A Real-Time Deep Neural Network–Based Architecture for Active Network Attack Identification and Classification Models

Karthikeyan Kaliyaperumal[1], Raja Sarath Kumar Boddu[2], Sai Kiran Oruganti [3], Gudisa Tesema Kebesa[4],

[1]Post Doctoral Fellow Researcher, Lincoln University College, KL-Malaysia
[2]Professor and Head of Computer Science & Engineering, Raghu Engineering College, Visakhapatnam, India.
[3]Professor in Faculty of Engineering & Built Science, Lincoln University College, KL- Malaysia.
[4]Dean, School of Informatics & Electrical Engineering, IoT-HH Campus, Ambo University, Ethiopia

Corresponding author Email id: pdf. kirithicraj@lincoln.edu.my

Abstract: In the context of computer science and technology, a group of linked devices, or nodes, that exchange data, resources, or services with one another is referred to as a network. An active network attack refers to a malicious activity in which an attacker deliberately attempts to disrupt, manipulate, or gain unauthorized access to a computer network or its resources. In today's digital context, network security is of vital importance as cyber threats continue to evolve in terms of sophistication and frequency. Active network attacks pose significant challenges to traditional detection methods, necessitating the exploration of advanced techniques such as deep learning. The proposed methodology involves the development of a model based on deep learning that was learned using a dataset comprising diverse network traffic data which is Network Security Laboratory-Knowledge Discovery in Databases (NSL-KDD). This study utilizes a comprehensive preprocessing pipeline, including data cleaning, feature selection for categorical variables and standardization of numerical features to prepare the dataset for modeling. To extract the pertinent information, preprocessing approaches are used. Metrics like as accuracy, precision, recall, F1-Score, and confusion matrix are used to evaluate performance as a result from deep learning models Deep Neural Network (DNN), Convolution Neural Networks (CNN), Long Short Term Memory(LSTM), Bi-Long Short Term Memory (Bi-LSTM) and Gated Recurrent Units (GRU) experiments done, Bi-LSTM model scored the best result of 99.15% and 99.12% accuracy for binary and multi classification, respectively.

Keywords: Active network, Cyber-attacks, Deep neural network, CNN, Deep learning, Detection

Introduction

Active network attack detection and classification using deep neural network learning model involve using deep learning techniques to identify and classify various types of network attacks in real time or near real time. Deep learning has shown promise in many fields, including cyber security. Building and training deep learning model using huge network dataset, researchers and practitioners can potentially create more effective and robust intrusion detection systems [1]. The term "active network attacks" typically refers to malicious activities aimed at disrupting or gaining unauthorized access to computer networks. Detecting and classifying these attacks is crucial for maintaining the security and integrity of networked systems [2]. Using deep learning for this purpose offers several advantages. Deep learning models can automatically extract relevant features from raw network data, eliminating the need for feature engineering. They can also adapt and learn from new attack patterns, making them potentially more proficient at detecting previously unseen threats. Additionally, deep learning models can handle with large-scale datasets efficiently, enabling the detection of attacks in real time or near real time [3].

In the context of computer science, a network refers to a collection of two or more computers linked or connected together to share the resources, exchange files, or enable electronic via communications [4]. It is

networked nodes and entities that share information with one another. it plays a fundamental role in modern computing, enabling communication between devices, sharing resources, and facilitating various services and applications[5].

Literature Review

A. Overview of Network

There are several types of networks, including Local Area Networks (LANs), which cover a specific area, such as a building, and Wide Area Networks (WANs), which connect several LANs across larger territories. Wireless networks, such as Wi-Fi and cellular networks, transmit data via radio or infrared signals. Peer-to-Peer (P2P) networks enable direct device communication without the need for a central server, which is often used for file sharing. Client-server networks, on the other hand, allow clients to access services from centralized servers, which is common in online applications and cloud computing. Network components include nodes (devices), connections (communication channels), protocols (data transmission regulations), and infrastructure (hardware and software support) [5].

B. Network Security and Attack Detection

The Internet's widespread use and continuous expansion are beneficial to many network users in many ways and preventing unwanted access and alteration is the goal of defense when it comes to computers, networks, programs, different types of data. This is where network security comes in [12]. However, as more and more systems in the financial, e-commerce, and military become internet-connected, they become targets for network attacks, which increases risk and causes significant harm. In essence, effective tactics for attack detection, defense, and network security maintenance are required. Thus, the primary problem in the field of network security to be solved and how to recognize various types of network attacks [13].

C. Machine Learning in Network Security

Traditional models have been widely employed in attack detection and classification in network security. However, Traditional machine learning approaches rely heavily on handcrafted feature engineering, where domain experts manually design and select relevant features from raw network traffic data. These features may include packet headers, flow statistics, payload content, or behavior-based features extracted from network logs. Feature engineering aims to capture discriminative information that distinguishes between normal network behavior and malicious activities [14].

Relevance of Works

Active network attacks involve attackers actively launching attacks against target servers, where the attacker attempts to change the data on the target. These attacks can include unauthorized changes to the system, such as the alteration of transmitting data and stored as well, the fabrication of data, masquerade attacks, messages replays, messages modifications, including service denial attacks [25]. These network components need to be reliable and secured through advanced deep learning technologies to detect and mitigate anomalies provided a comprehensive survey of Intrusion Detection Systems (IDSs) tailored for Wireless Sensor Networks (WSNs) [26]. Their work classified IDS based on detection approaches and deployment strategies and laid a foundational framework for understanding the landscape of intrusion. Building upon this taxonomy, presented a review focused on machine learning techniques for network intrusion detection. By synthesizing advancements in machine learning algorithms and their application to intrusion detection, the authors highlight the potential of these techniques in enhancing the accuracy and efficiency of network defense mechanisms.

A comprehensive study of deep learning techniques for anomaly detection was carried out. Deep learning techniques have emerged as potential approaches for anomaly detection in network traffic [27]. Demonstrating the effectiveness of neural network architectures in capturing complicated patterns

indicative of malicious activities. In a similar investigated the application of deep learning approaches specifically for network intrusion detection [28]. Their review offers insights into the design and evaluation of deep learning models, emphasizing their scalability and adaptability to evolving threat landscapes.
Furthermore, Tun *et al.* [29] offer an overview of network anomaly detection techniques, emphasizing the importance of a comprehensive classification to categorize detection methods based on their objectives and methodologies. Their work provides a holistic perspective on the diverse range of approaches employed in the detection and classification of network attacks.
Several studies [30−32] have highlighted the limitations of traditional misuse detection methods, such as signature-based Intrusion Detection Systems (IDSs). These methods rely on known attack signatures and struggle to detect novel or zero-day attacks, leading to increased vulnerability to emerging threats [33]. Hsu *et al.* [34] have emphasized the potential benefits of hybrid approaches that combine multiple detection methods to improve detection accuracy and resilience against evolving threats. By integrating misuse and anomaly detection methods using deep learning, it is possible to leverage the complementary strengths of both approaches and achieve more robust and accurate detection outcomes. Collectively, these studies contribute to advancing the state of the art in active network attack detection and classification. By synthesizing insights from various domains, including wireless sensor networks, machine learning, deep learning, security, researchers and practitioners are empowered to develop more resilient and adaptive intrusion detection systems capable of mitigating emerging threats in dynamic network environments.
This study results indicated that the multilayer perceptron, achieving an accuracy of 96.39% complexity [10]. Even if the accuracy is significant, it is particularly focused on only man-in-the-middle attacks. The summary of related works as shown in the Table I.

Table1. Summary of Related work

S/No	Ref.	Title	Technique	Accuracy	Gaps
1	[19]	(LSTM)-based CNN to detect network intrusions	Deep Learning	94.12% and 88.95% for binary classification and multi-classification, respectively.	- Compares only two models - Accuracy needs to be improved in both case
2	[21]	A Novel Statistical Analysis and Auto encoder Driven Intelligent Intrusion Detection Approach	Deep Learning	84.21% and 87%. For Binary (0's and 1's) classification and Multi-classification, respectively	- Done for both Binary classification and Multi-classification however, - Low Accuracy for both case
3	[25]	Efficient Deep Learning-Based Cyber-Attack Detection for IoMT devices.	Deep Learning	96.39%	- Focused on only man-in-the-middle attack
4	[9]	Attack Detection in IoT using Machine Learning algorithms	Machine Learning	85.34%	- Low accuracy - Used traditional machine learning which cannot detect novel anomalies without manually upgraded

Research Methodology and Design

The methodology is a method for systematically and scientifically solving a research problem. The most popular techniques are experimentation, observation, surveys, interviews, focus groups, and archival research. Data collection and analysis procedures are known as research methods. Surveys, experiments, interviews, and observations are examples of common methodologies [39]. Consequently, to conduct this research, we used an experimental research methodology.

Because, experimental research provides a quantitative basis for evaluating the performance of detection systems in terms of accuracy, detection rate, false positive rate, response time, and other relevant metrics. This allows researchers to compare different approaches and identify the most effective solutions for detecting and justifying specific types of network attacks. This section describes and explains the critical research methods for detecting and classifying active network attacks.

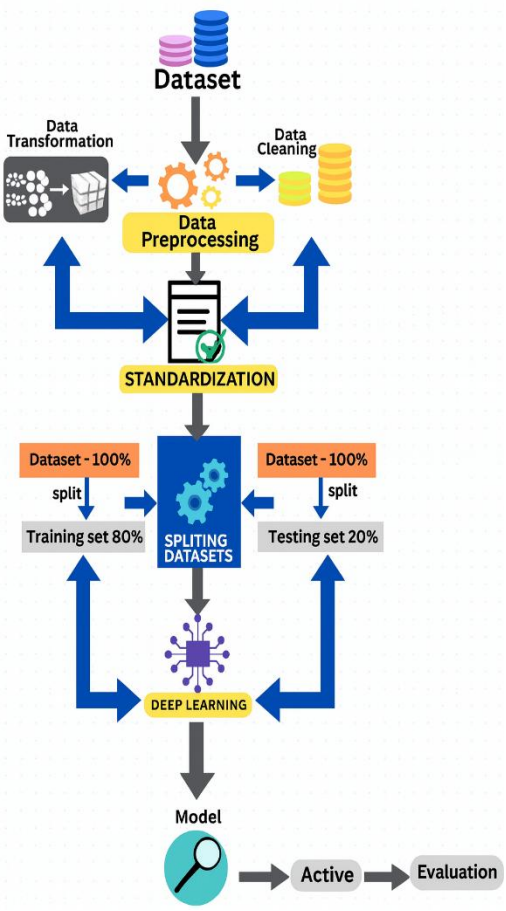

Fig. 1. Architecture evaluation model Model Architectural

Dataset Used

The availability of effective data set is a requirement for an improvement of intelligent attack detection system. An attack detection system can only benefit training and testing with a dataset which contains a lot of high quality data and simulates a crucial time. In the recent field of computer network attack detection, the NSL-KDD dataset is a commonly recognized benchmark dataset. This dataset is a carefully designed addressing the shortcomings of the original NSL-KDD Cup 99 dataset, offering an improved and more accurate version of the latter.

The NSL KDD dataset contains a wide range of network traffic data, including both normal and various types of attack activity. It thus becomes a precious tool for the assessment and development of network attack detection systems. Its capacity to accurately simulate real-world network traffic conditions increases its applicability, making it a top option for practitioners and researchers looking to systematically evaluate and improve their network attack detection algorithms [40].

The proposed deep learning models used for active network attack detection and classification were trained and tested using NSL-KDD dataset for both binary and multi classifications. Because, forty-one characteristics, including connection duration, protocol type, service type, and amount of bytes transferred, are included in the NSL-KDD dataset and describe different aspects of network traffic. By balancing the data, the majority class is less biased and models are trained more successfully. For scientific research, the NSL-KDD dataset is easily accessible. This shows all of the processing steps seen in the figure.

Description of the Model

Five hidden layers make up the Deep Neural Network (DNN), and each layer has 128, 64, 32, 16, and 8 neurons. All hidden layers employ the Rectified Linear Unit (ReLU) activation function. To enhance generalization and reduce overfitting, a dropout layer with a rate of 0.2 follows each hidden layer. The Methods of Regularization: Adam optimizer with a learning rate of 0.001 and L2 regularization with a penalty term of 0.01.

RESULTS AND DISCUSSIONS

A. Overviews

The experiment conducted to assess the effectiveness of the suggested models is covered in this chapter. In this process`s different tools utilized such as libraries, datasets, implementation specifics, and performance evaluation outcomes of models utilizing various evaluation criteria are all addressed.

B. Dataset Used

In this study, we utilized NSL-KDD dataset which is refined version of predecessor KDD99. Because, it addresses issue of redundant record in that found in its predecessor dataset. As stated above in Section III, the original dataset contained many duplicate records, which could lead to biased training results. NSL-KDD eliminates this redundancy.

Table 2. Classification Report for All Models

Models	Classification	Precision	Recall	F1-Score	Support
DNN	DoS	1.00	1.00	1.00	10,677
	Probe	0.99	0.97	0.98	2816
	R2L	0.88	0.93	0.90	750
	U2R	0.90	0.70	0.79	50
	Normal	0.99	0.99	0.99	15,411
	Accuracy	-	-	0.99	29,704
	Macro avg	0.95	0.92	0.93	29,704
	Weighted avg	0.99	0.99	0.99	29,704
CNN	DoS	0.99	1.00	1.00	10,677
	Probe	0.99	0.96	0.97	2816
	R2L	0.90	0.74	0.81	750
	U2R	0.78	0.62	0.69	50
	Normal	0.98	0.99	0.99	15,411
	Accuracy	-	-	0.98	29,704
	Macro avg	0.93	0.86	0.89	29,704
	Weighted avg	0.98	0.98	0.98	29,704
LSTM	DoS	1.00	1.00	1.00	10,677
	Probe	0.98	0.98	0.98	2816
	R2L	0.87	0.89	0.88	750
	U2R	0.88	0.74	0.80	50
	Normal	0.99	0.99	0.99	15,411
	Accuracy	-	-	0.99	29,704
	Macro avg	0.95	0.92	0.93	29,704
	Weighted avg	0.99	0.99	0.99	29,704
BI-LSTM	DoS	1.00	1.00	1.00	10,677
	Probe	0.98	0.99	0.99	2816
	R2L	0.90	0.91	0.91	750
	U2R	0.78	0.72	0.75	50
	Normal	0.99	0.99	0.99	15,411
	Accuracy	-	-	0.99	29,704
	Macro avg	0.93	0.92	0.93	29,704
	Weighted avg	0.99	0.99	0.99	29,704
GRU	DoS	1.00	1.00	1.00	10,677
	Probe	0.99	0.98	0.99	2816
	R2L	0.90	0.92	0.91	750
	U2R	0.84	0.74	0.79	50
	Normal	0.99	0.99	0.99	15,411
	Accuracy	-	-	0.99	29,704
	Macro avg	0.94	0.93	0.93	29,704
	Weighted avg	0.99	0.99	0.99	29,704

Table 2. shows the performance classification outcome for DNN utilizing the five classes' confusion matrices the TP, TN, FP, and TN counts for each class (Dos, probe, R2L, U2R, and normal). For each class the model produced results which are true positive and true negative. Out of the DoS test samples (10,677), 10,651 are correctly classified as DoS whereas none (0), 5, 0, 21 of DoS samples are incorrectly classified as probe, R2L, U2R, and normal, respectively.

Among the total 2,816 Probe samples, 2,744 were correctly classified as Probe, while 4, 1, 1, and 66 Probe samples were incorrectly classified as DoS, R2L, U2R, and Normal, respectively. For the R2L class, out of 750 test samples, 697 were correctly identified as R2L, whereas 1, 0, 2, and 50 samples were misclassified as DoS, Probe, U2R, and Normal, respectively.

Among the total U2R (50) sample, 35 samples are correctly classified as U2R whereas 0, 0, 3, 12 U2R sample are incorrectly classified as Dos, Probe, R2L, and normal, respectively. In the normal class from test sample (15,411), 15,291 sample are correctly classified as normal whereas 6, 27, 86, 1 of normal sample are incorrectly classified as Dos, Probe, R2L, and U2R, respectively.

Among the total 50 U2R samples, 31 were correctly classified as U2R. whereas 2, 0, 3, 14 U2R sample are incorrectly classified as Dos, Probe, R2L, and normal, respectively. In the normal class from test sample (15,411), 15,275 sample are correctly classified as normal whereas 38, 37, 56, 5 of normal sample are incorrectly classified as Dos, Probe, R2L, and U2R, respectively, as shown in the Fig. 13.

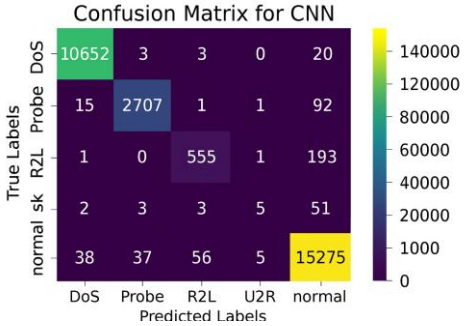

Fig. 2. Confusion matrix in LSTM for multi classification.

For each class the model produced results which are true positive and true negative. Out of the DoS test samples (10,677), 10,651 are correctly classified as DoS whereas 1, 3, none (0), 22 of DoS samples are incorrectly classified as probe, R2L, U2R, and normal, respectively. Among the total Probe (2816) sample, 2763 sample are correctly classified as Probe whereas 7, 2, 0, 44 Probe sample are incorrectly classified as Dos, R2L, U2R, and normal, respectively. In the R2L class from test sample (750), 666 sample correctly classified as R2L whereas 0, 0, 3, 81 samples of R2L wrongly classified as DoS, Probe, U2R, and normal, respectively. Among the total U2R (50) sample, 37 sample are correctly classified as U2R whereas 2, 0, 3, 8 U2R sample are incorrectly classified as Dos, Probe, R2L, and normal, respectively. In the normal class from test sample (15,411), 15,266 sample are correctly classified as normal whereas 13, 42, 88, 2 of normal sample are incorrectly classified as Dos, Probe, R2L, and U2R, respectively, as shown in the Fig. 14. When it both reach 99.38% and around 99.02% during the 1000th epoch, there is 0.002% gaps between training accuracy and validation accuracy. The start point of training and validation loss curves are shown in Fig. 2 as 0.5 and 0.23, respectively. The validation loss value goes down then experience goes up increase again decrease and training loss value also in the same way.

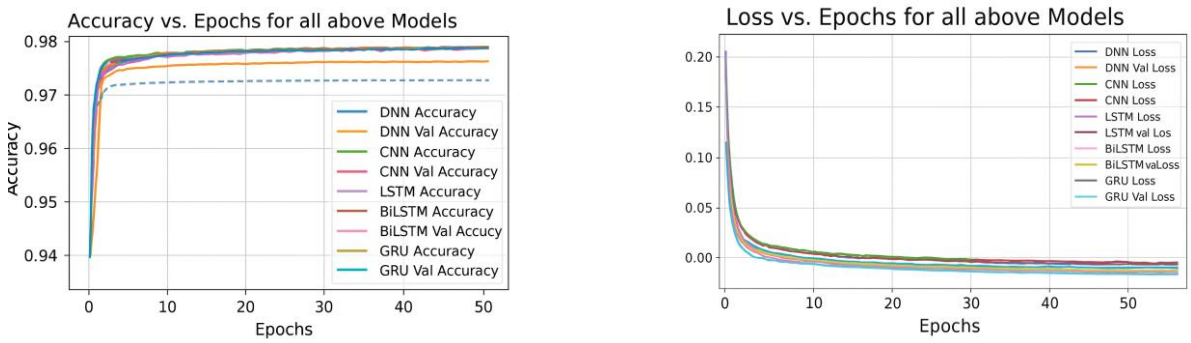

Fig. 3. Loss versus epochs for all above models using binary classification.

According to Fig. 3(a) and (b) shows which the train and validation progress of the suggested DNN model, the training accuracy value line begins nearly 92% while the validation accuracy value begins at nearly 96%. The validation accuracy value rapidly increases then when reaches above 98% decreases until 100th epoch, being below the values of the training accuracy line until the final epoch.

When it both reach 99.37% and around 98.98% during the 100th epoch, there is 0.002% gaps between training accuracy and validation accuracy. The start point of training and validation loss curves are shown in Fig. 23 is 0.3 and 0.1, respectively. The validation loss value then goes down experience nearly straight increase and training loss value also increases again decrease.

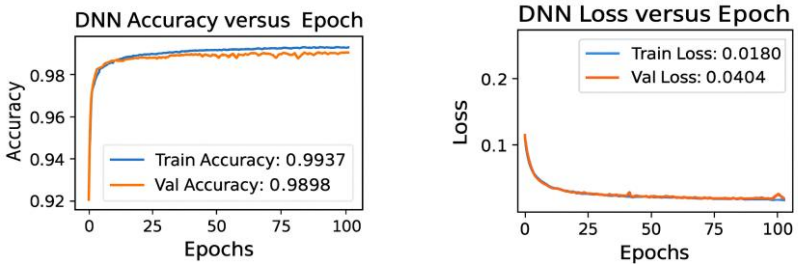

Fig. 4. Accuracy versus loss with their corresponding epochs for multi classification using DNN.

As shown in Fig.4(a) and (b), which the train and validation progress of the suggested DNN model, the training accuracy value line begins nearly 80% while the validation accuracy value begins at nearly 90%. The validation accuracy value rapidly increases then when reaches above 98% almost it continues as straight line until 100th epoch, showing nearly same values of the training accuracy line until the final epoch. When it both reach 98.49% and around 98.25% during the 100th epoch, there is 0.004% gaps between training accuracy and validation accuracy. The start point of training and validation loss curves are shown in Fig. 5. as 0.7 and 0.2, respectively. The validation loss value goes down then experience nearly straight decrease and training loss value also decreases. Extending the above analyses to the multi-class classification scenario, as illustrated in Figs. 29 and 30, the GRU and DNN models demonstrate superior performance, exhibiting higher training accuracy and lower validation loss than the other models, similar to their behavior observed in the binary classification case.

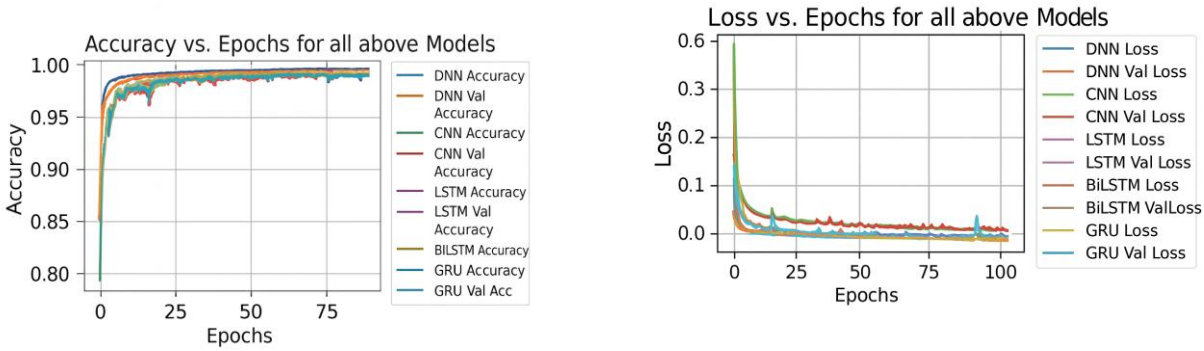

Fig. 5. Accuracy versus epochs for all above models using multi classification.

C. Test Results

The model is trained on 118,813 and tested on 29,704 for both binary and multi classification. The proposed model evaluated by using accuracy score in our study. As per the performance assessed Bi-LSTM could be the best model for both binary and multi classification of network attack. The following Table VIII and Figs. 5.which shows the test result of each model. As the Fig. 6 also shows, Bi-LSTM is the best model for multi classification when it comes to test accuracy among all the models we utilized for our investigation scoring accuracy of 99.12%.

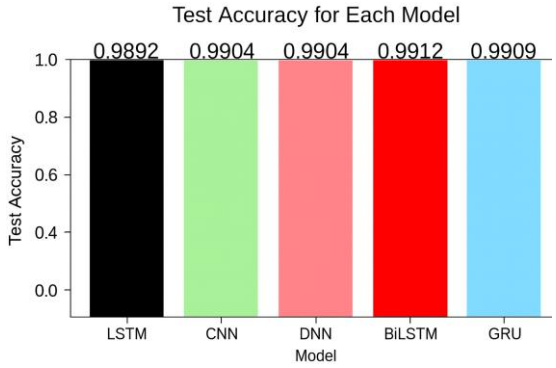

Fig. 6. Test accuracy on testing dataset sample for multi classification.

Table 3. Test Accuracy for Both Binary and Multi Classifications

Models	Accuracy	
	For binary classification	**For multi classification**
DNN	99.07%	99.04%
CNN	98.91%	98.37%
LSTM	98.94%	98.92%
Bi-LSTM	99.15%	99.12%
GRU	99.08%	99.09%

Table 3. shows the model scored best accuracy for both binary and multi classification which is 99.15% and 99.12% respectively. Therefore, this shows that Bi-LSTM is the best performing model from all models used in this study experiments even though all of them outperformed the related works stated in chapter two of this paper. As we have seen under classification reports accuracy value, recall, precision value and F1-Score is 99% for models in binary classification for both classes (normal and attack). However, as the above table shows the test results for all models used in the study, Bi-LSTM outperformed other models.

Conclusion

Computer networks have great impacts on public services, economic growth, healthcare, education, social development, and innovation are all significantly impacted by computer networks. Networks are essential to the general progress and well-being of people and communities because they enable efficient communication, information accessibility, and the seamless operation of many sectors. Four distinct types of network attacks—DoS, Probe, R2L, and U2R—were included in the 148,517 network records used in this study. The dataset was obtained from a publicly accessible source. The required data preprocessing methods, including cleaning, standardization, train-test split, label-encoding, and one-hot-encoding, are then carried out this research works. Deep learning methods were adopted for this study. To minimize training time and enhance computational efficiency, the models were trained using a Graphics Processing Unit (GPU) provided by the Google Colab environment.

This study found that Bi-LSTM outperformed the other models, achieving high accuracy to detect and classify active network attacks for binary and multi classification. As a contribution, we could experiment with five deep learning models after standardizing the data as needed to see which one can detect and classify active network attacks with a high detection rate or recall of 99.07%, low false positive rates of 0.9% and false negative rates of 0.8%, and high accuracy of 99.15% and 99.12% for binary and multi classification, respectively. Overall, this study demonstrates that the deep learning approach fared better than the earlier research listed under related works in detecting and classifying active network assault.

References

[1] M. A. T. Padmasiri, V. V. V. Ganepola, R. Herath, L. P. Welagedara, G. Ganepola, and P. Vekneswaran, “Survey on deep learning based network intrusion detection and prevention systems,” in Proc. 13th International Research Conference of General Sir John Kotelawala Defence University–2020, December 2020.

[2] G. Pang, C. Shen, L. Cao, and A. V. D. Hengel, “Deep learning for anomaly detection: A review,” ACM Computing Surveys, vol. 54, no. 2, pp. 1–36, 2021. https://doi.org/10.1145/3439950

[3] R. Chalapathy and S. Chawla, “Deep learning for anomaly detection: A survey,” arXiv Preprint, arXiv: 1901.03407v2, 2019. https://doi.org/10.48550/arXiv.1901.03407

[4] W. Yang, “Research on the relationship between computer network and economic development in information environment,” Journal of Physics: Conference Series, vol. 1744, no. 4, 2021, 042011. https://doi.org/10.1088/1742-6596/1744/4/042011

[5] R. Zeng, B. J. Jansen, H. Liang, and J. Ye, “Development of network security based on information technology,” in Proc. International Conference on Cognitive based Information Processing and Applications (CIPA 2021), 2021, pp. 321–328.

[6] Y. Bonaparte, “Global financial stability index,” SSRN, 2024. https://doi.org/10.2139/ssrn.2753667

[7] C. Ieracitano, A. Adeel, F. C. Morabito, and A. Hussain, “A novel statistical analysis and autoencoder driven intelligent intrusion detection approach,” Neurocomputing, vol. 387, pp. 51–62, 2020. https://doi.org/10.1016/j.neucom.2019.11.016

[8] A. Judith, G. J. W. Kathrine, and S. Silas, “Efficient deep learning-based cyber-attack detection for internet of medical things devices,” Engineering Proceedings, vol. 59, no. 1, 139, 2023. https://doi.org/10.3390/engproc2023059139

[9] M. Anwer, S. M. Khan, and M. U. Farooq, “Attack detection in IoT using machine learning,” Engineering, Technology and Applied Science Research, vol. 11, no. 3, pp. 7273–7278, 2021. https://doi.org/10.48084/etasr.4202

[10] S. Aftergood, “Cybersecurity: The cold war online,” Nature, vol. 547, pp. 30–31, 2017. https://doi.org/10.1038/547030a

[11] Y. Wu, D. Wei, and J. Feng, “Network attacks detection methods based on deep learning techniques: A survey,” Security and Communication Networks, vol. 2020, no. 1, 8872923, 2020. https://doi.org/10.1155/2020/8872923.

[12] M. De Lucia, P. E. Maxwell, N. D. Bastian, A. Swami, B. Jalaian, and N. Leslie, “Machine learning raw network traffic detection,” in Proc. Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications III, vol. 11746, 2021, pp. 185–194. https://doi.org/10.1117/12.2586114.

[13] V. Malhotra and M. Semwal. (August 2019). Detect malicious & benign websites using machine learning. [Online]. Available: https://www.researchgate.net/profile/Mayank-Semwal-/publication/334824944_ Comparison_of_3_ Supervised_MachineLearning_Models/links/5eb2fa7f92851cbf7fad90d4/Comparison-of-3-Supervised-Machine-Learning-Models.pdf

[14] M. Gao, L. Ma, H. Liu, Z. Zhang, Z. Ning, J. Xu, “Malicious network traffic detection based on deep neural networks and association analysis,” Sensors, vol. 20, no. 5, 1452, 2020. https://doi.org/10.3390/s20051452

[15] S. Abbas, I. Bouazzi, S. Ojo, A. Al Hejaili, G. A. Sampedro, A. Almadhor, and M. Gregus, “Evaluating deep learning variants for cyber-attacks detection and multi-class classification in IoT networks,” PeerJ Computer Science, vol. 10, e1793, 2024. https://doi.org/10.7717/peerj-cs.1793

[16] S. L. Ramaswamy and J. Chinnappan, “RecogNet-LSTM+CNN: A hybrid network with attention mechanism for aspect categorization and sentiment classification,” Journal of Intelligent Information Systems, vol. 58, no. 2, pp. 379–404, 2022. https://doi.org/10.1007/s10844-021-00692-3

[17] M. Kamyab, G. Liu, and M. Adjeisah, “Attention-based CNN and Bi-LSTM model based on TF-IDF and GloVe word embedding for sentiment analysis,” Applied Sciences, vol. 11, no. 23, 11255, 2021. https://doi.org/10.3390/app112311255

[18] B. Iung, “Cœur et grossesse,” EMC-Traité de Médecine AKOS, vol. 8, no. 2, pp. 1–4, 2013. https://doi.org/10.1016/s1634-6939(13)59289-1

[19] W. Stallings, Network Security Essentials: Applications and Standards, Chennai, India: Pearson Education India, 2011

[20] L. Alzubaidi, J. Zhang, A. J. Humaidi, A. Al-Dujaili, Y. Duan, O. Al-Shamma et al., “Review of deep learning: Concepts, CNN architectures, challenges, applications, future directions,” Journal of Big Data, vol. 8, no. 1, p. 53, 2021. https://doi.org/10.1186/s40537-021-00444-8

[21] F. Shahzad, M. Pasha, and A. Ahmad, “A survey of active attacks on wireless sensor networks and their countermeasures,” arXiv Preprint, arXiv:1702.07136, 2017. http://arxiv.org/abs/1702.07136

[22] A. A. Salih, S. Y. Ameen, S. R. M. Zeebaree, M. A. M. Sadeeq, S. F. Kak, N. Omar et al., “Deep learning approaches for intrusion detection,” Asian Journal of Research in Computer Science, vol. 9, no. 4, pp. 50–64, 2021. https://doi.org/10.9734/ajrcos/2021/v9i430229.

[23] A. A. Waoo and B. K. Soni, “Performance analysis of sigmoid and relu activation functions in deep neural network,” Intelligent Systems: Proceedings of SCIS 2021, Singapore: Springer Singapore, 2021, pp. 39–52. https://doi.org/10.1007/978-981-16-2248-9_5

[24] M. T. Tun, D. E. Nyaung, and M. P. Phyu, “Network anomaly detection using threshold-based sparse autoencoder,” in Proc. 11th International Conference on Advances in Information Technology, 2020, pp. 1–8. https://doi.org/10.1145/3406601.3406626.

[25] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, “A detailed analysis of the KDD CUP 99 data set,” in Proc. IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA 2009, 2009, pp. 1–6. https://doi.org/10.1109/CISDA.2009.5356528

[26] J. Terven, D. M. Cordova-Esparza, J. A. Romero-González et al., “A comprehensive survey of loss functions and metrics in deep learning,” Artif. Intell. Rev., vol. 58, no. 195, 2025. https://doi.org/10.1007/s10462-025-11198-7

[27] I. Butun, S. D. Morgera, and R. Sankar, “A survey of intrusion detection systems in wireless sensor networks,” IEEE Communications Surveys and Tutorials, vol. 16, no. 1, pp. 266–282, 2014. https://doi.org/10.1109/SURV.2013.050113.00191

[28] A. Chatterjee and B. S. Ahmed, “IoT anomaly detection methods and applications: A survey,” Internet of Things, vol. 19, 100568, 2022. https://doi.org/10.1016/j.iot.2022.100568

[29] C. M. Hsu, H. Y. Hsieh, S. W. Prakosa, M. Z. Azhari, and J. S. Leu, “Using long-short-term memory based convolutional neural networks for network intrusion detection,” in Proc. Wireless Internet. WICON 2018. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, 2019, vol. 264. https://doi.org/10.1007/978-3-030-06158-6_9.