Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Deep Learning-Based Network Traffic Analysis For Intrusion Detection In Cyber Security Systems

Sasi Kiran Malladi
Independent Researcher
Kakatiya Institute of Technology and Science
skmalladi.tech@gmail.com

ARTICLE INFO

Received: 29 Dec 2024

Revised: 15 Feb 2025

Accepted: 24 Feb 2025

ABSTRACT

The development of internet-based applications has led to a more complex cyberspace, a major challenge to the cybersecurity experts in the development of intelligent real-time cybersecurity tools. In this paper, we propose a very effective intrusion detection model based on a hybrid GRU + BiLSTM on the BoT-IoT dataset. The suggested method combines data preprocessing, feature selection through Chi-square method, normalization, and data balancing through SMOTE to optimize model performance. The combination of GRU and BiLSTM allows for a model that detects malicious actions at extremely high rates by successfully capturing bidirectional and temporal patterns in network data. Experimental findings show high performance, with 99.1% precision, 99.3% F1-score, and 99.7% ROC-AUC, which show the good capability of classification and high robustness. The training and validation trends also indicate that the model has good generalization with little overfitting. The proposed approach is more effective than traditional and deep learning methods compared to the current models. In general, the research establishes that hybrid deep learning models are well fit to detect intrusion in IoT settings, and they offer effective and cost-effective security measures.

Keywords: Cybersecurity, IoT Security, Intrusion Detection System (IDS), Network Traffic Analysis, Deep Learning, BoT-IoT dataset

I. INTRODUCTION

The fast growth of internet-based services in business, government and personal sectors has positioned networks to be an inseparable component of the contemporary world. Nevertheless, this wide usage has also made people more susceptible to cyber threats. The use of network anomaly detection and log analyses has thus become a critical part of cybersecurity because anomalous behaviors may cause serious effects like data breaches, outages, and system failures [1]. The contemporary networks are vulnerable to various risks including DDoS attacks, malware, ransomware, phishing, and data exfiltration [2][3]. IDS plays a vital role in detecting such malevolent activities [4]. Conventional IDS systems, primarily signature and rule-based approaches, are limited in identifying unknown or zero-day threats, frequently experience high FPR, and lack flexibility [5][6].

ML methods have been developed to improve intrusion detection based on data mining and automatic feature extraction to address these challenges [7][8]. MLmodels can detect better than traditional methods but are still heavily dependent on manual feature engineering and unable to handle high-dimensional, non-linear and dynamic network traffic characteristics [9][10]. As a result, they do not perform well in complex and large-scale networks, highlighting the need for more advanced and dynamic intrusion detection schemes. DL, a subfield of ML, has recently emerged as a powerful technique for network intrusion detection. DL models can learn higher-level and hierarchical feature representations from raw network data without human input, while they can also learn more complex and nonlinear relationships [11][12]. Therefore, deep learning has become a leading solution in cybersecurity, including intrusion detection, anomaly detection, adaptive threat mitigation, and has shown to outperform the traditional and conventional methods of ML [13][14].

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A. Motivation and Contribution

The rapid growth and sophistication of cyber-attacks highlight the failure of the traditional intrusion detection frameworks to keep up with the contemporary network environment. This leads to the adoption of more advanced procedures like the DL to learn complex patterns automatically and improve the detection of the performance. In addition, scalable, real-time and adaptive security solutions also require the study of intelligent intrusion detection mechanisms. This study makes a number of important contributions as discussed below:

- Implements comprehensive data preprocessing techniques, including normalization, feature selection, and SMOTE-based data balancing.
- Applies visualization techniques like bar plots and heatmaps to analyze data distribution and feature correlations.
- Proposes a hybrid DL model combining GRU and BiLSTM for improved intrusion detection in network traffic.
- Performed extensive study by evaluating the model's efficacy using several metrics, such as ROC-AUC, F1-score, recall, accuracy, and precision.
- Validates robustness and generalization through comprehensive experimental results on the BoT-IoT dataset

B. Justification and Novelty

The proposed approach is driven by the fact that highly precise and reliable intrusion detection in IoT environments is required, and traditional models are unable to detect complex sequential patterns observed on network data. The research uses the BoT-IoT dataset, which includes a diversity of large-scale information to analyze real-life assault situations. The novelty of the work is that GRU and BiLSTM are integrated into one architecture, and the temporal features with useful learning are combined with the bidirectional context-awareness. Furthermore, Chi-square-based feature selection and SMOTE-based data balancing are introduced to increase the model performance and stability. This combination results in improved detection power, reduced false alarms, and enhanced performance compared to current ML and DL methods.

C. Organization of the Paper

The following is the paper's structure: The literature review is presented in Section II, the methodology is described in Section III, the findings and comparisons are presented in Section IV, and the conclusions and future research are addressed in Section V.

II. LITERATURE REVIEW

The production of this work is made easier by doing a thorough evaluation and analysis of important research works on Network Traffic analysis as a technique for intrusion detection.

M et al. (2026) suggest a hybrid DL-based intrusion detection framework that combines an Autoencoder, Transformer architecture, and Capsule Network (CapsNet) to overcome these drawbacks. Extensive experiments on widely used datasets, such as NSL-KDD, CIC-IDS2017 and UNSW-NB15 demonstrate the proposed model's superior performance against traditional and hybrid baselines, achieving more than 98% accuracy and generalization to new attack types [15].

Gurram (2025) proposes a new artificial intelligence-based IDS with deep-learning based architecture and traffic characterization. Several architectures were implemented and tested to process and evaluate the CICIDS2017 dataset including CNN, RNN, LSTM autoencoder. The experimental results illustrated that the LSTM model had the best overall performance of 97.4 % accuracy and 96.2 % recall and 95.8 and had best performance in terms of capturing the historical traffic temporal element. CNN model was next best with 96.5 % of overall accuracy and 94.9 % recall and is probably the lightest in terms of computational overhead in real-time IDS. Autoencoders were also found to be very useful according to anomaly detection, with an accuracy rate of 94.1 percent, particularly useful when it comes to detecting zero-day attacks [16].

Zhao et al. (2024) present DL-ProS2, a deep learning-based approach for binary protocol reversing, focusing on format segmentation and semantic inference from network traffic. This method harnesses the extract protocol knowledge

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

from publicly available protocol documents, such as RFCs, as the foundational rules for the simulation. Empirical results substantiate the efficacy of approach, demonstrating precision rates exceeding 0.95 and recall rates surpassing 0.97 for partially unknown protocol format segmentation and semantic inference. It also retains effectiveness in the inference of completely unknown protocols, with average prec and rec rates of 0.69 and 0.62 for format segmentation, and 0.43 and 0.47 for semantic inference, respectively [17].

Mebawondu et al. (2024) integrate deep learning techniques to develop an intelligent Intrusion Detection model. The integrated models provide an NIDS that outperforms individual strategies. The findings show that compared to individual DL models, the ensemble model obtains a higher accuracy of 79% [18].

Daher (2023) investigates a healthcare dataset and constructs models that use Q-learning for deep reinforcement learning and conventional ML to form various IDS. They ran large-scale simulations utilizing the built models, comparing the outcomes using several performance measures with an accuracy level higher than 92% [19].

Abdullahi et al. (2022) proposed a DL model for CPS cyber threat detection that is based on LSTM. Additionally, real-world datasets from the gas pipelines, which included 19 characteristics and seven attack types, were used to evaluate the model. The experiment's findings demonstrate that, after validation, the suggested model attained an accuracy of 98.22%. Additionally, the report offers a suggestion for possible further research [20].

Table I provides an overview of recent research on network traffic analysis to detect intrusion, including the proposed models, datasets, major findings, and the problems that are faced.

TABLE I. SUMMARYSUMMARY OF RECENT STUDIES ON NETWORK TRAFFIC ANALYSIS USING MACHINE LEARNING TECHNIQUES

Author	Data	Approaches	Results	Limitations & Future Work
M et al. (2026)	NSL-KDD, CIC-IDS2017, UNSW-NB15	Adaptive attention-based fusion layer for combining feature representations in IDS	Accuracy > 98% on NSL-KDD, CIC-IDS2017, UNSW-NB15	Needs validation in real-time and large-scale network environments
Gurram (2025)	CICIDS2017 dataset	LSTM, CNN, and Autoencoders for IDS	LSTM: 97.4% accuracy, CNN: 96.5%, Autoencoder: 94.1%	Trade-off between computational cost and performance; real-time deployment challenges
Zhao et al. (2024)	Network protocol data (RFC-based)	Protocol format segmentation and semantic inference using deep learning	Precision > 0.95, Recall > 0.97 (known); lower for unknown protocols	Needs improvement for completely unknown protocol inference
Mebawondu et al. (2024)	Network intrusion data	Ensemble-based Network Intrusion Detection System	Accuracy: 79%	Lower accuracy compared to advanced deep learning; needs optimization
Daher (2023)	Healthcare cybersecurity dataset	Hybrid IDS using ML and Q-learning (reinforcement learning)	Accuracy > 92%	Requires further testing on diverse datasets and real-time systems

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Abdullahi et al. (2022)	ICS gas pipeline dataset	IDS using ICS gas pipeline dataset with 7 attack types	Accuracy: 98.22%	Future work suggested for broader datasets and attack scenarios

Research Gap: Although intrusion detection with machine learning and DL models has made substantial progress, there are still gaps in research. Most of the available research has high accuracy and is not validated in real-time and large-scale network settings which restricts their applicability. Also, high computational complexity, poor performance on totally unseen attacks, or zero-day attacks, and dependence on particular datasets are also problematic, leading to the need to create more generalized, efficient, and adaptive models. Thus, it is evident that there is a necessity for strong hybrid solutions that can strike the right balance between accuracy, scalability and real-time deployment

III. METHODOLOGY

The proposed methodology utilizes the BoT-IoT dataset to classify network intrusions through a structured pipeline. Initially, the data is cleaned, normalized using Min–Max scaling, and balanced using SMOTE to handle class imbalance, followed by feature selection using the Chi-square method. The processed data is then split into training, validation, and testing sets and fed into a hybrid GRU + BiLSTM model to capture both temporal dependencies and bidirectional patterns in network traffic. The last step in making sure the model is successful in intrusion detection is to analyze its performance using measures like recall, accuracy, precision, F1score, and AUC-ROC. Figure. 1 illustrates the proposed flowchart for network traffic analysis for intrusion detection using ML.

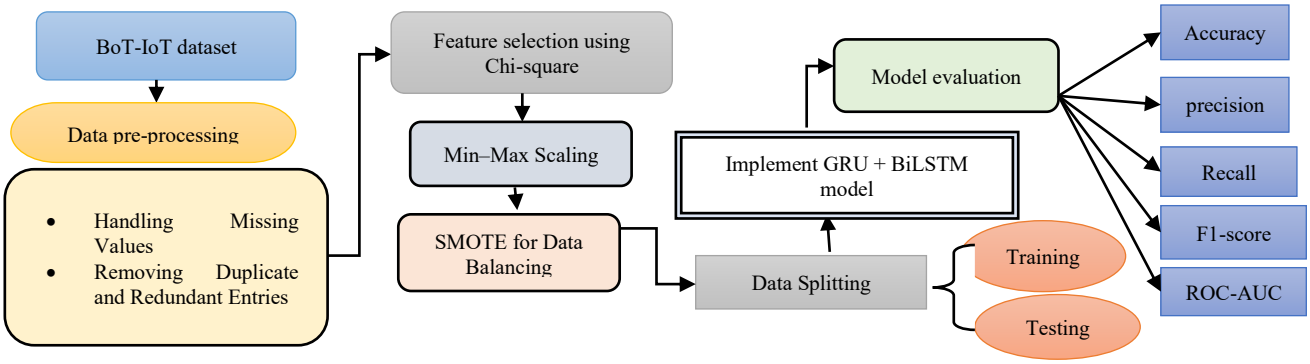

Fig. 1. Proposed flowchart for network traffic analysis for intrusion detection

The following section gives a detailed overview of each aspect of the proposed methodology:

A. Data Gathering and Analysis

The objective of this work is to classify network intrusions using the BoT-IoT dataset, which contains over 73 million records with 46 features and multiple attack types such as DDoS, DoS, reconnaissance, and theft. Data visualization techniques, including bar plots and heatmaps, are employed to analyze attack distribution and feature correlations:

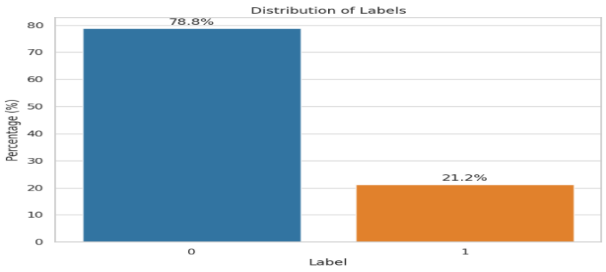

Fig. 2. Distribution of Labels on BoT-IoT Dataset

A distribution of labels in the BoT-IoT dataset is shown in Figure 2. A clear imbalance between classes is observed. Label 0 is about 78.8% of the samples and Label 1 is only 21.2%. This skewed distribution illustrates the dominance of

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

benign traffic over malicious traffic, and underscores the importance of data balancing techniques to encourage fair and effective training and evaluation of models.

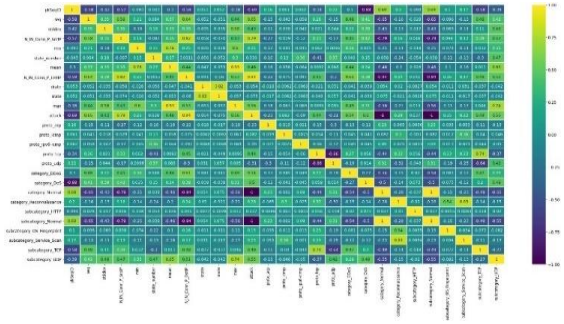

Fig. 3. Correlation Heatmap of Features

Figure 3 shows the Correlation seat map, reflecting the trends of strong positive and negative relationships between features of N-network traffic. It assists in determining feature dependencies and redundancy, and can therefore be used in choosing the most pertinent variables to be used in intrusion detection models.

B. Data Pre-processing

The data preparation phase for the BoT-IoT dataset included data integration, cleaning, and feature engineering, such as concatenation and cleansing. Preprocessing involved the treatment of missing values, removal of duplicate and redundant data to maintain data quality. Lastly, normalization was used to promote consistency and better model performance.

C. Feature selection using Chi-square

The feature selection procedure defines the most useful characteristics in order to improve model performance and simplify it by removing unnecessary features. The significance of each characteristic may be determined by testing its connection with the target variable using a chi-square test. Attributes having the higher Chi-square scores are chosen which results in better accuracy and effective calculation.

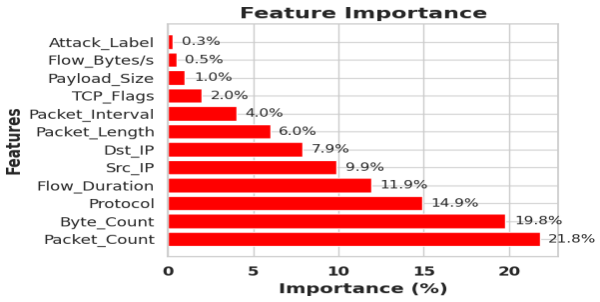

Fig. 4. Plot Feature importance Score

Figure 4 indicates that the high-level traffic characteristics are the ones that have the most significant role in identifying botnet activity, with data volume and the frequency of transmissions being the most powerful factors. More detailed features, on the contrary, have the least contribution, demonstrating that global traffic patterns have a greater impact on efficient intrusion detection.

D. Min–Max Scaling

The min-max scaling approach is used to normalize FeatureValues to a range of 0 to 1. This approach helps improve classifier performance while reducing the influence of outliers. The normalization process is defined by the following mathematical Equation (1):

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

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

where X indicates the feature's initial value, X' is the normalized value, X_{min} is the feature's lowest value, and X_{max} is the highest value of the same.

E. Data balancing using SMOTE

Class Imbalance is solved by using data balancing to redistribute samples in order to better the model performance. The SMOTE algorithm generates artificial samples of the minority group by determining the nearest neighbors depending on the Euclidean distance. They are constructed through interpolation and placed into the data set to have a more equal distribution of classes. Label 0 and Label 1 are equally represented at 50% in the distribution of labels following SMOTE balancing (Figure. 5). This balanced allocation gets rid of the skew in the original data, making the training fairer as well as enhancing the performance of the detection across classes.

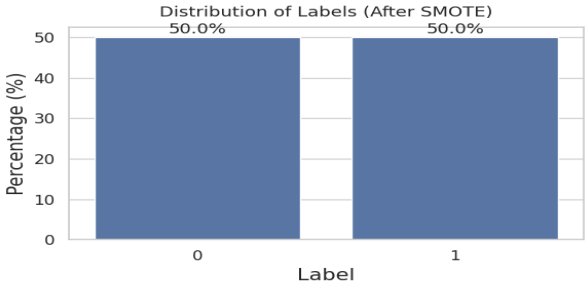

Fig. 5. Bar Graph for Data Distribution After Balancing

F. Data Splitting

To achieve accurate model generalization, the dataset is separated into 70% training and 30% testing sets.

G. Proposed GRU + BiLSTM Model

GRU + BiLSTM model is a hybrid DLmodel that incorporates the efficiency of GRU and contextual learning capability of BiLSTM. BiLSTM enhances the ability of the model to understand complex patterns of network traffic by operating in both directions, and GRU requires fewer parameters to model temporal relationships. The hidden state update in the GRU unit is given by Equation.(2)

$$h_t = (1 - Z_t) \odot h_{t-1} + z_t \odot \bar{h}_t \qquad (2)$$

GRU unit employs update and reset gates to regulate the information flow and keep significant characteristics over time. This assists in mitigating the problem of vanishing gradient and improves sequence intrusion data learning. The BiLSTM hidden state is computed as Equation.(3

$$h_t = \overrightarrow{h_t} \oplus \overleftarrow{h_t} \qquad (3)$$

The model can understand the past and the future since the BiLSTM layer examines the sequence both forward and backward and integrates forward and backward hidden states. This GRU + BiLSTM architecture enhances accuracy and robustness in intrusion detection tasks by effectively modeling more complex temporal relationships. The model is composed of GRU and BiLSTM layers each having 128 units to learn the temporal dependencies. The model was trained using Adam optimizer and Learning Rate 0.001 and Binary Cross-entropy loss function. There was a pruning done in the form of dropout with a ratio of 0.2. It used an optimal learning approach that is called mini-batch gradient descent to train the model in the 30 epochs; the batch size being 32. The training process has validation to check the performance and to ensure that the training gets the right convergence, thus high accuracy and high generalization.

H. Evaluation Metrics

The model's performance is evaluated using a variety of measures, including F1score, accuracy, precision, recall, and the area under the ROCcurve. The confusion matrices produced by each of the classifiers offer a detailed analysis of the prediction results. These matrices show the TP, TN, FP and FN distribution which can help to provide a better understanding of the true and false positives and negatives. In sum, this assessment approach may be used to gauge

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

the model's efficacy in distinguishing between malicious and benign traffic. The following matrix are Equation (4 to 7) in below:

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

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

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

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

Accuracy is a measure of overall performance; it reflects the model's ability to classify correctly. Precision assesses the dependability of a good forecast and is used to reduce FP, which is critical in intrusion detection to prevent needless false alarms that might interrupt system operations. Recall or TPR is an indicator of the model's ability to detect intrusion; a strong recall value is required to avoid missed detection and ensure a reliable system with complete detection capability. The harmonic mean of recall and precision is known as the F1-score; it is used to measure the model's overall performance, while showing its accuracy and comprehensiveness. ROCcurves are a representation of the TPR and FPR of a classifier for different levels, and the AUC-ROC is the discrimination power of the model.

IV. RESULTS AND DISCUSSION

The experimental setup and performance of the suggested model are covered in this section, with special attention to its assessment and computational effectiveness.

A. Experimental Setup

The experimental setup consists of an Intel Core i7 3.5 GHz, 16 GB of RAM, and an NVIDIA RTX 3060 12 GB VRAM for the model training, and Python 3.10, TensorFlow 2.15 and Scikit-learn for its implementation and evaluation, is set up on an Ubuntu 22.04 LTS system.

B. Result Demonstrations

The experimental results on the BoT-IoT dataset demonstrate that the proposed GRU+BiLSTM model achieved good performance in intrusion detection via network traffic analysis (Table II). The model had an acc of 99.4% and an F1score of 99.3, which demonstrated its capacity to both detect and control false alarms. Additionally, the model had a high ROC-AUC of 99.7%, demonstrating its ability to distinguish between benign and harmful network activity.

TABLE II. RESULTS OF PROPOSED MODEL FOR INTRUSION DETECTION USING BOT-IOT DATASET

Matrix	GRU+BiLSTM Model
Accuracy	99.4
Precision	99.1
Recall	99.5
F1-score	99.3
ROC-AUC	99.7

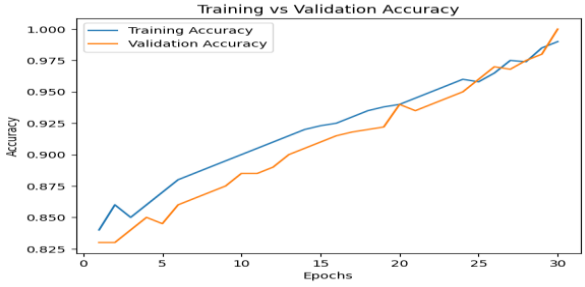

Fig. 6. Training and Validation Accuracy for the GRU+BiLSTM Model

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Figure. 6 demonstrates the training and validation accuracy over 30 epochs of training, where the two curves rise steadily, indicating successful learning by the model. The Validation Accuracy is almost similar to the Training Accuracy with a minor difference indicating that there is good generalization and low overfitting.

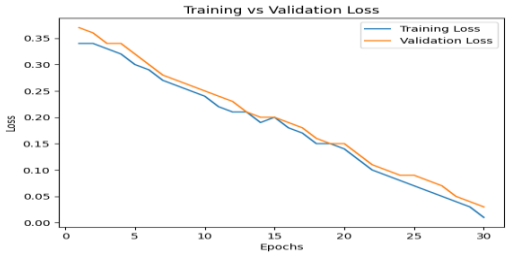

Fig. 7. Training vs Validation loss for the GRU+BiLSTM Model

Figure 7 depicts the training and validation loss after 30 epochs, with both curves performing downwards, indicating that the model is learning and being improved effectively. There is a close relationship between the validation and training losses with a slight variation indicating high generalization performance and low overfitting during the training process.

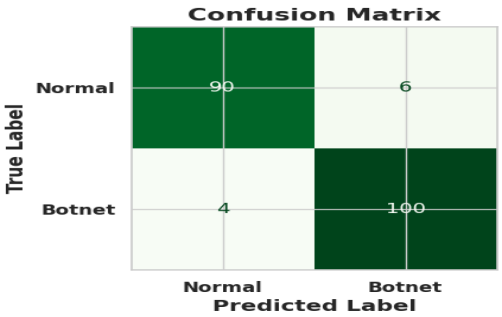

Fig. 8. Confusion Matrix of Proposed the proposed Model

Figure. 8 shows the proposed model classification performance in distinguishing between Normal and Botnet traffic. The matrix highlights that 90 Normal instances were correctly identified, while 6 were misclassified as Botnet. In the same way, 100 Botnet cases were correctly identified with only 4 being falsely identified as Normal. The model's strength and excellent balance are shown by the few misclassifications and the deeper shade, which indicates strong detection capabilities.

Figure 9 displays the Recurve of the proposed model, which proves its high accuracy in the class differentiation. Curve is classifying excellently, as it is closely following the top-left border; random guessing is seen in the diagonal line. The model has an AUC of 0.997, which indicates close to perfect discrimination and the fact that the model is robust in identifying cybersecurity threats with minimal false positives.

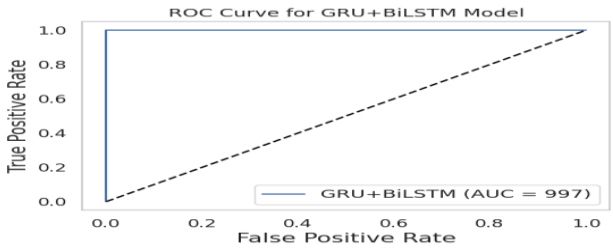

Fig. 9. Plot ROC Curve for Propose Model

C. Comparative Analysis

Table III and BoT-IoTdataset include a comparative analysis of performance with existing models. The outcomes show that SVM has an acc of 88.3% with high prec but less rec compared to BPNN which has an accuracy of 95.3% with

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

more balanced measures. CNN model also increases classification to 96 and high F1-score of 94. FFNN and ANN have moderate performance, whereas ViT and KNN models have superior results on the datasets. In comparison, the proposed GRU + BiLSTM model on the BoT-IoTdataset works best because it is the most accurate and has superior overall performance metrics.

TABLE III. COMPARITIVE ANALYSIS FOR INTRUSION DETECTION ON MULTIPLE DATASETS

Model	Dataset	Acc.	Pre.	Rec.	F1.
FFNN[21]	UNSW-NB15	77.7	61.7	78.9	69.2
ANN[22]		79.9	89	65	76
ViT[23]	ToN-IoT	88.3	86	75.7	75.7
KNN[24]		95.1	93.5	96.9	95.2
BPNN[25]	BoTNet-IoT-L01	95.3	93.6	94.2	-
CNN[26]	BoT-IoT	96	94	93	94
SVM[27]		88.3	99.9	88.3	-
GRU+BiLSTM		99.4	99.1	99.5	99.3

The key advantages of the proposed GRU + BiLSTM model include high detection accuracy, good generalization, and ability to detect complex temporal variations in IoT network traffic, which makes it applicable in real-time intrusion detection. Ethical aspects however, need to be considered including data privacy, ensuring that the sensitive network data is not abused and transparency of model decisions are maintained. Also, the reduction of bias during pre-processing (e.g., SMOTE) and responsible and equitable implementation in different network environments should be considered.

V. CONCLUSION AND FUTURE STUDY

ML-based IDS has become the focus of enhanced cybersecurity because they are able to detect and react to possible threats in real time. This paper hypothesizes that hybrid GRU + BiLSTM model will be able to attain high accuracy and reliability in detecting intrusions on the BoT-IoT dataset. The model effectively represents complex time- and context-dependent trends to network data, leading to high scores on all evaluation measures, such as 99.4% accuracy and 99.7% ROC-AUC. These results reveal its ability to differentiate between normal and malicious activity and have a reasonable detection and false alarm balance. Moreover, the proposed model outperforms the current methods at all times, which indicates the superiority of hybrid DL methods in cybersecurity tasks. In general, the results validate the hypothesis that such architectures provide a powerful and effective IoT intrusion detection solution with high real-life applicability.

The suggested GRU + BiLSTM model is quite accurate but has certain limitations. It is primarily evaluated at the BoT-IoTdataset that might not be generalizable to other datasets such as UNSW-NB15. The hybrid model also has high computational cost, making real-time deployment difficult. Additionally, SMOTE-based balancing may introduce bias. Future research need to concentrate on real-time implementation, lightweight model design, and cross-dataset validation.

REFERENCES

[1] B. Madupati, M. M. Mohammed, L. Upadhyay, D. P. Guda, K. Kaushik, and M. Soni, “Integrating Artificial Intelligence with Cybersecurity for Resilient Wireless Communication Against Advanced Threats,” in *2025 International Conference on Artificial Intelligence and Machine Vision (AIMV)*, IEEE, Aug. 2025, pp. 1–5. doi: 10.1109/AIMV66517.2025.11203666.

[2] I. Hamid and M. M. H. Rahman, "AI, machine learning and deep learning in cyber risk management," *Discov. Sustain.*, vol. 6, no. 1, 2025, doi: 10.1007/s43621-025-01012-3.
[3] M. Kumar and M. K. Shah, "AI-Driven DDoS Detection for Network Security: A Performance Analysis of Machine-Deep Learning Methods on Network Traffic Data," in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, IEEE, Feb. 2026, pp. 1–6. doi: 10.1109/ICAIC67076.2026.11395710.
[4] S. Singh, "Advancing Network Security in 5G: Leveraging the 5G-NIDD Dataset for Intrusion Detection and Mitigation," in *2025 IEEE 12th International Conference on Cyber Security and Cloud Computing (CSCloud)*, IEEE, Nov. 2025, pp. 1–6. doi: 10.1109/CSCloud66326.2025.00055.
[5] P. Nutalapati, J. R. Vummadi, S. Dodda, and N. Kamuni, "Advancing Network Intrusion Detection: A Comparative Study of Clustering and Classification on NSL-KDD Data," in *2025 International Conference on Data Science and Its Applications (ICoDSA)*, IEEE, Jul. 2025, pp. 880–885. doi: 10.1109/ICoDSA67155.2025.11157595.
[6] D. Bhattacharjee, "Design and Evaluation of Deep Generative AI Model for Intrusion Detection in Cyber Threat Monitoring," in *2025 7th International Symposium on Advanced Electrical and Communication Technologies (ISAECT)*, 2025, pp. 1–6. doi: 10.1109/ISAECT68904.2025.11318752.
[7] I. Ullah and Q. H. Mahmoud, "Design and Development of RNN Anomaly Detection Model for IoT Networks," *IEEE Access*, vol. 10, pp. 62722–62750, 2022, doi: 10.1109/ACCESS.2022.3176317.
[8] M. K. Shah, "Artificial Intelligence (AI)- Based Threat Detection Models for Privileged App Abuse in Modern Systems," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 6, no. 4, p. 11, 2026.
[9] M. Ahsan, R. Gomes, M. M. Chowdhury, and K. E. Nygard, "Enhancing Machine Learning Prediction in Cybersecurity Using Dynamic Feature Selector," *J. Cybersecurity Priv.*, vol. 1, no. 1, pp. 199–218, Mar. 2021, doi: 10.3390/jcp1010011.
[10] S. Gupta, C. Maple, and R. Passerone, "An Investigation of Cyber-Attacks and Security Mechanisms for Connected and Autonomous Vehicles," *IEEE Access*, vol. 11, pp. 90641–90669, 2023, doi: 10.1109/ACCESS.2023.3307473.
[11] Y. Feng, J. Zhong, C. Ye, and Z. Wu, "Clustering based on Self-Organizing Ant Colony Networks with Application to Intrusion Detection," in *Sixth International Conference on Intelligent Systems Design and Applications*, IEEE, Oct. 2006, pp. 1077–1080. doi: 10.1109/ISDA.2006.253761.
[12] D. Jain and S. Jain, "Artificial Intelligence (AI)-Driven Network Traffic Anomaly Detection for IT Infrastructure Security," IEEE, 2026, pp. 1–6. doi: https://doi.org/10.1109/ICAIC67076.2026.11395685.
[13] M. Alazab, R. A. Khurma, M. García-Arenas, V. Jatana, A. Baydoun, and R. Damaševičius, "Enhanced threat intelligence framework for advanced cybersecurity resilience," *Egypt. Informatics J.*, vol. 27, no. September, p. 100521, 2024, doi: 10.1016/j.eij.2024.100521.
[14] A. Behera, K. S. Sahoo, T. K. Mishra, and M. Bhuyan, "A combination learning framework to uncover cyber attacks in IoT networks," *Internet Things (The Netherlands)*, vol. 28, no. December 2023, p. 101395, 2024, doi: 10.1016/j.iot.2024.101395.
[15] A. M, K. K. R, S. S, M. Boomika, B. S. J, and S. D. K, "A Multi-Model Deep Learning Approach for Advanced Cybersecurity Threat Detection," in *2026 Second International Conference on Multi-Agent Systems for Collaborative Intelligence (ICMSCI)*, IEEE, Mar. 2026, pp. 386–391. doi: 10.1109/ICMSCI67830.2026.11469498.
[16] N. T. Gurram, "AI-Based Intrusion Detection Systems Using Deep Learning and Network Traffic Analysis," in *2025 OITS International Conference on Information Technology (OCIT)*, IEEE, Dec. 2025, pp. 492–497. doi: 10.1109/OCIT66168.2025.11400454.
[17] S. Zhao, S. Yang, Z. Wang, Y. Liu, H. Zhu, and L. Sun, "Crafting Binary Protocol Reversing via Deep Learning With Knowledge-Driven Augmentation," *IEEE/ACM Trans. Netw.*, vol. 32, no. 6, pp. 5399–5414, Dec. 2024, doi: 10.1109/TNET.2024.3468350.
[18] O. J. Mebawondu, T. A. Badmos, O. D. Alowolodu, and J. Olorunshogo Mebawondu, "Development of an Intelligent Intrusion Detection Model using an Ensemble of Deep Learning Paradigm," in *2024 IEEE 5th International Conference on Electro-Computing Technologies for Humanity (NIGERCON)*, 2024, pp. 1–5. doi: 10.1109/NIGERCON62786.2024.10927302.
[19] L. A. Daher, "Towards Secure IoMT: Attack Detection Using Deep Q-Learning in Healthcare Networks," in *2023*

Research Article

16th International Conference on Developments in eSystems Engineering (DeSE), IEEE, Dec. 2023, pp. 407–412. doi: 10.1109/DeSE60595.2023.10468942.

[20] M. Abdullahi, H. Alhussian, N. Aziz, S. J. Abdulkadir, and Y. Baashar, "Deep Learning Model for Cybersecurity Attack Detection in Cyber-Physical Systems," in *2022 6th International Conference On Computing, Communication, Control And Automation (ICCUBEA*, 2022, pp. 1–5. doi: 10.1109/ICCUBEA54992.2022.10010717.

[21] B. Das and G. Kakarla, "Deep Learning-Based Network Traffic Signal Analysis for Intelligent Cyber Threat Detection," vol. 12, no. 2, pp. 2305–2314, 2026.

[22] M. Farhan *et al.*, "Network-based intrusion detection using deep learning technique," *Sci. Rep.*, vol. 15, no. 1, p. 25550, Jul. 2025, doi: 10.1038/s41598-025-08770-0.

[23] C. Du, Y. Guo, and Y. Zhang, "A Deep Learning-Based Intrusion Detection Model Integrating Convolutional Neural Network and Vision Transformer for Network Traffic Attack in the Internet of Things," *Electron.*, vol. 13, no. 14, 2024, doi: 10.3390/electronics13142685.

[24] A. M. Almasabi, M. Khemakhem, F. E. Eassa, A. Ahmed Abi Sen, A. B. Alkhodre, and A. Harbaoui, "A Smart Framework to Detect Threats and Protect Data of IoT Based on Machine Learning," *IEEE Access*, vol. 12, no. November, pp. 176833–176844, 2024, doi: 10.1109/ACCESS.2024.3498603.

[25] H. El-Sofany, S. A. El-Seoud, O. H. Karam, and B. Bouallegue, "Using machine learning algorithms to enhance IoT system security," *Sci. Rep.*, vol. 14, no. 1, pp. 1–19, 2024, doi: 10.1038/s41598-024-62861-y.

[26] A. A. Jain, B. Srinivasa Rao, S. Chattopadhyay, A. Kumar, M. S. Muthuraman, and A. Manjula, "An Artificial Intelligence Network based-Host Intrusion Detection System for Internet of Things Devices," *2023 4th Int. Conf. Electron. Sustain. Commun. Syst. ICESC 2023 - Proc.*, pp. 656–661, 2023, doi: 10.1109/ICESC57686.2023.10193232.

[27] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," *Futur. Gener. Comput. Syst.*, vol. 100, no. May 2019, pp. 779–796, 2019, doi: 10.1016/j.future.2019.05.041..