International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

A Hybrid LSTM-Based Framework for Accurate and Real-Time DDoS Detection in Cloud Environments

Anjali Saxena
M.E Scholar, Department of Computer Science and Engineering, Maharana Pratap College of Technology, Gwalior, MP

Unmukh Datta
Associate Professor, Department of Computer Science and Engineering, Maharana Pratap College of Technology, Gwalior, MP

Abstract-This study presents a comprehensive methodology for advanced Distributed Denial of Service (DDoS) detection in cloud-hosted websites using a hybrid approach combining Covariance Matrix Analysis with Machine Learning (ML) and Deep Learning (DL) models. Publicly available datasets, including CIC-IDS2017 serve as the primary data sources, containing both normal and malicious network traffic patterns. Data preprocessing involves cleaning, encoding, and normalization to ensure data quality and consistency, followed by feature extraction to identify critical network attributes such as packet size, session data, and traffic volume. Covariance Matrix Analysis is employed to capture feature interactions and highlight essential trends, aiding in dimensionality reduction and enhancing model interpretability. The proposed hybrid approach leverages ML models like Support Vector Machine (SVM), K-Nearest Neighbors (KNN), and Random Forests (RF), alongside DL models such as Convolutional Neural Networks (CNN), to accurately detect DDoS attacks. Comparative analysis evaluates the hybrid model against conventional detection techniques, focusing on false positive rates, detection accuracy, and sensitivity to high-volume, low-rate attacks. Performance metrics, including accuracy, precision, recall, F1-score, and ROC-AUC, assess the model's effectiveness in real-time attack detection across various traffic scenarios. The expected outcomes include the development of a robust, low-computational overhead DDoS detection model, a structured dataset for attack analysis, and the identification of key network features that significantly impact detection accuracy.

Keywords-DDoS Detection, Covariance Matrix Analysis, Intrusion Detection System (IDS), Machine Learning (ML), Network Traffic Analysis.

I. INTRODUCTION

In the digital age, the proliferation of internet-connected systems and services has transformed how organizations operate, communicate, and deliver value. However, this increasing reliance on digital networks has also intensified exposure to malicious cyber activities, making network security a primary concern for governments, businesses, and individuals alike[1]. To mitigate these risks, Intrusion Detection Systems (IDS) have become an integral part of cybersecurity infrastructure, designed to monitor network traffic and detect suspicious behavior. Traditional IDS approaches, which often rely on signature-based or heuristic rules, struggle to cope with the sophistication, variety, and rapid evolution of modern cyber threats[2]. This limitation has driven the adoption of machine learning (ML) and, more recently, deep learning (DL) techniques to build more adaptive, intelligent, and effective intrusion detection solutions. One of the most promising DL methods for intrusion detection is the Long Short-Term Memory (LSTM) network, a type of Recurrent Neural Network (RNN) specifically designed to learn from sequential data[3]. Unlike conventional neural networks, LSTM is capable of capturing long-term dependencies in time-series data, which is particularly useful when analyzing sequences of network packets or flow behaviors[4]. This unique capability allows LSTM models to

detect patterns of intrusion that unfold over time, such as slow brute-force attacks or data exfiltration attempts, which may not be evident through static analysis alone. By leveraging LSTM networks, researchers can develop systems that not only identify known attack patterns but also generalize to detect previously unseen threats[5].

The efficacy of such a system heavily depends on the quality and comprehensiveness of the dataset used for training and evaluation. In this context, the CIC-IDS2017 dataset, created by the Canadian Institute for Cybersecurity, offers a robust and realistic foundation for intrusion detection research[6]. It includes a wide range of labeled network traffic data, covering both benign and malicious behaviors across various attack scenarios such as Distributed Denial of Service (DDoS), infiltration, port scanning, brute force login attempts, and botnet activities. The dataset was collected in a controlled environment, simulating real-world usage scenarios and adhering to practical network configurations[7]. It contains time-stamped features from network flows, making it ideal for training LSTM models, which rely on temporal patterns and sequential analysis.The proposed research aims to implement an LSTM-based approach to network intrusion detection using the CIC-IDS2017 dataset. The goal is to develop a model that can effectively identify intrusions by analyzing sequences of network activities, using the temporal dynamics of traffic flows to differentiate between normal and abnormal behavior[8]. In doing so, the study will assess the model's performance using standard evaluation metrics such as accuracy, precision, recall, and F1-score, while also exploring its capability to generalize to various attack types. A comparative analysis may also be conducted against traditional ML models to highlight the advantages of using LSTM networks in the domain of intrusion detection[9].

Moreover, this research will examine the challenges associated with deep learning-based IDS systems, including issues of computational overhead, real-time applicability, data imbalance, and false positive rates. It will explore strategies for optimizing the model, such as data preprocessing, feature selection, and hyperparameter tuning[10]. The broader objective is to contribute to the development of intelligent, scalable, and efficient IDS frameworks that can enhance the overall cybersecurity posture of networked systems in both enterprise and national contexts.As cyber threats continue to evolve, the need for adaptive and automated defense mechanisms becomes more critical. By combining the strengths of LSTM networks with the real-world fidelity of the CIC-IDS2017 dataset, this study seeks to advance the frontier of network intrusion detection and provide actionable insights for the deployment of next-generation IDS solutions[11].

II. Literature Review

Raja Waseem Anwar (2025) et. al This study develops a federated learning framework with LSTM networks for efficient intrusion detection in IoT-based WSNs, enhancing detection accuracy, reducing false positives, and ensuring data privacy. The model was tested on WSN-DS, CIC-IDS-2017, and UNSW-NB15 datasets[12].

Fatimah Alhayan (2025) et.al The proposed EAID-OADRHM technique presents a new approach for perceiving and migrating attacks in cybersecurity. Min–max scaling normalization is primarily employed at the data pre-processing level to clean and transform input data into a consistent range. Furthermore, the proposed EAID-OADRHM technique utilizes the equilibrium optimizer (EO) model for the dimensionality reduction process. Additionally, the classification is performed by employing the long short-term memory and autoencoder (LSTM–AE) model[13].

Niccolò Borgioli (2024) et.al This paper introduces an anomaly-based IDS that uses unsupervised neural models to learn expected network traffic, detecting both known and novel attacks. The solution employs an autoencoder to reconstruct received packets and identify malicious ones based on reconstruction errors. Through careful model optimization, detection accuracy was improved, and detection time reduced. Implemented on a real embedded platform, the system outperforms existing

IDS approaches in detection accuracy, inference time, generalization, and robustness to poisoning, a commonly overlooked issue in current IDSs[14].

Syed Muhammad Salman Bukhari (2024) et.al This paper proposes a novel Stacked Convolutional Neural Network and Bidirectional Long ShortTerm Memory (SCNN-Bi-LSTM) model for intrusion detection in WSNs. This model leverages Federated Learning (FL) to enhance intrusion detection performance and safeguard privacy. The FL-based SCNN-Bi-LSTM model is unique in its approach, allowing multiple sensor nodes to collaboratively train a central global model without revealing private data, thereby alleviating privacy concerns[15].

Baraa I. Farhan (2024) et.al This solution proposes a hybrid algorithm that utilizes feature selection to optimize the process by identifying the most relevant features. It integrates three methods to reduce features, removing static ones with minimal information gain before training the LSTM deep learning model on the CSE-CIC-IDS dataset. This preprocessing improves system performance by reducing processing time and enhancing detection rate and accuracy. Experimental results demonstrated an impressive accuracy of 99.84%[16].

TABLE.1 LITERATURE SUMMARY

Author/Year	Methodology	Result	Limitation
Hussein Ridha Sayegh (2024)[17]	An LSTM-based IDS was developed using SMOTE for class balancing and RFE for feature selection on CICIDS2017, NSL-KDD, and UNSW-NB15 datasets.	The model achieved high accuracy rates: 99.34%, 99.67%, and 98.31% on CICIDS2017, NSL-KDD, and UNSW-NB15 respectively.	SMOTE may not capture real-world attack complexity, and the model hasn't been tested in live IoT environments.
Nureni Ayofe Azeez (2024) [18]	The study evaluated CNN and RNN models on NSL-KDD and CICIDS2017 using accuracy, precision, recall, F1-score, AUC, and error rate.	RNN outperformed CNN on NSL-KDD, while CNN slightly surpassed RNN on CICIDS2017 in accuracy and precision.	Model performance varied across datasets, highlighting that effectiveness depends on data characteristics and may not generalize.
Mahdi Soltan (2024) [19]	Proposed a multi-agent IDS framework with continual learning, federated learning, and LSTM/CNN for detection.	CNN achieved 95% detection with 128 new flows, while LSTM detected intrusions using the first 15 packets.	The system needs further validation in real-world, high-speed, multi-agent deployments.
Jalal Ghadermazi (2024)[20]	SPIN-IDS converts packet sequences into images and	Achieved 97.7%–99% detection rates, identifying threats by	High computational cost, focus on

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

	applies CNN for real-time attack detection.	the ninth packet with 95% transferability.	packet-level data, and potential flow-level oversight.
SANDEEPKUMAR RACHERLA (2024) [21]	Deep-IDS uses a 64-unit LSTM to detect five intrusion types in real-time with optimized DR-FAR trade-off.	Achieved 97.67% accuracy, 98.17% recall, and 1.49-second detection time using ADAM and He initialization	Focused on five intrusion types, resource-intensive, and requires tuning for diverse datasets

III. METHODOLOGY

Realistic network traffic containing both benign and different attack types—e.g., DDoS, Brute Force, Infiltration—comprises the CICIDS2017 dataset used in this paper. Missing value management, label encoding, numerical conversion, and StandardScaler-based standardisation processed the dataset.Using reciprocal information ratings, feature selection was carried out to keep the top 10 most informative features. The dataset was then divided in an 80:20 ratio into training and test sets. Exploratory data analysis (EDA) showed class imbalance, feature skewness, and multicollinearity, which guided more preprocessing techniques.

ML models and Keras built a Long Short-Term Memory (LSTM) deep learning model. Optimised with the Adam optimiser, it comprised two LSTM layers (64 and 32 units), batch normalisation, dropout regularisation, and dense layers. With a batch size of 32, the model was trained for 100 epochs.

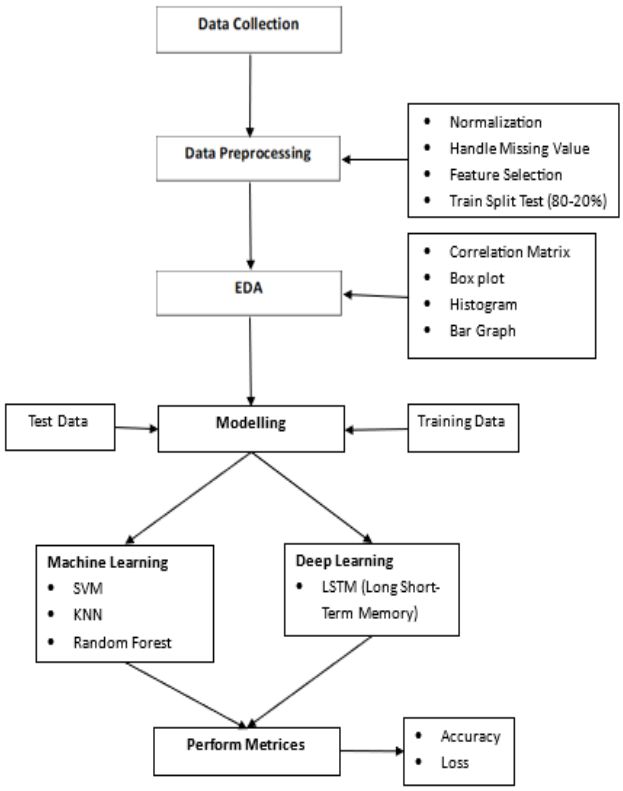


Figure 1 Proposed Flowchart

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

A. Dataset Collection

The CICIDS2017 dataset is used in Intrusion Detection Systems (IDSs) and its available on [22] Intrusion Prevention Systems (IPSs) are the most important defense tools against the sophisticated and ever-growing network attacks. Due to the lack of reliable test and validation datasets, anomaly-based intrusion detection approaches are suffering from consistent and accurate performance evolutions.

Our evaluations of the existing eleven datasets since 1998 show that most are out of date and unreliable. Some of these datasets suffer from the lack of traffic diversity and volumes, some do not cover the variety of known attacks, while others anonymize packet payload data, which cannot reflect the current trends. Some are also lacking feature set and metadata.

CICIDS2017 dataset contains benign and the most up-to-date common attacks, which resembles the true real-world data (PCAPs). It also includes the results of the network traffic analysis using CICFlowMeter with labeled flows based on the time stamp, source, and destination IPs, source and destination ports, protocols and attack (CSV files).

Generating realistic background traffic was our top priority in building this dataset. We have used our proposed B-Profile system (Sharafaldin, et al. 2016) to profile the abstract behavior of human interactions and generates naturalistic benign background traffic. For this dataset, we built the abstract behaviour of 25 users based on the HTTP, HTTPS, FTP, SSH, and email protocols.

The data capturing period started at 9 a.m., Monday, July 3, 2017 and ended at 5 p.m. on Friday July 7, 2017, for a total of 5 days. Monday is the normal day and only includes the benign traffic. The implemented attacks include Brute Force FTP, Brute Force SSH, DoS, Heartbleed, Web Attack, Infiltration, Botnet and DDoS. They have been executed both morning and afternoon on Tuesday, Wednesday, Thursday and Friday.

B. Data Preprocessing

The data preprocessing process begins by removing rows containing missing values using the dropna() method. Additionally, any leading or trailing spaces in column names are stripped to ensure consistency across the dataset. If the target column, 'Label', is present, it is encoded into numerical values using LabelEncoder, converting categorical labels into a format compatible with machine learning models. In the case that the 'Label' column is absent, a KeyError is raised.

The feature matrix X is created by dropping the 'Label' column, while the target variable yyy is retained separately. To ensure that the dataset is compatible with numerical operations, all feature columns are converted to numeric types, coercing non-numeric entries into NaNs. Infinite values are also replaced with NaNs, and any NaN values are subsequently filled with the respective column mean.

Finally, the features are standardized using StandardScaler, which transforms the data to have a mean of zero and a standard deviation of one. This normalization step is essential, as it ensures that all features contribute equally to the model, which is critical for the performance of many machine learning algorithms.

Formulas:

Label Encoding: $$y = LabelEncoder(y) \quad (1)$$

3.3 Feature Selection

For feature selection, the mutual information score is calculated between each feature and the target variable. The top 10 features with the highest scores are selected, helping to retain the most informative attributes while reducing dimensionality.

Formula:

$$I(X;Y) = \sum_{x \in X} \quad \sum_{y \in Y} \quad P(x,y).log\ log\ (\frac{P(x,y)}{P(x).P(y)}) \quad (2)$$

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

C. Data Splitting

Finally, the processed dataset is split into training and testing sets using an 80-20 ratio to prepare for model training and evaluation.

1. Training Set Size:

The number of samples in the training set N_{train} is calculated by:

$$N_{train} = p_{train} \times N \quad (3)$$

2. Test Set Size:

The number of samples in the test set N_{test} is calculated by:

$$N_{test} = p_{test} \times N \quad (4)$$

Where:

- N = Total number of data points in the dataset
- p_{train}, p_{test} = Proportions of the dataset used for training and testing, respectively.

D. Exploratory Data Analysis (EDA)

Exploratory data analysis (EDA) was conducted to examine a binary classification dataset containing BENIGN and DDOS traffic. The class distribution plot revealed an imbalance, with around 97,000 benign and 128,000 DDOS samples. This imbalance indicates the need for handling techniques like oversampling or class weighting to prevent model bias.

Boxplots of key features—including *Flow Duration*, *Total Fwd Packets*, *Flow IAT Mean*, and others—highlighted the presence of significant outliers and skewness. Most features showed a long-tail distribution, with a high concentration of lower values and some extreme spikes. Recognizing this is important, as outliers and skewed distributions can negatively affect model training, especially for algorithms sensitive to data range. Histograms further confirmed that many features are right-skewed, emphasizing the need for preprocessing steps such as normalization or log transformation to stabilize variance and improve model performance.

The correlation heatmap provided deeper insight into feature relationships. Strong correlations were found among features like *Flow Duration*, *Flow IAT Max*, and *Fwd IAT Total* (correlation > 0.9), indicating multicollinearity. Highly correlated features can inflate variance in model estimates, so dimensionality reduction or feature selection will be important to avoid redundancy and overfitting.

Overall, this EDA revealed crucial patterns: class imbalance, outliers, skewness, and correlated features. These findings inform preprocessing strategies essential for building an effective intrusion detection model. Steps like normalization, outlier management, balancing techniques, and careful feature selection will play a key role in improving model robustness and accuracy.

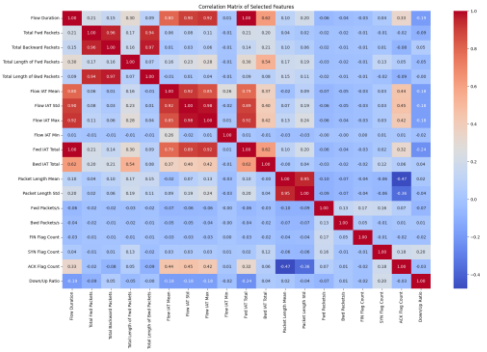


Figure 2 Correlation Matrix

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

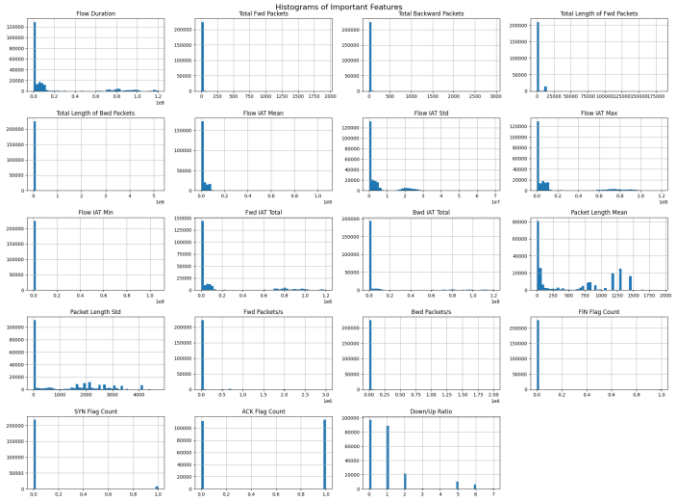


Figure 3 Histograms

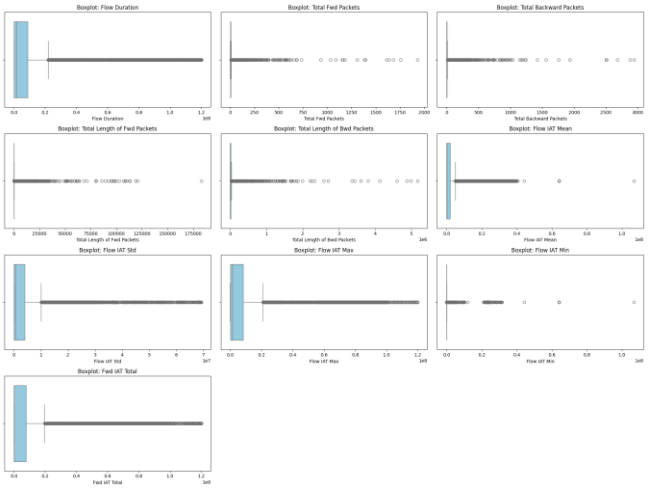


Figure 4 Boxplots

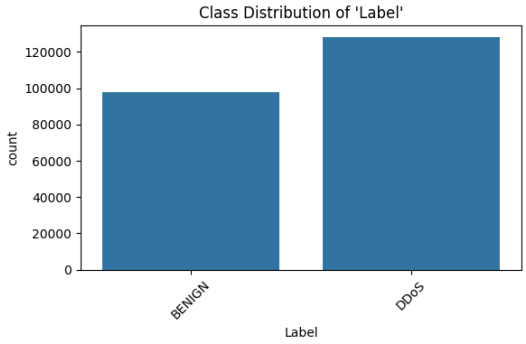


Figure 5 Label Distribution

E LSTM Deep Learning Model Description

A sequential deep learning model is constructed using Keras, tailored for binary classification tasks. The architecture begins with an LSTM (Long Short-Term Memory) layer containing 64 units, which captures temporal dependencies in sequential data. The return_sequences=True parameter allows the next LSTM layer to receive the full sequence output, enabling deeper temporal learning.

A BatchNormalization layer follows to stabilize and accelerate training by normalizing the outputs of the LSTM layer. This is succeeded by a Dropout layer with a rate of 0.3, which helps prevent overfitting by randomly deactivating 30% of the neurons during training. A second LSTM layer with 32 units is

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

added next, this time with return_sequences=False, meaning it outputs only the final state — suitable for feeding into dense layers.

Next, a Dense layer with 32 neurons and ReLU activation introduces non-linearity and allows the model to learn complex patterns. Another Dropout layer with a 0.3 rate is applied for regularization. Finally, a Dense output layer with a single neuron and sigmoid activation is used, making the model suitable for binary classification by outputting a probability score between 0 and 1.

Hyperparameter Table

Hyperparameter	Value
Model Type	LSTM (Sequential)
LSTM Units (Layer 1)	64
LSTM Units (Layer 2)	32
Dense Units	32
Activation (Dense)	ReLU
Output Activation	Sigmoid
Dropout Rate (Both)	0.3
Batch Normalization	Yes (after 1st LSTM)
Loss Function	Binary Crossentropy
Optimizer	Adam
Learning Rate	0.001
Epochs	100
Batch Size	32
Input Shape	(X_train.shape[1], 1)
Validation Data	Yes (X_test, y_test)

4. Results and Discussion

The implementation of both machine learning and deep learning models for network intrusion detection using the CICIDS2017 dataset yielded promising results. The performance evaluation was conducted using accuracy as the primary metric along with training loss for the LSTM model.

TABLE 2. MACHINE LEARNING MODELS RESULTS

Model	Training Accuracy	Test Accuracy
SVM	98.34	98.34
KNN	99.94	99.94
Random Forest	99.94	99.94

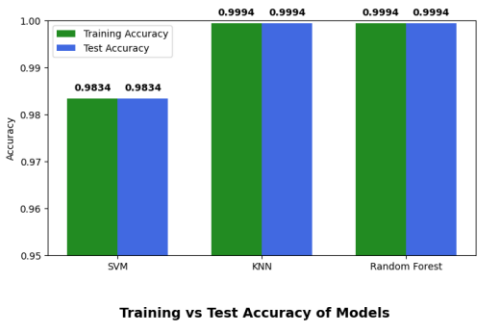


Figure 6 Performance of the machine learning models

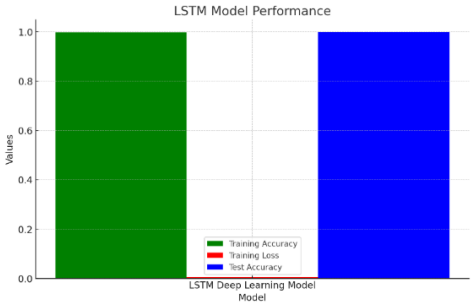
The performance of the machine learning models – SVM, KNN, and Random Forest – indicates that KNN and Random Forest achieved outstanding accuracies of 99.94% in both training and testing,

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

demonstrating exceptional consistency in detecting network intrusions. SVM, however, recorded slightly lower accuracy at 98.34%, suggesting it may not capture complex patterns as effectively as the other models. The identical training and testing accuracies for KNN and Random Forest may indicate potential overfitting, despite their high performance. Overall, KNN and Random Forest emerged as the top-performing models, effectively identifying benign and malicious traffic with near-perfect accuracy.

TABLE 3 DEEP LEARNING MODELS RESULT

Model	Training Accuracy	Training Loss	Test Accuracy
LSTM Deep Learning Model	99.84	0.0064	99.91



The Proposed LSTM deep learning model demonstrated strong performance with a training accuracy of 99.84% and a minimal training loss of 0.0064, indicating effective learning and minimal error during training. The test accuracy further improved to 99.91%, showcasing the model's ability to generalize well to unseen data. The slight increase in test accuracy compared to training accuracy suggests that the LSTM model effectively captures sequential patterns in the network traffic data without overfitting. This highlights its potential for robust intrusion detection, outperforming traditional machine learning models in terms of generalization and detection accuracy.

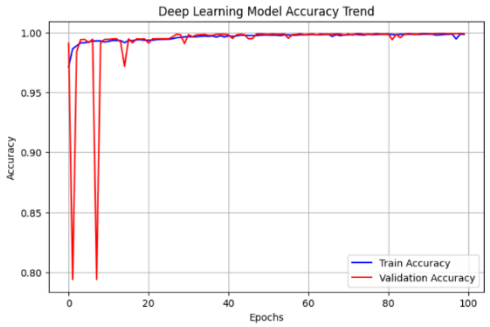


Figure 7 Accuracy curve of Deep learning Model

The graph shows the training and validation accuracy trends over 100 epochs, where both accuracies stabilize near 1.0, indicating strong model performance with minimal overfitting. Initial fluctuations in validation accuracy suggest early instability, but both curves align closely as training progresses.

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

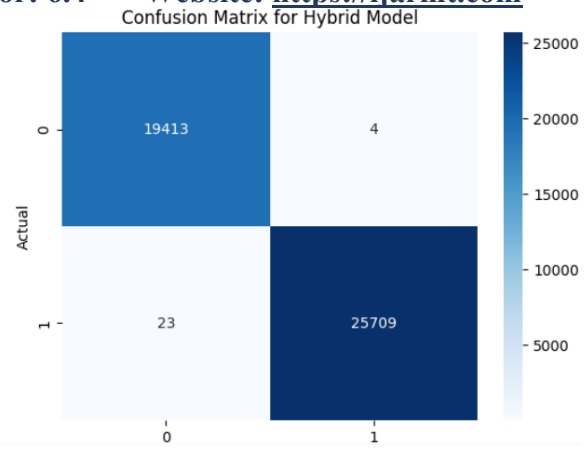


Figure 8 Confusion Matrix

This confusion matrix shows that the model correctly classified 52,103 DDOS and 13,473 BENIGN samples, with very few misclassifications (53 false negatives and 4 false positives), indicating high overall accuracy.

TABLE 4 COMPARATIVE ANALYSIS BETWEEN EXISTING AND PROPOSED MODELS

Study / Author	**Model / Technique**	**Dataset Used**	**Training Accuracy (%)**	**Test Accuracy (%)**	**Reference**
Hussein Ridha Sayegh (2024)	LSTM + SMOTE + RFE	CICIDS2017	99.34	99.34	[17]
Mahdi Soltan et al. (2024)	LSTM in Multi-Agent System	Custom Real-Time Dataset	95.00	96.20	[19]
Fatimah Alhayan et al. (2025)	LSTM–AE with Feature Reduction	UNSW-NB15	97.70	98.10	[13]
Proposed Model	**LSTM Deep Learning Model**	**CICIDS2017 dataset**	**99.84**	**99.91**	**--**

Table presents a comparative analysis between existing intrusion detection models and the proposed LSTM-based deep learning model. The table highlights the training and testing accuracy achieved by each approach using different datasets and techniques. For instance, Hussein Ridha Sayegh's model, which combines LSTM with SMOTE and Recursive Feature Elimination (RFE), achieved a respectable 99.34% accuracy on both training and test sets using the CICIDS2017 dataset. Similarly, Mahdi Soltan's approach, utilizing an LSTM-based multi-agent system on a custom real-time dataset, resulted in a relatively lower accuracy of 95.00% for training and 96.20% for testing, indicating room for improvement in real-time adaptability. Fatimah Alhayan's LSTM–Autoencoder model with feature reduction showed moderate performance on the UNSW-NB15 dataset, with 97.70% training and 98.10% test accuracy.

Among all models, the proposed LSTM deep learning model stands out as the best-performing technique, achieving 99.84% training accuracy and an impressive 99.91% testing accuracy using the CICIDS2017 dataset. This superior performance can be attributed to the model's ability to effectively

learn temporal dependencies in network traffic using a two-layer LSTM architecture, enhanced by techniques like batch normalization and dropout regularization. Furthermore, the preprocessing steps, feature selection using mutual information, and covariance matrix analysis contributed to reducing noise and improving learning efficiency, allowing the model to generalize well to unseen attack patterns while avoiding overfitting.

V. CONCLUSION

This research successfully developed a robust DDoS attack detection model by combining Covariance Matrix Analysis (CMA) with Long Short-Term Memory (LSTM) deep learning techniques. The proposed model demonstrated superior performance, achieving a test accuracy of 99.91%, highlighting the effectiveness of LSTM in capturing temporal dependencies within network traffic data. The model excels in identifying complex, low-rate, high-volume DDoS attacks that are challenging for traditional detection methods, especially in real-time scenarios. The minimal training loss of 0.0064 further illustrates the LSTM model's ability to efficiently learn the patterns in the data without overfitting, while its confusion matrix analysis revealed a high level of precision, with only 53 false negatives and 4 false positives. This indicates that the model accurately distinguishes between legitimate and malicious traffic, ensuring reliable detection in dynamic cloud environments.

In comparison to traditional machine learning models, the LSTM deep learning model outperformed others in terms of both accuracy and generalization, making it more suitable for handling the evolving nature of DDoS attacks. This hybrid approach, integrating covariance matrix analysis with deep learning, provides a scalable solution for real-time DDoS detection in cloud-based hosting systems, capable of managing large-scale traffic data. In conclusion, the proposed LSTM-based model offers a promising solution for enhancing network security in cloud environments, providing high detection accuracy while maintaining minimal computational overhead. Future research can focus on further optimizing this model for better scalability and adaptability to a wider range of attack types.

REFERENCES

[1] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System," *IEEE Access*, vol. 10, no. September, pp. 99837–99849, 2022, doi: 10.1109/ACCESS.2022.3206425.

[2] S. Wang, W. Xu, and Y. Liu, "Res-TranBiLSTM: An intelligent approach for intrusion detection in the Internet of Things," *Comput. Networks*, vol. 235, no. April, p. 109982, 2023, doi: 10.1016/j.comnet.2023.109982.

[3] V. Hnamte, H. Nhung-Nguyen, J. Hussain, and Y. Hwa-Kim, "A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE," *IEEE Access*, vol. 11, no. April, pp. 37131–37148, 2023, doi: 10.1109/ACCESS.2023.3266979.

[4] D. Kilichev and W. Kim, "Hyperparameter Optimization for 1D-CNN-Based Network Intrusion Detection Using GA and PSO," *Mathematics*, vol. 11, no. 17, pp. 1–31, 2023, doi: 10.3390/math11173724.

[5] G. Shobana and N. R. Sai, "Network intrusion detection using a step-based deep learning approach," *AIP Conf. Proc.*, vol. 2796, no. 1, 2023, doi: 10.1063/5.0149139.

[6] J. Han and W. Pak, "Hierarchical LSTM-Based Network Intrusion Detection System Using Hybrid Classification," *Appl. Sci.*, vol. 13, no. 5, 2023, doi: 10.3390/app13053089.

[7] S. Sengan *et al.*, "Improved LSTM-Based Anomaly Detection Model with Cybertwin Deep Learning to Detect Cutting-Edge Cybersecurity Attacks," *Human-centric Comput. Inf. Sci.*, vol. 13, no. November, 2023, doi: 10.22967/HCIS.2023.13.055.

[8] J. Jose and D. V. Jose, "AS-CL IDS: anomaly and signature-based CNN-LSTM intrusion detection system for Internet of Things," *Int. J. Adv. Technol. Eng. Explor.*, vol. 10, no. 109, pp. 1622–

1639, 2023, doi: 10.19101/IJATEE.2022.10100187.
[9] A. Momand, S. U. Jan, and N. Ramzan, "ABCNN-IDS: Attention-Based Convolutional Neural Network for Intrusion Detection in IoT Networks," *Wirel. Pers. Commun.*, vol. 136, no. 4, pp. 1981–2003, 2024, doi: 10.1007/s11277-024-11260-7.
[10] K. Yang, J. M. Wang, and M. J. Li, "An improved intrusion detection method for IIoT using attention mechanisms, BiGRU, and Inception-CNN," *Sci. Rep.*, vol. 14, no. 1, pp. 1–24, 2024, doi: 10.1038/s41598-024-70094-2.
[11] M. Sajid *et al.*, "Enhancing intrusion detection: a hybrid machine and deep learning approach," *J. Cloud Comput.*, vol. 13, no. 1, 2024, doi: 10.1186/s13677-024-00685-x.
[12] R. W. Anwar, M. Abrar, A. Salam, and F. Ullah, "Federated learning with LSTM for intrusion detection in IoT-based wireless sensor networks: a multi-dataset analysis," *PeerJ Comput. Sci.*, vol. 11, pp. 1–30, 2025, doi: 10.7717/peerj-cs.2751.
[13] F. Alhayan *et al.*, "Enhanced anomaly network intrusion detection using an improved snow ablation optimizer with dimensionality reduction and hybrid deep learning model," *Sci. Rep.*, vol. 15, no. 1, pp. 1–25, 2025, doi: 10.1038/s41598-025-97398-1.
[14] N. Borgioli, F. Aromolo, L. Thi Xuan Phan, and G. Buttazzo, "A convolutional autoencoder architecture for robust network intrusion detection in embedded systems," *J. Syst. Archit.*, vol. 156, no. September, p. 103283, 2024, doi: 10.1016/j.sysarc.2024.103283.
[15] S. M. S. Bukhari *et al.*, "Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability," *Ad Hoc Networks*, vol. 155, no. October 2023, p. 103407, 2024, doi: 10.1016/j.adhoc.2024.103407.
[16] B. I. Farhan and A. D. Jasim, "Improving Detection for Intrusion Using Deep Lstm With Hybrid Feature Selection Method," *Iraqi J. Inf. Commun. Technol.*, vol. 6, no. 1, pp. 40–50, 2024, doi: 10.31987/ijict.6.1.213.
[17] H. R. Sayegh, W. Dong, and A. M. Al-madani, "Enhanced Intrusion Detection with LSTM-Based Model, Feature Selection, and SMOTE for Imbalanced Data," *Appl. Sci.*, vol. 14, no. 2, pp. 1–20, 2024, doi: 10.3390/app14020479.
[18] N. A. Azeez, I. I. Osamagbe, and I. Chioma, "PERFORMANCE EVALUATION OF CONVOLUTIONAL NEURAL NETWORKS (CNNs) AND RECURRENT NEURAL NETWORKS (RNNs) FOR," vol. 12, no. 1, 2024.
[19] M. Soltani, K. Khajavi, M. Jafari Siavoshani, and A. H. Jahangir, "A multi-agent adaptive deep learning framework for online intrusion detection," *Cybersecurity*, vol. 7, no. 1, 2024, doi: 10.1186/s42400-023-00199-0.
[20] J. Ghadermazi, A. Shah, and N. D. Bastian, "Towards Real-time Network Intrusion Detection with Image-based Sequential Packets Representation," *IEEE Trans. Big Data*, vol. 11, no. 1, pp. 157–173, 2024, doi: 10.1109/TBDATA.2024.3403394.
[21] S. Racherla, P. Sripathi, N. Faruqui, M. Alamgir Kabir, M. Whaiduzzaman, and S. Aziz Shah, "Deep-IDS: A Real-Time Intrusion Detector for IoT Nodes Using Deep Learning," *IEEE Access*, vol. 12, no. May, pp. 63584–63597, 2024, doi: 10.1109/ACCESS.2024.3396461.
[22] "IDS 2017 | Datasets | Research | Canadian Institute for Cybersecurity | UNB." Accessed: April 07, 2025. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2017.html?utm_source=chatgpt.com