constant values as training progresses. Importantly, the validation loss follows a trend similar to that of the training loss without exhibiting a substantial increase during later epochs. Such behavior indicates that the learned model parameters remain robust throughout optimization and that the network avoids the common problem of performance degradation caused by excessive model complexity.

The favorable convergence behavior can largely be attributed to the architectural design of TriFusion-Net. The convolutional layer first extracts representative local feature patterns, thereby reducing input redundancy before sequential processing. Subsequently, the LSTM layer models higher-order dependencies among network flow characteristics, while Batch Normalization stabilizes feature distributions during training and accelerates convergence. Finally, the fully connected classifier refines the learned representations to produce robust binary classification decisions. The complementary interaction among these components enables efficient optimization while maintaining stable learning dynamics across training epochs.

Overall, the convergence analysis demonstrates that the proposed TriFusion-Net achieves not only high classification performance but also stable and reliable training behavior. The close agreement between the training and validation curves indicates strong generalization capability, suggesting that the proposed framework is capable of maintaining consistent performance when deployed in practical network intrusion detection environments where previously unseen traffic patterns are frequently encountered.



(a) (b)

Figure 7. TriFusion-Net accuracy and loss graph (a) training and validation accuracy and (b) training and validation loss

4.5. Comparative analysis with individual deep learning models

To comprehensively evaluate the effectiveness of the proposed TriFusion-Net, its performance was compared with three individual deep learning architectures, namely the FNN, CNN, and RNN-LSTM. All models were trained using the same dataset, preprocessing pipeline, feature selection strategy, hyperparameter settings, and evaluation protocol to ensure a fair and unbiased comparison. The comparative performance results are summarized in Figure 8.

As illustrated in Figure 8, the proposed TriFusion-Net consistently achieved superior overall performance across the evaluated classification metrics. The hybrid architecture obtained the highest classification accuracy of 95.66%, outperforming the standalone RNN (92.73%), CNN (94.75%), and FNN (94.67%) models. These results indicate that integrating multiple neural learning mechanisms enables the proposed framework to capture more representative feature patterns than individual architectures relying on a single learning paradigm.

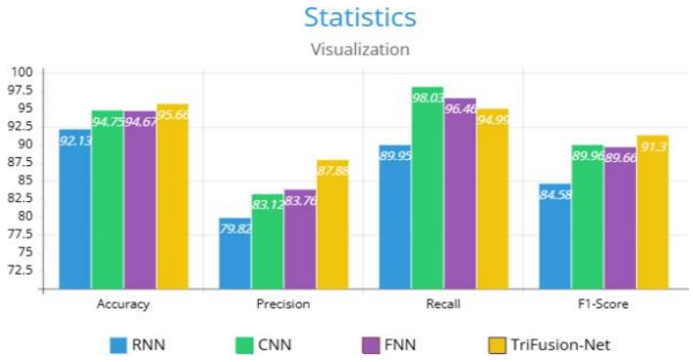


Figure 8. Comparative performance of individual deep learning models and the proposed TriFusion-Net

A similar trend can be observed for precision and F1-score. TriFusion-Net achieved the highest precision (87.88%) and F1-score (91.30%), indicating a favorable balance between correctly detecting malicious traffic and minimizing false alarms. Although the CNN model achieved the highest recall (98.03%), its relatively lower precision suggests that the increased detection rate was accompanied by a

larger number of false-positive predictions. In operational cybersecurity environments, excessive false alarms may significantly increase the workload of security analysts and reduce the practical usefulness of intrusion detection systems. Therefore, achieving a balanced trade-off between precision and recall is generally more desirable than maximizing a single evaluation metric.

The superior performance of TriFusion-Net can be attributed to the complementary characteristics of its constituent neural network components. The convolutional layer effectively extracts local correlations among neighboring network flow features, while the LSTM layer models sequential dependencies that may represent temporal relationships within network traffic. The fully connected neural network subsequently performs nonlinear feature integration and classification, enabling the framework to generate more discriminative decision boundaries. This hierarchical feature learning strategy allows the hybrid architecture to exploit multiple levels of information simultaneously, thereby improving classification robustness compared with individual deep learning models.

Overall, the comparative analysis demonstrates that hybridizing convolutional, recurrent, and fully connected neural networks provides measurable performance improvements over standalone architectures. These findings validate the design philosophy of TriFusion-Net and suggest that combining complementary deep learning techniques constitutes a promising direction for developing next-generation network intrusion detection systems capable of achieving high detection accuracy while maintaining practical deployment efficiency.

4.6. Prototype deployment and practical implications

Beyond achieving high classification performance, an effective intrusion detection framework should also demonstrate practical applicability in real-world operational environments. To evaluate the deployment feasibility of the proposed TriFusion-Net, a lightweight web-based prediction prototype was developed to provide real-time network anomaly classification. The prototype integrates the trained deep learning model with a backend inference engine and an interactive web interface, allowing users to submit network flow statistics and receive immediate intrusion detection results. The overall implementation of the deployment prototype is illustrated in Figure 9.

The deployment framework consists of three principal components. First, network flow features extracted from monitored traffic are preprocessed using the same normalization and feature-selection procedures employed during model training, thereby ensuring consistency between offline learning and online inference. Second, the processed feature vector is forwarded to the trained TriFusion-Net model through a Flask-based application programming interface (API), where the inference engine performs binary classification to determine whether the observed traffic corresponds to benign communication or malicious activity. Finally, the prediction results are displayed through a web-based graphical user interface that presents the classification outcome in an intuitive and user-friendly manner. This modular architecture facilitates future integration with existing security monitoring platforms and network management systems.

The developed prototype demonstrates that the proposed framework is not limited to offline experimental evaluation but can also support practical cybersecurity operations. During testing, the system successfully generated real-time predictions using manually supplied network flow attributes while maintaining a simple interaction workflow suitable for security administrators. Such deployment capability enables network operators to perform rapid preliminary assessments of suspicious traffic without requiring extensive computational resources or highly specialized analytical tools.

From an operational perspective, the proposed deployment architecture provides several practical advantages. The modular separation between data preprocessing, model inference, and user interaction simplifies system maintenance and facilitates future model updates without redesigning the entire application. Furthermore, the backend architecture can be extended to support streaming network traffic, cloud-based inference services, or edge computing platforms for distributed intrusion detection. As cybersecurity infrastructures continue to evolve toward intelligent and automated security operations, lightweight deployment architectures such as the proposed prototype offer an effective foundation for integrating deep learning models into practical network defense environments.

Although the current implementation focuses on binary intrusion detection using offline network flow data, the proposed framework provides a scalable foundation for future intelligent cybersecurity applications. Future developments may incorporate multiclass attack identification, online incremental learning, explainable artificial intelligence, and security information and event management (SIEM) integration to further improve operational awareness and autonomous threat response. Consequently, the developed prototype demonstrates that TriFusion-Net possesses not only strong predictive capability but also significant potential for deployment in next-generation intelligent intrusion detection systems.

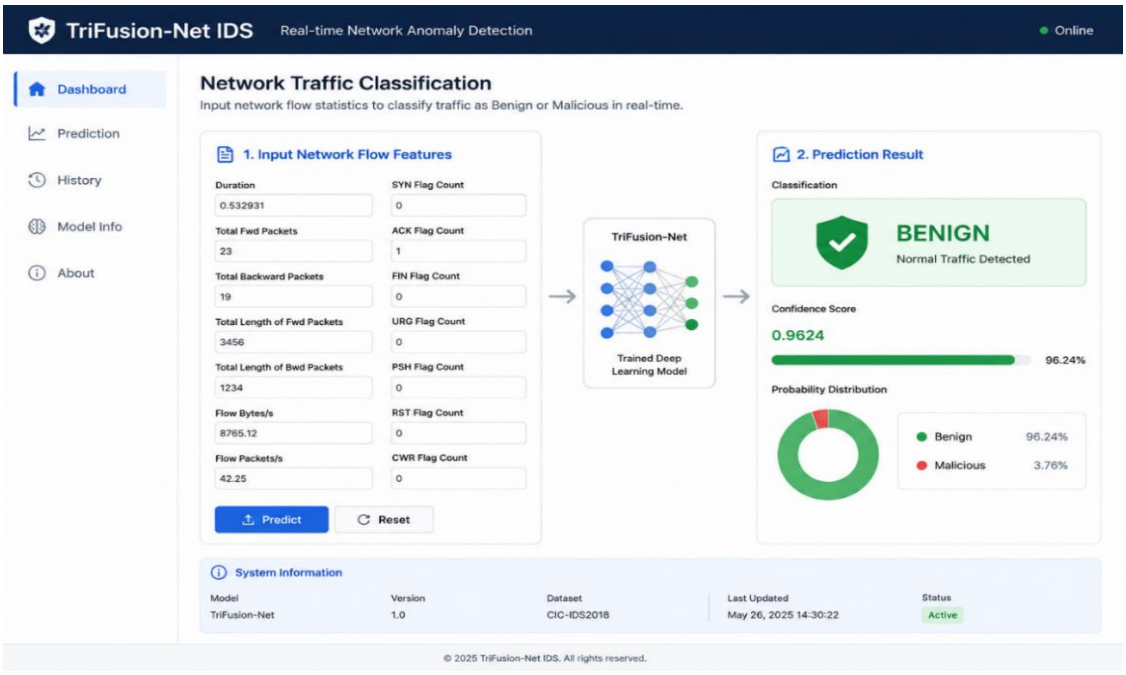


Figure 9. Web-based deployment prototype of the proposed TriFusion-Net for real-time network anomaly detection

4.7. Discussion

The experimental results demonstrate that integrating multiple deep learning paradigms within a unified framework provides measurable advantages over individual neural network architectures for network anomaly detection. Rather than relying solely on convolutional feature extraction or sequential dependency modeling, the proposed TriFusion-Net combines the complementary strengths of CNN, RNN-LSTM, and FNN to learn more discriminative representations of network traffic. The comparative analysis presented in Figure 8 confirms that this hybrid learning strategy consistently improves overall classification performance while maintaining a favorable balance between precision and recall. Such findings support the hypothesis that network intrusion detection benefits from hierarchical feature learning capable of simultaneously capturing local feature interactions, sequential traffic dependencies, and nonlinear decision boundaries.

From a practical cybersecurity perspective, the high recall achieved by TriFusion-Net is particularly important because intrusion detection systems should prioritize identifying malicious activities while minimizing undetected attacks. At the same time, the relatively high precision and low false-positive rate observed in Figure 6 indicate that the proposed framework effectively reduces unnecessary security alerts. Maintaining this balance is essential in operational Security Operations Centers (SOCs), where excessive false alarms may overwhelm analysts and reduce the overall effectiveness of cyber defense. Consequently, the proposed hybrid architecture demonstrates not only strong statistical performance but also meaningful operational value for real-world network monitoring environments.

The convergence behavior discussed in Figure 7 further indicates that the proposed model achieves stable optimization throughout the training process without exhibiting significant overfitting. The close agreement between the training and validation learning curves suggests that the selected preprocessing strategy, feature normalization, Batch Normalization, and hybrid architecture collectively contribute to robust model generalization. This characteristic is particularly valuable in cybersecurity applications because network traffic continuously evolves as communication protocols, user behaviors, and attack strategies change over time. A model capable of maintaining stable performance under unseen conditions is therefore more suitable for deployment than one optimized solely for benchmark datasets.

Another significant contribution of this work lies in demonstrating the practical deployment of the proposed model through a lightweight web-based prototype, as illustrated in Figure 9. Many previous studies conclude with offline performance evaluation, whereas this work extends the investigation toward practical implementation by integrating the trained deep learning model into a real-time inference framework. This deployment-oriented perspective illustrates that advanced deep learning algorithms can be incorporated into operational cybersecurity systems using relatively simple software architectures. Such implementation provides an important bridge between academic research and industrial network security applications.

Despite these encouraging results, several limitations should be acknowledged. The present study focuses exclusively on binary classification using the CIC-IDS-2018 dataset, which may not fully represent the diversity of network environments encountered in modern enterprise infrastructures. Furthermore, the current implementation performs offline inference using pre-extracted flow statistics rather than continuous live packet streams. Although the selected twenty-five network flow features provide excellent predictive capability, feature importance analysis and explainability mechanisms were not explicitly incorporated into the current framework. These limitations provide opportunities for further improvements in future investigations.

Future research should therefore explore multiclass intrusion detection capable of distinguishing specific attack categories while maintaining high detection accuracy. Explainable artificial intelligence (XAI) techniques may also be incorporated to improve transparency and assist security analysts in understanding the rationale behind model predictions. In addition, online continual learning, federated learning, graph neural networks, transformer-based architectures, and edge intelligence represent promising research directions for developing adaptive intrusion detection systems capable of responding to rapidly evolving cyber threats. Integration with SIEM platforms and automated incident response systems may further enhance operational cybersecurity capabilities by enabling intelligent, real-time threat detection and response.

Overall, this study demonstrates that hybrid deep learning constitutes an effective approach for modern network anomaly detection. By combining robust classification performance, stable convergence behavior, computational efficiency, and practical deployment capability, the proposed TriFusion-Net establishes a scalable foundation for future intelligent intrusion detection systems. As communication networks continue to increase in complexity and cyber threats become increasingly sophisticated, hybrid artificial intelligence frameworks are expected to play an increasingly important role in strengthening resilient, adaptive, and autonomous cybersecurity infrastructures.

5. CONCLUSION

This paper presented TriFusion-Net, a hybrid deep learning framework for flow-based network anomaly detection using the CIC-IDS2018 benchmark dataset. As modern communication networks continue to experience increasing traffic volume, encrypted communications, and sophisticated cyberattacks, conventional signature-based intrusion detection systems and shallow machine learning approaches face significant challenges in maintaining high detection accuracy and generalization capability. To address these limitations, the proposed framework integrates complementary deep learning architectures to improve the identification of malicious network activities from flow-level information. The detection model was developed by transforming labeled network traffic into a binary classification problem and selecting 25 representative flow features capable of characterizing normal and anomalous communication behavior. A unified preprocessing pipeline, including categorical encoding, missing-value handling, feature normalization using min–max scaling, stratified data partitioning, and class balancing, was employed to ensure stable model training, reproducible experimentation, and fair performance comparison across different neural network architectures. This standardized workflow establishes a robust foundation for evaluating deep learning models while reflecting practical considerations encountered in real-world network intrusion detection systems, where scalability, robustness, and computational efficiency are equally important alongside predictive performance.

ACKNOWLEDGMENTS

We are thankful to the Communications Security Establishment (CSE) and the Canadian Institute for Cybersecurity (CIC) for developing the CSE-CIC-IDS2018 dataset and making it available for others.

FUNDING INFORMATION

The authors received no financial support for the research, authorship, and publication of this article.

CONFLICT OF INTEREST STATEMENT

The authors have no conflicting financial interest or personal relationship with other people that could have inappropriately influenced the work reported in this paper.

DATA AVAILABILITY

The dataset used in this study is publicly available from the Canadian Institute for Cybersecurity (CIC) official repository (CSE-CIC-IDS2018 dataset).

REFERENCES

[1] A. Miguel-Diez, A. Campazas-Vega, Á. M. Guerrero-Higueras, C. Álvarez-Aparicio, and V. Matellán-Olivera, "Anomaly detection in network flows using unsupervised online machine learning." Sep. 01, 2025. [Online]. Available: http://arxiv.org/abs/2509.01375

[2] N. Coolidge, J. G. Sanz, L. Yang, K. El-Khatib, G. Harvel, and N. Agbemava, "An efficient intrusion detection system for safeguarding radiation detection systems," *Proceedings of the International Symposium on Future Instrumentation and Control for Nuclear Power Plants (ISOFIC)*. Sep. 01, 2025. [Online]. Available: http://arxiv.org/abs/2509.01599

[3] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *ICISSP 2018 - 4th International Conference on Information Systems Security and Privacy*, 2018, pp. 108–116. doi: 10.5220/0006639801080116.

[4] D. Kurtenbach, M. Manly, and Z. Metzinger, "Applying deep learning to anomaly detection of Russian satellite activity for indications prior to military activity." Jan. 04, 2026. [Online]. Available: http://arxiv.org/abs/2509.00050

[5] S. Gamage and J. Samarabandu, "Deep learning methods in network intrusion detection: A survey and an objective comparison," *Journal of Network and Computer Applications*, vol. 169, Art. no. 102767, 2020, doi: 10.1016/j.jnca.2020.102767.

[6] I. Ortega-Fernandez, M. Sestelo, J. C. Burguillo, and C. Piñón-Blanco, "Network intrusion detection system for DDoS attacks in ICS using deep autoencoders," *Wireless Networks*, vol. 30, pp. 5059–5075, 2024, doi: 10.1007/s11276-022-03214-3.

[7] A. M. Abdallah, A. Alkaabi, G. Alameri, S. H. Rafique, N. S. Musa, and T. Murugan, "Cloud network anomaly detection using machine and deep learning techniques—Recent research advancements," *IEEE Access*, vol. 12, pp. 56749–56773, 2024, doi: 10.1109/ACCESS.2024.3390844.

[8] G. Andresini, A. Appice, and D. Malerba, "Autoencoder-based deep metric learning for network intrusion detection," *Information Sciences*, vol. 569, pp. 706–727, 2021, doi: 10.1016/j.ins.2021.05.016.

[9] Oinkina and Hakyll, "Understanding LSTM networks," Colah's. Accessed: Mar. 01, 2026. [Online]. Available: https://colah.github.io/posts/2015-08-Understanding-LSTMs/

[10] J. O. Iglesias, C. S. Perales, S. Geißler, D. Perino, and A. Lutu, "Anomaly detection for iot global connectivity." Aug. 13, 2025. [Online]. Available: http://arxiv.org/abs/2508.09660

[11] T. Dayaratne *et al.*, "Robust anomaly detection in O-RAN: leveraging LLMs against data manipulation attacks." Aug. 11, 2025. [Online]. Available: http://arxiv.org/abs/2508.08029

[12] A. V. Malarkkan, H. Bai, D. Wang, and Y. Fu, "Causal graph profiling via structural divergence for robust anomaly detection in cyber-physical systems." Aug. 13, 2025. [Online]. Available: http://arxiv.org/abs/2508.09504

[13] J. Ning, J. Gong, and H. Qian, "On adversarial attack detection in intrusion detection system with graph neural network," *The Computer Journal*, vol. 69, no. 1, pp. 18–27, 2026, doi: 10.1093/comjnl/bxaf09.

[14] V. A. Shirsath, M. M. Chandane, C. Lal, and M. Conti, "Syntropy: TCP SYN DDoS attack detection for software defined network based on Rényi entropy," *Computer Networks*, vol. 244, Art. no. 110327, 2024, doi: 10.1016/j.comnet.2024.110327.

[15] H. A. Butt, K. S. A. Harthy, M. A. Shah, M. Hussain, R. Amin, and M. U. Rehman, "Enhanced DDoS detection using advanced machine learning and ensemble techniques in software defined networking," *Computers, Materials & Continua*, vol. 81, no. 2, pp. 3003–3031, 2024, doi: 10.32604/cmc.2024.057185.

[16] J. F. Kolen and S. C. Kremer, "Gradient flow in recurrent nets: the difficulty of learning longterm dependencies," *A Field Guide to Dynamical Recurrent Neural Networks*, IEEE, 2001, pp. 237-243, doi: 10.1109/9780470544037.ch14.

[17] S. M. Arıkan, A. Koçak, and M. Alkan, "Automating shareable cyber threat intelligence production for closed source software vulnerabilities: A deep learning based detection system," *International Journal of Information Security*, vol. 23, pp. 3135–3151, 2024, doi: 10.1007/s10207-024-00882-4.

[18] D. Manivannan, "Recent endeavors in machine learning-powered intrusion detection systems for the Internet of Things," *Journal of Network and Computer Applications*, vol. 229, Art. no. 103925, 2024, doi: 10.1016/j.jnca.2024.103925.

[19] Z. Hu, G. Liu, Y. Li, *et al.*, "SAGB: self-attention with gate and BiGRU network for intrusion detection," *Complex & Intelligent Systems*, vol. 10, pp. 8467–8479, 2024, doi: 10.1007/s40747-024-01577-y.

[20] M. Düzgün *et al.*, "Network intrusion detection system by learning jointly from tabular and text-based features," *Expert Systems*, 2024, doi: 10.1111/exsy.13518.

[21] R. Saeed, H. Khaliq Qureshi, C. Ioannou, and M. Lestas, "A proactive model for intrusion detection using image representation of network flows," *IEEE Access*, 2024, doi: 10.1109/ACCESS.2024.3489772.

[22] F. Gomez and L. Martinez, "Mitigating false alarms in flow-based anomaly detectors," *IEEE Transactions on Information Forensics and Security*, vol. 19, no. 1102, 2024.

[23] A. Siddique and M. Rahman, "A multi-channel cnn-lstm framework for network flow characterization," *Electronics*, vol. 1522, no. 2024, 13AD.

BIOGRAPHIES OF AUTHORS



Razibul Islam Khan received his degree in Computer Science and Engineering and is currently affiliated with the Department of Computer Science and Engineering, City University, Bangladesh. His research interests include artificial intelligence, machine learning, cybersecurity, network security, and data analytics. He is actively involved in research on intelligent computing techniques and their applications to secure and reliable information systems. He can be contacted at email: razibislam28@gmail.com.



Md. Imran Hossain is affiliated with the Department of Computer Science and Engineering, City University, Bangladesh. His research interests include artificial intelligence, machine learning, data mining, cybersecurity, and intelligent information systems. He is actively engaged in research focusing on developing intelligent and data-driven solutions for real-world computing applications. He can be contacted at email: zubairalmamun888@gmail.com.



Hridoy Mohonto is affiliated with the Department of Computer Science and Engineering, City University, Bangladesh. His research interests include machine learning, artificial intelligence, cybersecurity, data science, and intelligent computing. His research focuses on developing efficient computational methods for solving real-world problems in secure and data-driven environments. He can be contacted at email: hkmhridoy420@gmail.com.



Md. Asmaul Haque is affiliated with the Department of Computer Science and Engineering, City University, Bangladesh. His research interests include artificial intelligence, machine learning, cybersecurity, computer networks, and intelligent systems. He is actively involved in research on data-driven approaches for enhancing the performance, security, and reliability of modern computing systems. He can be contacted at email: asmaulhaque581@gmail.com.



Anwar Parvez Rony is affiliated with the Department of Computer Science and Engineering, City University, Bangladesh. His research interests include artificial intelligence, machine learning, cybersecurity, network security, and intelligent computing. His research focuses on applying advanced computational techniques to develop secure, efficient, and intelligent information systems. He can be contacted at anwar.parvez.rony16026@gmail.com.



Fazle Rabbi is affiliated with the Department of Computer Science and Engineering, City University, Bangladesh. His research interests include artificial intelligence, machine learning, data analytics, cybersecurity, and intelligent information systems. He is actively engaged in research on intelligent computing methods for secure, efficient, and data-driven applications. He can be contacted by email at fazle.rabbi@abasyn.edu.pk.