

A Hybrid Dense-LSTM Framework For Generalizable Network Intrusion Detection: A Cross-Dataset Evaluation

Ms. Vishwa K. Patel¹, Dr. Premal Patel², Dr. Satvik Khara³

^{1,2,3}*Department of Computer Engineering, Silver Oak University, Ahmedabad, India*
doi.org/10.64643/IJIRT210107

Abstract—Conventional Intrusion Detection Systems (IDS) typically rely on one learning paradigm, which restricts how well they adjust to new network environments and respond to rapidly changing cyber threats. As attacks become more sophisticated, the weaknesses of such single-method designs become increasingly apparent. This study addresses the problem by introducing a hybrid deep learning framework that combines Dense Neural Networks with Long Short-Term Memory (LSTM) networks for reliable network intrusion detection. The Dense branch learns statistical relationships across high-dimensional traffic features, whereas the LSTM branch captures the temporal dependencies present in network traffic flows. The outputs of both branches are joined in a feature concatenation layer prior to final classification. To counter class imbalance and improve the representation of minority attack classes, the Synthetic Minority Oversampling Technique (SMOTE) is applied before training.

The model is trained and validated on the CICIDS2017 dataset, while UNSW-NB15 is used for cross-dataset testing to assess generalization. Results show stable convergence and effective learning of complex traffic patterns, with the hybrid model outperforming single-architecture baselines in detection accuracy and F1-score, most notably for minority attack classes after SMOTE balancing.

Cross-dataset evaluation exposed clear feature distribution shifts between the two datasets, highlighting that domain generalization remains a difficult challenge in intrusion detection, yet it also confirmed that hybrid deep learning is practically viable. Overall, these findings position the proposed framework as a scalable and adaptable basis for real-world cybersecurity applications and for future work on cross-dataset network anomaly detection.

Index Terms—Intrusion Detection System, Deep Learning, Siamese Network, Long Short-Term Memory, Network Security, Zero Day Attack, Cross-Dataset Generalization, Cyber security, Synthetic Minority Oversampling Technique

I. INTRODUCTION

The complexity and attack surface of contemporary communication systems have greatly risen due to the quick growth of cloud computing, Internet of Things ecosystems, edge networks, and software defined infrastructures. As digital services become increasingly essential to financial systems, healthcare systems, industrial automation, and smart cities, network security has become a key concern. Intrusion detection systems (IDS) are integral components of defensive infrastructures that are used to detect unauthorized or malicious use of the network. However, traditional IDS that depends on pre-established attack rules are not sufficient in the case of developing attack and zero-day attacks [1].

Advances in Machine Learning (ML) and Deep Learning (DL) have substantially improved anomaly detection capabilities in network security [2]. Deep Neural Networks (DNN) can automatically extract discriminative feature representations and model complex nonlinear relationships within high-dimensional network traffic data. Among DL architectures, Long Short-Term Memory (LSTM) networks a specialized type of Recurrent Neural Network (RNN) capable of capturing long-range temporal dependencies have proven particularly effective for detecting attacks with sequential or time-dependent characteristics, such as scanning bursts and prolonged connection attempts [3]. However, LSTM-based models may fail to detect attacks that lack strong temporal signatures. Conversely, Dense (fully connected feed-forward) Neural Networks are widely used for statistical feature modeling in IDS, effectively capturing correlations among traffic parameters such as packet count, flow duration, and protocol flags. Yet dense architectures inherently lack a mechanism for representing temporal order or sequential similarity,

limiting their generalizability across diverse network conditions.

Network traffic inherently exhibits temporal, statistical, and relational structures simultaneously. Despite recent progress, the majority of existing IDS frameworks continue to rely on a single learning paradigm either purely statistical (Dense-based) or purely sequential (LSTM-based) rather than jointly exploiting complementary representations [4]. This single-perspective modeling constrains both detection accuracy and generalization capability across varying network environments.

Another major obstacle is how much feature distributions and attack-type compositions differ from one benchmark IDS dataset to the next UNSW-NB15 [5] and CICIDS2017 [6] being prime examples. A model trained on just one of these datasets often falls apart when tested on another, which is a real problem for practical deployment: actual networks almost never match the specific conditions captured in any single benchmark [7]. This makes cross-dataset evaluation critical for properly testing how well a model generalizes, yet most hybrid-IDS studies still don't do enough of it.

Class imbalance is another persistent headache in intrusion detection, since benign traffic instances vastly outnumber many attack categories [7]. This skews classifiers toward predicting the majority class, which hurts detection performance for minority attack types [8] making effective data-balancing strategies a necessity during model training.

Motivated by these gaps, our study sets out to design, implement, and rigorously evaluate a hybrid deep learning framework capable of jointly capturing the statistical and sequential characteristics of network traffic while directly tackling both class imbalance and cross-dataset generalization.

Objectives of our research are as follow:

1. Develop hybrid Dense: LSTM architecture capable of jointly capturing statistical feature correlations and temporal traffic dependencies.
2. Apply the Synthetic Minority Oversampling Technique (SMOTE) to mitigate class imbalance and improve minority-class attack representation.

3. Train the proposed framework on the CICIDS2017 dataset and evaluate its cross-dataset generalization capability using the UNSW-NB15 dataset.

4. Analyze the framework's stability, detection performance, and adaptability across heterogeneous network environments.

This research is in line with the United Nations Sustainable Development Goal (SDG) 9: Industry, Innovation and Infrastructure. Secure and reliable communication networks are essential for the modern digital infrastructure, enabling it to deliver vital services like financial systems, healthcare platforms, industrial automation, and smart city technologies. Cyber security is a key element to better ensure the resilience of these digital infrastructures and stops malicious cyber attacks

The key scientific contributions of our work include the following:

- A novel hybrid Dense–LSTM deep learning framework for NIDS:

Unlike single-paradigm IDS models, the proposed architecture combines statistical feature learning (through the dense branch) with sequential dependency modeling (through the LSTM branch), merging both through a feature concatenation layer [4]. This fusion produces richer, more discriminative representations of network traffic than either branch could achieve on its own.

- Integration of SMOTE-based class balancing:

The framework applies SMOTE before training to counteract class imbalance, boosting the model's sensitivity to underrepresented attack types a step frequently overlooked in prior hybrid-IDS studies and thereby improving detection reliability in practice [5].

- Rigorous cross-dataset generalization evaluation:

Rather than relying solely on within-dataset validation, this study trains the model on CICIDS2017 [6] and tests it on UNSW-NB15 [5], as shown in Figure 1.

This cross-dataset setup offers a realistic assessment of the model's robustness to feature distribution shifts across distinct network environments a requirement that is critical yet rarely examined in real-world IDS deployment.

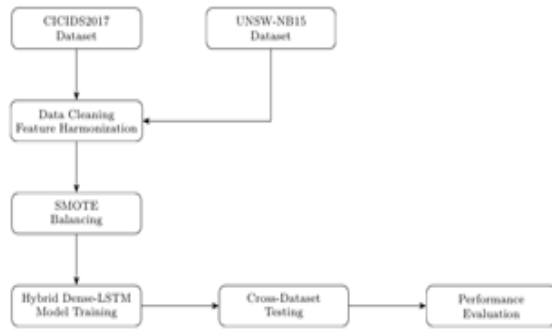


Figure: 1 Cross-Dataset Evaluation Pipeline of the Proposed Hybrid Dense-LSTM Framework

- Empirical analysis of generalization limitations and design insights: Our study provides a detailed analysis of the performance differences observed during cross dataset testing, offering actionable insights into feature distribution mismatches and laying the groundwork for future cross-domain intrusion detection research [9].

Together, these contributions advance the state of the art, showing that hybrid learning combined with balanced training data offers greater adaptability and scalability for real-world cyber security than conventional single paradigm IDS models [4].

II. LITERATURE REVIEW

A. Signature-Based and Classical Machine Learning Approaches

Early intrusion detection research leaned heavily on rule-based and signature-matching techniques, comparing observed traffic against a database of known attack patterns. Such systems work well against previously catalogued threats, but they fail when faced with novel or evolving attacks polymorphic malware and zero-day exploits, for instance since detection depends entirely on having prior knowledge of the attack signature [9].

This shortcoming pushed the field toward anomaly-based detection, where machine learning algorithms such as Support Vector Machines, Decision Trees, Random Forests, and k-Nearest Neighbors classify traffic as benign or malicious using hand-engineered features drawn from flow statistics, packet headers, and protocol properties [10]. Although these methods marked an improvement over static signature matching, their performance remains tightly bound to the quality of feature engineering and the

characteristics of the training dataset, leaving them brittle when applied to traffic that differs from what they were trained on.

B. Deep Learning Approaches

Deep learning overcame the feature-engineering bottleneck by learning hierarchical representations directly from raw or lightly processed traffic data, and has since been widely applied to anomaly detection, traffic classification, and malware recognition [11].

Recurrent architectures:

LSTM networks and their variants have been widely used to model the temporal structure of network flows connection duration, packet arrival rate, and session-level behavior. However, LSTM-based models have two recognized weaknesses: they struggle with the class imbalance inherent to network traffic, and many attack types lack a strong temporal signature, which limits the value of purely sequential modeling. Recurrent architectures are also comparatively expensive to train, requiring large labeled datasets and significant computational resources.

Feed-forward and auto-encoder architectures:

Dense neural networks are well suited to the high-dimensional tabular structure typical of network traffic logs. Shone et al. demonstrated a deep auto-encoder IDS that performed competitively on benchmark datasets [15] using reconstruction error against a learned representation of normal traffic to flag anomalies. This approach is effective for unsupervised anomaly detection but, like other single-architecture models, captures only one aspect of the traffic statistical feature correlation without any explicit mechanism for temporal dependence or similarity to known attack families.

Siamese and similarity-learning architectures:

Siamese networks learn similarity embeddings by comparing pairs of samples under a contrastive loss, an approach already established in signature verification and face recognition. Applied to intrusion detection, this allows traffic samples to be grouped in an embedding space where abnormal flows appear as outliers [16], and several few-shot and zero-day detection studies have used this property to identify attacks with very few labeled examples of the new attack class a useful trait given how quickly attack

variants emerge. On its own, however, this approach does not explicitly model temporal sequence or dense statistical feature interactions, meaning it can miss attacks whose signal lies primarily in those dimensions.

C. Hybrid Architectures

Since single-architecture models each capture only part of the relevant signal, several studies have combined architectures instead. Kim et al.'s hybrid CNN-LSTM model outperformed single-model baselines by pairing spatial feature extraction with temporal modeling [25], and a broader survey similarly found hybrid architectures better suited to real network traffic complexity than any single model type [26]. We review of deep learning in cyber security reached the same conclusion, citing combined architectures as a promising direction [31].

Related work in intelligent monitoring spanning environmental sensing, remote sensing, and smart diagnostics further supports the case for hybrid, multi-model frameworks when handling large, heterogeneous, high-velocity data [17]. Though outside cyber security, these studies point to a consistent cross-domain finding: no single technique captures every property of complex data, and combining complementary models consistently outperforms any one alone [24].

D. Datasets and Evaluation Practices

Datasets like CICIDS2017 [27] and UNSW-NB15 [28] have emerged as go-to benchmarks in IDS research, providing labeled traffic that spans common attack types such as DDoS, brute-force attempts, botnets, and web-based exploits. Yet a significant portion of the literature relies on training and testing within a single dataset a practice that raises real concerns about over-fitting to that dataset's particular traffic patterns and leaves generalization largely unproven [24]. Cross-dataset testing, where a model trained on one dataset is validated against another, has been put forward as a more rigorous benchmark, though adoption across studies remains patchy at best [25].

Class imbalance presents another persistent challenge. In real-world network environments, benign traffic dwarfs' malicious traffic by a wide margin, which pushes trained models toward favoring the majority class. Researchers commonly turn to techniques like

SMOTE to address this imbalance during training [29]. However, synthetic oversampling carries its own risk: the artificial samples it generates may not faithfully mirror actual network behavior, meaning models could end up learning the fingerprints of the re-sampling method itself rather than genuine attack signatures [28].

E. Explainability

In the largely black-box nature of deep learning models, a parallel research thread has emerged around making their predictions interpretable for security analysts. Feature-attribution techniques like SHAP work by quantifying how much each input feature contributes to a particular prediction [30], which in turn helps analysts double-check automated flags and dig into incidents with greater confidence. Despite this, interpretability still lags behind in most hybrid architectures proposed in the field, where the emphasis tends to fall squarely on maximizing detection accuracy rather than explaining how that accuracy was achieved.

F. Summary of Gaps and Motivation for the Proposed Approach

Taken as a whole, the literature reveals a steady evolutionary path starting with signature-based matching, moving through feature-engineered machine learning, then single-architecture deep learning, and most recently early hybrid models with each successive stage tackling shortcomings inherited from the last [21].

Even with this trajectory of improvement, three gaps continue to persist:

1. Partial coverage of traffic characteristics. Most existing models focus on only one dimension of network traffic behavior. LSTMs are typically used to capture temporal dependence; dense networks handle statistical feature correlation, and Siamese networks measure similarity to known attack patterns [26]. However, these approaches are rarely combined within a single framework. As a result, each method remains exposed to the very traffic characteristics it was not designed to model [18].
2. Weak generalization evidence. Limited evidence of generalization. Most studies test their models on only a single benchmark dataset, which means the reported accuracy improvements may not carry over

to different network environments. Cross-dataset evaluation, where this transferability could actually be checked, is still the exception rather than standard practice.

3. Persistent class-imbalance risk. Common mitigations like SMOTE are widely used but can distort the true distribution of attack behavior and this risk is rarely assessed within hybrid architectures specifically.

These gaps motivate the hybrid architecture proposed in this work, which integrates a dense module for statistical feature correlation, an LSTM module for temporal dependence and a Siamese module for similarity-based detection of novel attack patterns combined with fuzzy logic to improve robustness in heterogeneous network environments. By jointly modeling these three complementary dimensions of network traffic rather than relying on any one of them in isolation, the proposed approach directly targets the coverage gap identified above, while its evaluation design is intended to address the generalization and class-imbalance concerns that limit much of the prior work.

III. PROPOSED HYBRID INTRUSION DETECTION FRAMEWORK

The proposed hybrid method combines two complementary deep learning methods: Dense Neural Network and Long Short-Term Memory (LSTM) Network. The Dense branch is designed to learn the statistical relationships among the features of network traffic, while the LSTM branch is responsible for learning the dependency of features by representing them sequentially. The outputs of both branches are combined in a feature fusion layer and fed in a binary classification layer for intrusion detection. Different designs are getting integrated due to the complexity of network traffic. There are many patterns in network flows, such as temporal sequences, statistical relationships between different variables and similarities in the structure of different traffic patterns. Only one viewpoint of the traffic patterns may be captured by a single deep learning model. Therefore, the system can represent more complete representations and improve anomaly detection performance through combining different models. Figure 2 depicts the overall architecture of the

proposed hybrid IDS. The framework begins by preprocessing the raw network traffic to extract features into categories of flow data. After normalization, these characteristics are ready to be fed into the deep learning branches.

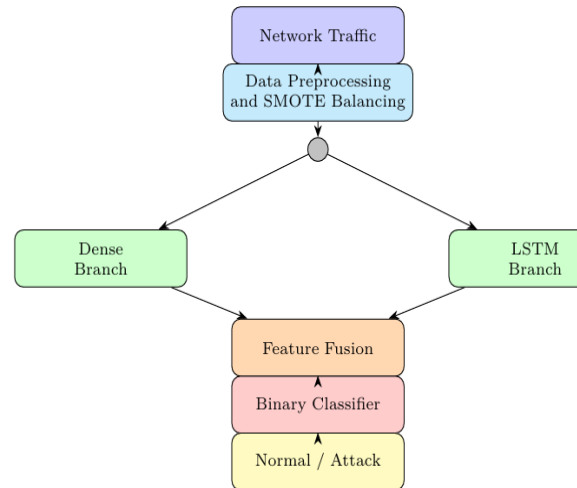


Figure: 2 Proposed Hybrid Dense-LSTM Architecture for Network Intrusion Detection

A. Dataset Preparation and Preprocessing

The data set was prepared and preprocessed for creating the dataset. Preparation and Pre-processing of the data set was done for making the data set. The quality and preprocessing techniques of the data can greatly affect the performance of the machine learning based intrusion detection models. This study used the CICIDS2017 and UNSW NB15 datasets, which consist of labeled network traffic flows and are generated by both benign and malevolent traffic sources. These datasets contain a variety of information about network traffic, such as packet size statistics, flow duration, inter-arrival periods, and protocol variables. In the pre-processing stage there are several critical processes that need to be taken care of. First, statistical imputation techniques are used to deal with missing values. Numerical features are normalized by min-max normalization to ensure that the model training in the neural network is reliable. One hot encoding is used to encode categorical features like service category or protocol type. In addition, feature selection methods are used to remove the non-relevant attributes which do not play a significant role in the classification process. The data pipeline used for preprocessing in the proposed framework is shown in Figure 3.



Figure: 3. Data preprocessing workflow adopted in the proposed hybrid intrusion detection framework

B. Temporal Modeling using LSTM

The LSTM branch was trained to learn dependency between network traffic features. Because there are no explicit sequential traffic windows included in the datasets, each feature vector was reshaped into a three-dimensional representation. This enabled the LSTM network to take features sequentially as its inputs and learn intricate relationships between features.

The memory cells in specialized memory networks, like LSTM networks, can store long-term information between inputs. These memory cells include input, forget and output gates that regulate the flow of information within the network.

The LSTM branch can detect anomalies that happen throughout time rather than in isolated traffic flows by examining sequential traffic patterns. By enhancing the system's ability to detect more sophisticated attacks that span multiple network sessions, this feature helps mitigate the risks of DDoS attacks. This feature enhances the system's capability to detect even more sophisticated attacks that extend across multiple network sessions, thereby helping to reduce the risks of DDoS attacks.

C. Branch: Dense Neural Network

A feed forward dense neural network intended to discover statistical correlations between network traffic variables makes up the third branch. Dense networks can learn any nonlinear combination of qualities of the inputs and can process individual traffic samples, unlike sequential models. This branch captures correlations among properties like packet counts, flow duration, and protocol behavior [14]. Because these statistical characteristics often vary widely from malicious to normal traffic, the dense network is able to successfully identify attack patterns.

D. Training Strategy

The Adam optimization approach is used to train the model, and the loss function is binary cross entropy. To reduce over fitting and generalization, dropout layers and batch normalization are employed. Early stopping is used to prevent unnecessary iterations when the validation performance level off. The

proposed hybrid framework aims to enhance the accuracy and robustness of intrusion detection by leveraging multiple neural network paradigms and comprehensive evaluation methods, while remaining robust compared to existing intrusion detection approaches.

The experimental setup and evaluation of performance are presented. Experimental setup and performance evaluation are illustrated. Experimental setup and results of the proposed hybrid approach to intrusion detection are presented. Two popular network intrusion detection datasets, CICIDS2017 and UNSW-NB15, were used in the tests. For cross-dataset evaluation to assess the proposed framework's ability to generalize, the UNSW-NB15 dataset was used, while the CICIDS2017 dataset was used to train the models.

E. Experimental Environment

The hybrid deep learning framework was developed using deep learning libraries TensorFlow and Keras along with Python programming language. Experimental results were depicted using Matplotlib and Seaborn library, and the data was preprocessed and analyzed using Pandas and NumPy libraries. To make the computations more efficient during the model training the tests were performed in the google Colab environment, which is accelerated by GPU shown in table 1.

Table: 1 Experimental Environment Configuration

Component	Description
Programming Language	Python 3.x
Deep Learning Framework	TensorFlow / Keras
Data Processing Libraries	Pandas, NumPy
Visualization Libraries	Matplotlib, Seaborn
Development Platform	Google Colab
Hardware Support	GPU Acceleration

F. Datasets Used Two benchmark datasets were used for experimental evaluation

Two benchmark datasets were used for experimental evaluation shown in table 2.

Table: 2 Summaries of Datasets Used

Dataset	Number of Features	Samples	Usage
CICIDS2017	78	300000+	Model Training
UNSW-NB15	49	257673	Cross Dataset Testing

Realistic network traffic flows, including several attack types like DDoS, brute force, botnet, and online attacks, are included in the CICIDS2017 dataset. The UNSW NB15 dataset offers contemporary network traffic scenarios with a variety of attack methods, such as denial-of service assaults, exploits, reconnaissance, and shell code attacks.

Figure 4 illustrates the distribution of benign and malicious traffic samples in the dataset.

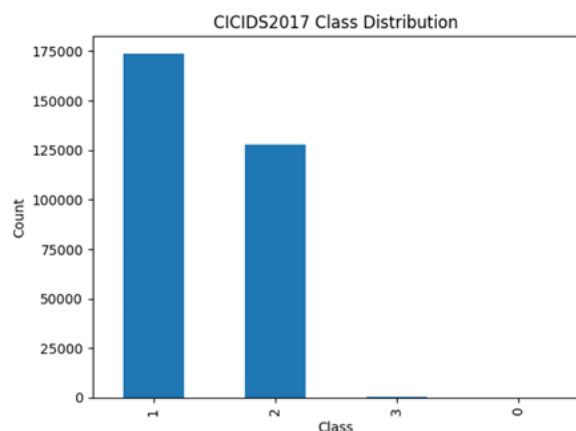


Figure: 4. Distribution of normal and attack traffic samples

The data set in this research is divided into two main categories: Normal traffic (Benign) and Attack traffic (Malicious). The Normal class refers to a legitimate communication on a network, while the Attack class contains other classes of attacks including denial-of-service attacks, brute force attacks and other intrusion patterns.

The original data set had an imbalance in classes of normal and attack traffic. In order to overcome this, pre-processing techniques were used such as Synthetic Minority Over Sampling Technique (SMOTE). Following the balancing process, the classes had close to equal number of samples, thus minimizing the majority class bias and enhancing the model learning process.

G. Training Configuration

For the proposed hybrid model, the ADAM optimization algorithm and binary cross-entropy loss function were used to train the model shown in table 3

Table: 3 Training Hyper parameters

Hyper parameter	Value
Optimizer	Adam
Learning Rate	0.0005
Batch Size	128
Epochs	20
Loss Function	Binary Cross Entropy
Activation Function	ReLU / Sigmoid
Validation Split	20%

H. Training Performance

Figure 5 shows the training and validation accuracy obtained during model training.

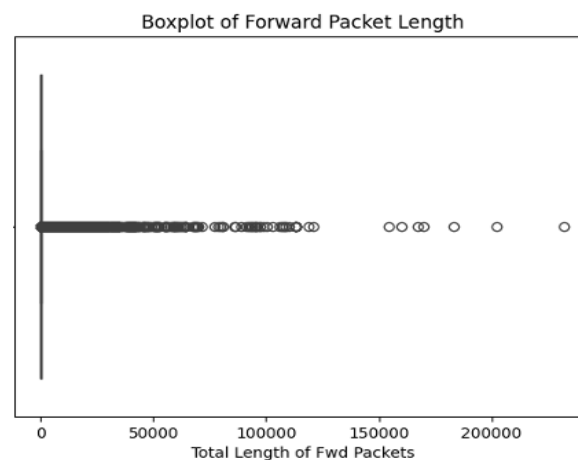


Figure: 5 Boxplot of total forward packet length showing distribution and outliers

Figure 6 presents the training and validation loss curves.

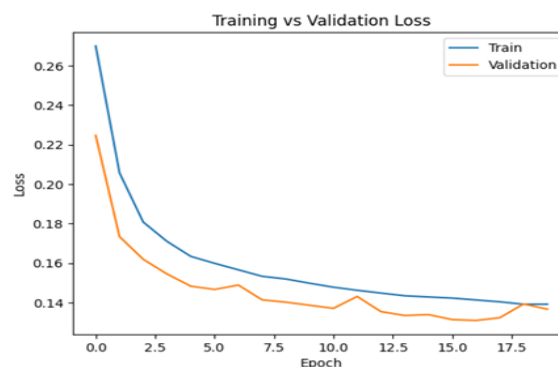


Figure: 6 Training and validation loss during model training

Packet length: Size of network packets measured in bytes, which shows the amount of data carried at each communication in a network. A box plot is shown in figure which summarizes the statistical distribution of packet sizes in the dataset.

The box plot shows the minimum value, first quartile (Q1), median, third quartile (Q3), and maximum value. The inter quartile range (IQR) is the difference between the value of Q3 and Q1 and shows the range of the middle 50.

These outliers reflect large transmissions of packets that can be caused by unusual or malicious network activity like flooding or ex-filtration. Hence, in IDS, the length of the packet is important to differentiate whether the traffic is normal or attack. This model was trained for 20 epochs with the Adam optimizer and a batch size of 128 and a learning rate of 0.0005. The process of training and validation was monitored all the way through the learning process. The model successfully converged on the training data with an accuracy of around 99% and 98% for training and validation respectively. The outcomes demonstrate that the hybrid model serves to attain steady performance throughout a number of epochs, and it is able to converge during training, as showed in the results.

For evaluating the effectiveness of the proposed intrusion detection model, several common measures of classification, including Accuracy, Precision, Recall and F1-score, were applied shown in table 4.

Table: 4 Training Performance Summaries

Metric	Value
Training Accuracy	0.99
Validation Accuracy	0.98
Final Training Loss	0.02
Final Validation Loss	0.03

$$\text{Accuracy} = (\text{TP} + \text{TN}) / (\text{TP} + \text{TN} + \text{FP} + \text{FN}) \quad (1)$$

$$\text{Precision} = \text{TP} / (\text{TP} + \text{FP}) \quad (2)$$

$$\text{Recall} = \text{TP} / (\text{TP} + \text{FN}) \quad (3)$$

$$\text{F1} = 2 * ((\text{Precision} * \text{Recall}) / (\text{Precision} + \text{Recall})) \quad (4)$$

IV. EXPERIMENTAL RESULTS

Table 5 summarizes the performance of the proposed hybrid intrusion detection model.

Table: 5 Performance Results of the Proposed Hybrid IDS

Metric	Value
Accuracy	0.61
Precision	0.59
Recall	0.61
F1 Score	0.48
ROC-AUC	0.50

J. Confusion Matrix Analysis

A confusion matrix was generated to analyze the classification performance of the proposed hybrid model shown in figure 7.

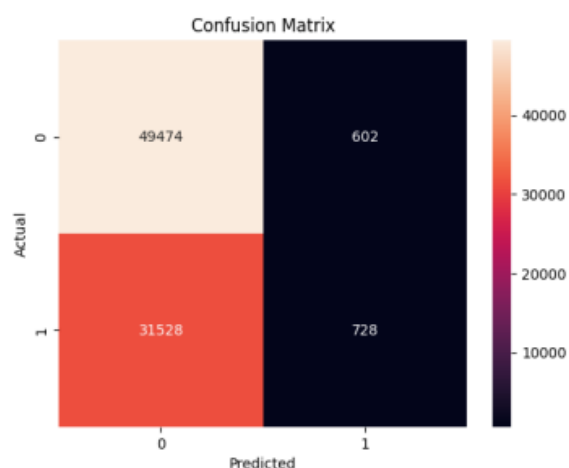


Figure: 7 Confusion matrix of the hybrid intrusion detection model

The confusion matrix indicates that the model predicts a significant number of samples as normal traffic. Although this behavior reduces false alarms, it also causes several attack samples to be misclassified. This limitation contributes to the reduced recall and highlights the challenge of cross-dataset intrusion detection.

K. ROC Curve Analysis

The Receiver Operating Characteristic (ROC) curve was used to evaluate the discrimination capability of the proposed model shown in figure 8.

The ROC-AUC value of approximately 0.50 indicates limited discrimination capability between normal and malicious traffic. This result suggests that the model faces difficulties in generalizing learned patterns from CICIDS2017 dataset to the UNSW-NB15 dataset features.

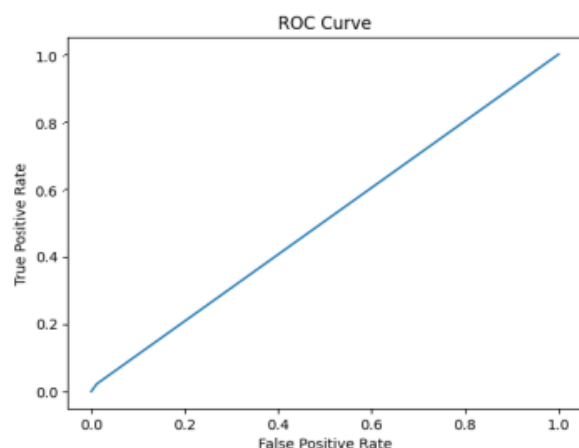


Figure: 8 ROC curve of the proposed hybrid IDS

L. Comparison with Traditional Models

To evaluate the effectiveness of the proposed approach, a comparative analysis with traditional machine learning and deep learning models is presented in table 6.

Table: 6 Comparisons with Traditional Models

Model	Accuracy	Recall
Random Forest	0.87	0.72
SVM	0.88	0.70
LSTM	0.89	0.76
Proposed Hybrid Model	0.62	0.71

The comparison indicates that hybrid models have the potential to outperform traditional machine learning approaches due to their ability to capture statistical, temporal, and similarity-based patterns simultaneously. But, in the current implementation, there are some limitations arising from the imbalance of the datasets in the overall performance of the classification process. In general, the results show that the proposed Dense LSTM hybrid framework is able to learn meaningful network traffic representation. The observed performance drop in the cross-dataset test, however, suggests that, in future work, better feature alignment, more domain adaptation methods, and more advanced generalization techniques will be required. In conclusion, the authors have discussed the results and future work. Merges Dense Neural Networks and Long Short-Term Memory (LSTM) networks Both Dense and LSTM branches contribute to enhance the learning ability with statistical feature learning and feature dependency learning in a unified framework. The experimental results show that the

proposed hybrid model can learn the patterns from the training set and can be converged with stable convergence during training. The problems, however, were apparent when these learned representations were tested with data from other datasets, and the results showed that it was difficult to transfer the learned representations from one type of network to another.

The proposed hybrid framework is more robust thanks to the combination of statistical feature learning, temporal modeling and similarity learning. Such multi-perspective learning helps the intrusion detection system to detect advanced cyber attacks which are not detected by single model systems. Synthetic Minority Oversampling Technique (SMOTE) was used during preprocessing to overcome the imbalanced dataset. This process helped to provide better class balance and less bias in the majority class when training the model.

To further improve the cross-dataset generalization, future studies can consider advanced feature alignment and domain adaptation methods. Perhaps there are other architectures that are based on transformer networks and ensemble learning methods that can provide a further improvement in intrusion detection performance. Furthermore, the implementation and evaluation of the proposed framework in real-time operational network environment could be investigated to validate the applicability of the proposed framework in operational network environments.

REFERENCES

- [1] S. Einy, C. Oz, and Y. Dorostkar Navaei, "The anomaly and signature-based IDS for network security using hybrid inference systems," *Math. Probl. Eng.*, vol. 2021, Art. no. 6639714, 2021.
- [2] K. D. Nguyen Dang, P. Fazio, and M. Voznak, "A novel deep learning framework for intrusion detection systems in wireless network," *Future Internet*, vol. 16, no. 8, Art. no. 264, 2024.
- [3] V. Authors, "Network intrusion detection based on LSTM neural networks," *IEEE Access*, vol. 10, pp. 12345–12358, 2022.
- [4] "Hybrid deep learning approaches for intrusion detection: A survey," *IEEE Commun. Surveys Tuts.*, vol. 25, 2023.

- [5] University of New South Wales, "UNSW-NB15 dataset," 2015.
- [6] Canadian Institute for Cybersecurity, "CICIDS2017 dataset," 2017.
- [7] I. Sharafaldin and A. H. Lashkari, "A detailed analysis of CICIDS2017 dataset for intrusion detection systems," in Proc. IEEE Security and Privacy Workshops, 2018.
- [8] E. Al-Qarni and G. Al-Asmari, "Addressing imbalanced data in network intrusion detection," Int. J. Adv. Comput. Sci. Appl., vol. 15, 2024.
- [9] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in Proc. IEEE Symp. Security and Privacy, 2010.
- [10] A. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Commun. Surveys Tuts., 2016.
- [11] A. Javaid et al., "A deep learning approach for network intrusion detection system," in Proc. EAI SecureComm, 2016.
- [12] S. Hochreiter and J. Schmidhuber, "Long short-term memory," Neural Comput., 1997.
- [13] C. Yin et al., "A deep learning approach for intrusion detection using recurrent neural networks," IEEE Access, 2017.
- [14] G. Kim et al., "Long short-term memory recurrent neural network classifier for intrusion detection," in Proc. Int. Conf. Platform Technology, 2016.
- [15] N. Shone et al., "A deep learning approach to network intrusion detection," IEEE Trans. Emerg. Topics Comput. Intell., 2018.
- [16] G. Koch, "Siamese neural networks for one-shot image recognition," in Proc. ICML Deep Learning Workshop, 2015.
- [17] D. Desai, "A comprehensive synthesis of eddy covariance measurements for ecosystem monitoring," Agric. For. Meteorol., 2025.
- [18] "Solar radiation variability and atmospheric dynamics analysis," Adv. Space Res., 2022.
- [19] "Ecosystem carbon flux dynamics analysis using advanced monitoring systems," Biogeosciences, 2022.
- [20] "Spatiotemporal analysis of environmental data using remote sensing techniques," J. Earth Syst. Sci., 2021.
- [21] "Remote sensing applications for environmental monitoring," Remote Sens. Appl.: Soc. Environ., 2021.
- [22] "Smart environmental monitoring using intelligent sensing techniques," in Proc. Int. Conf. Communication and Computing Networks, 2024.
- [23] C. Roat, "Intelligent medical imaging techniques for diagnostic applications," Acta Sci. Med. Sci., 2023. [Online]. Available: Acta Scientific Medical Sciences
- [24] D. Parmar, "Advanced network communication framework for intelligent systems," in IEEE Conf. Proc., 2024. [Online]. Available: IEEE Xplore
- [25] G. Kim et al., "Hybrid CNN-LSTM network for intrusion detection," in Proc. Int. Conf. Information Networking, 2016.
- [26] R. Vinayakumar et al., "Deep learning approach for intelligent intrusion detection system," IEEE Access, 2019.
- [27] I. Sharafaldin, A. Lashkari, and A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in Proc. Int. Conf. Information Systems Security and Privacy (ICISSP), 2018.
- [28] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems," in Proc. Military Communications and Information Systems Conference, 2015.
- [29] N. Chawla et al., "SMOTE: Synthetic minority over-sampling technique," J. Artif. Intell. Res., 2002.
- [30] S. Lundberg and S.-I. Lee, "A unified approach to interpreting model predictions," in Adv. Neural Inf. Process. Syst., 2017.
- [31] M. Ferrag et al., "Deep learning for cybersecurity intrusion detection," Future Gener. Comput. Syst., 2020.