NETWORK ATTACK SYSTEM PREDICTION AND THREAT ANALYSIS USING VARIOUS MACHINE LEARNING AND DEEP LEARNING TECHNIQUES

Dr. Karthikeyan Kaliyaperumal[1], Prof. Raja Sarath Kumar Boddu[2], Prof. Sai Kiran Oruganti [3]

[1]Lincoln University College, Malaysia
[2]Professor and Head of Computer Science and Engineering, Raghu Engineering College, Visakapatnam, India.
[3]Professor in Faculty of Engineering & Built Science, Lincoln University College, KL – Malaysia.

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

Abstract: The exponential rise in internet traffic and the quick development of network technologies have led to an increase in the frequency of network attacks. When someone gains unauthorized access to a network, it's called a network attack. This covers any effort to take down the network, which could have disastrous results. Traditional network infrastructure security features like firewalls, encryption, and antivirus software are heavily relied upon by organizations. These tactics do, however, offer some protection against viruses and increasingly complex attacks. Two significant artificial intelligence concepts that gained traction at the turn of the century are machine learning (ML) and deep learning (DL). By teaching computers to think like humans, these strategies' emphasis on statistical methodologies and data may significantly increase computing capacity. By teaching computers to think like humans, these strategies' emphasis on statistical methodologies and data may significantly increase computing capacity. Therefore, computer scientists began using intelligent approaches in network security to solve the shortcomings of non-intelligent systems. Many deep learning and machine learning techniques for attack detection and classification are thoroughly examined.

Keywords: *Cyber Security attacks, Machine learning, , Intrusion detection, DNN, CNN, Network attacks*

I. INTRODUCTION

The objective of a network attack aims to gain unauthorized access to a company's network in order to steal information or carry out harmful activities. An internal assault or an external attack are two potential origins of the danger. Enhancing data transmission and circulation has been a persistent objective of networking systems. Their dedication to ongoing development has made it easier to launch a number of cutting-edge services. Cloud computing, which allows the on-demand delivery of various applications, services, and processing and storage resources to numerous users via the Internet, has been made possible by recent developments in network technology.

This paradigm offers several advantages, including enhanced accessibility, efficiency, and dependability; less administrative load; cost-effective resource utilization; and other additional benefits. A multitude of individuals that engage with networks benefit from the Internet's continual enhancement and extensive use from many perspectives. The significance of network security is increasing as network use becomes more prevalent. Network security encompasses computers, networks, software, data, and related components, with the objective of safeguarding against unauthorized access and modification. Cyberattacks provide a substantial risk and inflict considerable damage on the growing array of internet connected equipment used in the banking industry, e-commerce, and the military. Ten percent of active assaults are denial-of-service (DoS) attacks. When offenders implement actions to incapacitate a tool or network, it is termed a Denial-of-Service attack. The first user may lose access to the device or network as a consequence of this.

An assailant may render a device or network unusable or even incinerate it by inundating it with traffic. Services such as online banking, email, and websites are affected. A denial-of-service attack (DoS) may be initiated

from any location. Disrupting an ongoing conversation or data transfer is referred to as a man-in-the-middle attack, a kind of eavesdropping. The offenders assume the identities of two legitimate entities after positioning themselves in the intermediary role of the transfer [5-7].

An intrusion detection system may discover malicious activity by collecting and analyzing data from the network, its connected computers, and the security log. An intrusion detection system may protect a system via real-time responses by assessing anomalous behaviors against the security policy and signs of an attack. In traditional setups, an intrusion detection system (IDS) enhances a firewall—primarily a passive defence mechanism—in a rational, proactive, and efficient manner. Intrusion Detection Systems (IDSs) can identify cyberattacks that may jeopardise information systems. Intrusion Detection Systems (IDS) perform their functions by examining two categories of data: one related to the operating system (HIDS) and the other related to the network (NIDS). The use of NIDSs has efficiently utilized data mining techniques, which are also applied in several other domains. Network data, however, resists uncomplicated use by commercially accessible data mining techniques. The intricate procedure of intrusion detection starts with the aggregation of network data and proceeds with its preparation and preprocessing. Machine Learning (ML) verses Deep Learning (DL), two factor key artificial intelligence techniques in network security, underpin several innovative detection procedures designed to swiftly and efficiently identify attacks.

1) Machine Learning versus Deep Learning

A lot of machine learning (ML) is used to recognize different kinds of attacks. A machine learning methodology could help the network administrator take the necessary steps to prevent breaches. However, the majorities of conventional machine learning techniques fall within the category of shallow learning and often pay attention to feature selection and engineering. Shallow learning is unable to effectively address the categorization problem when faced with massive amounts of intrusion data that emerge in a real-time network environment [29]. In contrast, Deep learning techniques can generate considerably more effective prototypes and have the ability to derive better representations from dynamic data sets(Yin et al., 2017).

A collection of techniques known as "representation learning" or "feature learning" in classical models makes the algorithm automatically learn the representations needed for feature detection from the training dataset. On the contrary, deep learning (DL) may be viewed as establishing machine learning and representation learning jointly. With many levels of cumulative complexity and generalization, as well as the final prediction, DL aims to jointly learn fundamental traits.

2) Limitations of machine learning

Manual Feature Engineering: Traditional machine learning approaches often rely on manual feature engineering, which can be time-consuming, labor-intensive, and prone to bias. Handcrafted features may fail to capture refined or complex patterns in the data and may not generalize well to new or unseen attack scenario [28].

Limited Generalization: Traditional machine learning models may struggle to generalize effectively to new or unseen attack patterns, especially in dynamic and evolving network environments. Models trained on historical data may become outdated or ineffective in detecting novel or sophisticated attack strategies, which leads toward reduced detection performance [50]. Limited Adaptability: Traditional machine learning models may have limited adaptability to changing network conditions, attack tactics, and enemy strategies over time. These models may not dynamically adjust to new attack patterns or concept drift in network traffic data, requiring frequent retraining or manual intervention to maintain effectiveness.

3) Deep Learning Approaches

Deep learning has emerged as a powerful approach for active network attack detection and classification, offering significant advantages over traditional methods [1].

Feature Learning: Deep learning models can automatically learn hierarchical representations of raw input data, such as network traffic packets or logs, without the need for handcrafted feature engineering. By processing raw data through multiple layers of nonlinear transformations, deep learning models extract informative features directly from

the input, enabling them to capture complex patterns and relationships that may be difficult to specify manually. Deep learning models, including Deep Neural Networks (DNNs), Convolutional Neural Networks (CNNs), Long Short-Term Memory networks (LSTMs), Bidirectional LSTMs (BiLSTMs), and Gated Recurrent Units (GRUs), have significant applications in network attack detection and classification.

4) Deep Neural Networks (DNN)

DNNs can be employed for general network attack detection by learning complex patterns in network traffic data. It consists of multiple layers of neurons, typically including an input layer, several hidden layers, and an output layer. Each layer performs linear combinations of inputs followed by a non-linear activation function. DNNs can be fully connected; meaning every neuron in one layer is connected to every neuron in the subsequent layer. DNNs are versatile and can learn complex patterns from network traffic data. Their ability to learn from large datasets makes them effective for identifying previously unseen attack patterns. It can be used to classify traffic as normal or malicious based on features like packet size, timing, and source/destination addresses [38].

5) Networks (CNNs) Convolutional Neural

CNNs are commonly used for analyzing spatial data, such as images, but they can also be applied to sequential data, such as network traffic sequences. In the context of active attack detection, CNNs can learn spatial features from network traffic data, such as packet headers or content, to identify characteristic patterns associated with different types of attacks. By twisting filters across input sequences and combining spatial information, CNNs can effectively capture local dependencies and spatial correlations in network traffic data, enabling accurate detection and classification of active attacks [33].

6) Long Short Term Memory (LSTM)

Long short-term memory (LSTM) is a unique kind of artificial recurrent neural network (RNN) architecture that is utilized in the deep learning field. It is effective in detecting network attacks due to their ability to capture long-term dependencies in sequential data, particularly in analyzing time-series data like traffic logs or sequences. For example, LSTMs can identify anomalies in user behavior by analyzing sequences of actions taken over time, helping to distinguish between legitimate and malicious activities. They consist of memory cells and information-controlling gates (input, forget, and output gates). Because of this, LSTMs may retain and pick up dependencies throughout lengthy sequences. LSTMs are ideally suited for studying sequential data, such as traffic flows over time, which makes them useful for network attack detection [23].

7) Bidirectional LSTMs (BiLSTMs)

BiLSTMs extend the capabilities of LSTMs by processing data in both forward and backward directions. This bidirectional approach allows the model to consider context from both past and future states, enhancing its ability to detect complex attack patterns. BiLSTMs have been shown to outperform traditional LSTM models in tasks requiring a deeper understanding of context, such as identifying specific types of network attacks based on historical traffic behavior [21].

8) Gated Recurrent Units (GRUs)

GRUs are similar to LSTMs but with a simplified architecture that combines the forget and input gates into a single update gate. This makes GRUs computationally efficient while still effectively capturing dependencies in sequential data. In network attack detection, GRUs can be used to analyze patterns in network traffic and identify deviations from normal behavior, making them suitable for real-time monitoring applications.

B. Types of network attacks

Broadly applicable security attacks are classified into passive attacks and active attacks. A passive attack attempts to learn or make use of information from the system but does not affect system resources, whereas an active attack attempts to alter system resources or affect their operation. Any effort to alter the system without authorization is considered an active attack. For instance, this could involve altering data that have been sent or stored, generating new data streams through masquerading or fabrication, replaying or changing messages, and causing a denial of service or availability disruption [9]. Network attack detection involves the proactive monitoring of network traffic, system logs, and behavior patterns to quickly identify and respond to unauthorized access attempts, malware infections, and other forms of cyber-attacks [40]. Our research will focus on active network attack detection and classification. Focusing on active network attack detection and classification is vital because of increasing

sophistication as well as prevalence of network attacks. Active attacks, where hackers attempt to alter or disrupt network operations, pose significant risks to the integrity and availability of systems.

In this study, attack types are classified using the following network attack classes:

Denial of Service (DoS): A DoS attack aims to overwhelm a system or network resource, making it unavailable to its intended users. This type of attack disrupts services by flooding the target with excessive traffic or requests, causing it to crash or become unresponsive [1].

Remote-to-Local (R2L): R2L attacks involve unauthorized users attempting to connect remotely and obtain local access to a system. Attackers exploit vulnerabilities of a system to increase their privileges and gain unauthorized access to sensitive data or resources [1].

User-to-Root (U2R): U2R attacks involve users with limited privileges attempting to gain root or administrative access to a system. Attackers exploit vulnerabilities to increase their privileges and gain unauthorized control over the system, potentially leading to data breaches or system compromise [45].

Probe: Probe attacks involve attackers scanning a network to gather information about potential vulnerabilities and system configurations. These attacks are reconnaissance activities aimed at identifying weaknesses that could be exploited in subsequent attacks [19].

C. Statement of the Problem:

Modern society has developed because of computer networks, which have an impact on public services, economic growth, healthcare, education, social development, and innovation. By facilitating effective communication, information accessibility, and the smooth functioning of diverse industries, networks play a vital role in the general advancement and well-being of individuals and communities.

According to the Director General, financial institutions, security institutions, media outlets, important government offices, ministries, regional offices, hospitals, and higher education establishments made up the majority of the targets of cyber-attacks.

To solve related problems stated above, a number of studies have been performed using traditional and advanced machine learning methods globally. Ieracitano et al. [20] employed NSL-KDD dataset in order to implement the method of intelligent intrusion detection driven by auto encoders. Even though it is encouraging, improvements are still needed to increase its accuracy and dependability. Other researchers [22] have also performed deep learning-based cyber-attack detection for the internet of Medical Things (IoMT). The approach achieved a significant accuracy of 96.39%, but it was limited to man-in-the-middle attacks, indicating the need for a more comprehensive detection system that can handle a wider range of cyber threats. Since traditional machine learning methods have difficulty in efficiently detecting and classifying attackers because cyber security issues take the form of new and sophisticated methods, it is essential to research and develop novel methods using deep learning techniques. The difficulty in choosing features as the amount of data increases is reducing the attack detection rate in terms of traditional machine learning. R2L, U2R, probe, and DoS attack types classified with low accuracy.

High False Positive Rates Moreover, due to the challenges in feature selection and classification accuracy, there is a risk of high false positive rates, where benign activities are incorrectly classified as attacks. Overall, these issues can significantly impact the effectiveness of attack detection systems, potentially leading to an increased risk of security breaches and false alarms.

D. Objectives

The general objective of this study is to develop a deep learning model for difficulty in efficiently detecting and classifying active network attack.

II. RELATED WORK

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.

These network components need to be reliable and secured through advanced deep learning technologies to detect and mitigate anomalies.

Shahzad et al.,[47] provided a comprehensive survey of intrusion detection systems (IDSs) tailored for wireless sensor networks (WSNs). 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, (Ni, 2023) 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.

Deep learning techniques have emerged as promising approaches for anomaly detection in network traffic. [25] conducted a thorough review of deep learning methods for anomaly detection, demonstrating the effectiveness of neural network architectures in capturing complicated patterns indicative of malicious activities.

In a similar [40] investigated the application of deep learning approaches specifically for network intrusion detection. Their review offers insights into the design and evaluation of deep learning models, emphasizing their scalability and adaptability to evolving threat landscapes.

Furthermore, [47] 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 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 [10].

Researchers 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 [12].

A novel approach to intelligent intrusion detection using auto encoder-driven intelligence and statistical analysis was developed by researchers, which achieved 87% accuracy for malt classification and 84.21% accuracy for binary classification using NSL-KDD [20]. Even though the work is appreciated, it still needs more improvement.

Other studies have also explored the use of long short-term memory (LSTM)-based convolutional neural networks to detect network intrusions. They emphasize the growing relevance of network security as the internet becomes more widely used. Researchers have suggested two deep learning models, LSTM-only and CNN-LSTM, to increase the performance of intrusion detection systems, with the NSL-KDD dataset serving as a benchmark. This work aimed to solve the constraints of existing machine learning algorithms in intrusion detection, and it achieved 94.12% and 88.95% accuracy for binary classification and multi-classification, respectively [18].

PCA has been utilized for feature reduction and employs a multilayer perceptron to classify unforeseen cyber-attack IoT-based healthcare devices. The study results indicated that the multilayer perceptron outperforms the other tested classifiers, achieving an accuracy of 96.39% while also improving the performance by reducing the time complexity [22]. Even if the accuracy is significant, it is particularly focused on only man-in-the-middle attacks.

Sarumi et al. compared intrusion detection systems, specifically examining Apriority, which use data mining association rule techniques, and Support Vector Machine, which utilizes machine learning methodologies. We assess the two systems based on the UNSW-NB15 and NSL-KDD datasets, which represent the University of New South Wales – Knowledge Discovery and Data Mining (Sahoo et al.) assert that the centralized control capability of SDN may be used to detect attack traffic.

Tuan et al. [48] suggested a detection method for botnet DDoS attacks using machine learning techniques. The UNBS-NB 15 and KDD99 publicity datasets, renowned for detecting Botnet DDoS attacks, were used to evaluate the methodology. We analyzed the dataset's sensitivity, accuracy, specificity, area under the curve (AUC), false positive rate (FPR), and used several machine learning techniques including support vector machine (SVM), naïve bayes (NB), unsupervised learning (USML), and decision tree (DT). Kim et al. developed the convolutional neural network (CNN) model for denial-of-service attacks. They created double types of invasion photographs: RGB and greyscale. In constructing their CNN model, they considered the kernel size and the number of convolutional layers. The CNN model exhibited superior results on the KDD dataset, attaining multiclass and binary classification accuracies of 99% or above. The RNN achieved an accuracy of 99% in binary categorization. The objective of the deep learning model created by Yang et al. was to detect malicious traffic inside an encrypted network. The proposed model originated from a Residual Neural Network (ResNet). The adversarial sample of encrypted traffic was produced with Deep Convolution Generative Adversarial Networks (DCGAN) and Deep Q-Network (DQN) reinforcement learning.

The open-source Balabit Mouse Dynamics challenge for the dataset and the CNN methodology were used. CNN exhibited robust efficacy in user authentication using mouse features, achieving a FAR of 2.94% and a FRR of 2.28%. A technique for the early identification of distributed denial-of-service (DDoS) assaults executed via a botnet integrates real network data with deep convolutional neural networks (CNNs), To execute a coordinated distributed denial of service (DDoS) attack inside a cell that might impair CPS operations. Liang et al. primarily focused on an intrusion detection system using a hybrid placement strategy that integrates multi-agent systems, blockchain technology, and deep learning algorithms. The system was meticulously created, deployed, and tested. The primary components of the system are data collection, data management, analysis, and response. The system is evaluated using the NSL-KDD dataset, which represents the National Security Lab Knowledge Discovery and Data Mining. The results demonstrate that deep learning systems are proficient at detecting transport layer attacks. The findings indicate that deep learning techniques are effective in identifying breaches inside IoT networks.

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 [5]. A novel approach to intelligent intrusion detection using auto encoder-driven intelligence and statistical analysis was developed by researchers, which achieved 87% accuracy for malt classification and 84.21% accuracy for binary classification using NSL-KDD [20]. Even though the work is appreciated, it still needs more improvement. Other studies have also explored the use of long short-term memory (LSTM)-based convolutional neural networks to detect network intrusions. A study entitled Efficient Deep Learning-Based Cyber-Attack Detection for internet of Medical Things Device has also been performed to detect cyber-security threats, with a particular focus on man-in-the-middle attacks that occur within the IoMT communication network. PCA has been utilized for feature reduction and employs a multilayer perceptron to classify unforeseen cyber-attack IoT-based healthcare devices. The study results indicated that the multilayer perceptron, achieving an accuracy of 96.39% complexity [22]. Even if the accuracy is significant, it is particularly focused on only man-in-the-middle attacks. Relevance to Deep Learning. Complex Patterns: Both CICIDS2017 and UNSW-NB15 datasets contain complex patterns and relationships, making them suitable for deep learning-based approaches. Large-Scale Data: In summary, the CICIDS2017 and UNSW-NB15 datasets are more relevant and modern, providing a more accurate representation of current cyber threats and realistic network traffic. They are well-suited for training deep learning-based intrusion detection models.

The study scores low accuracy in the context of a secure network. As we reviewed a number of related works, most studies have been performed using traditional machine learning models. However, such a system may have unsatisfactory results due to its low capability for problem space definition and complexity in modeling malicious activities [50].

A. Research Gap and Future Directions

Therefore, in this research, we used deep learning approach to improve the detection and classification of active network attacks. The proposed study aims to address the identified research gap by developing a novel deep learning-based architecture for active network attack detection and classification. active network attack. Even though the researcher did all necessary to obtain the intended results and the level of accuracy for this approach; there is still opportunity for improvement as long as the accuracy is not exactly 100% and some problems remain unresolved. Future research directions for applications to detect and classify active network attack. It includes: Expanding the scope of this study rather than using only five models (DNN, CNN, LSTM, BiLSTMs and GRU) by including other deep learning models, such as transfer learning to detect and classify active network attack developing real time application and integrating to networked technologies using the model that outperformed in this study. Although deep learning based BiLSTMs model has been demonstrated as the best-performing model according to methods and procedures used in this study, using other experimental methodology could be improve model performance than this study.

By addressing this research gap and proposing a novel approach to active network attack detection and classification using deep learning, this study aims to contribute to advancing the most recent developments in cyber security and strengthening networked systems' resistance to changing threats.

.

III. RESEARCH METHODS

Support Vector Machines (SVM) are used for classification, regression, and outlier detection. It is a supervised learning model. The data is split linearly by the hyperplane. Support vector machines (SVMs) split data into classes by using a hyperplane that maximizes the model margin between class occurrences, after the mapping of data into feature space. This classifier can do both binary and multi-class classification. Support Vector Machines excel in the presence of nonlinear data. Several research using SVM to detect intrusions. The SVM concludes data categorization by identifying the largest classification margin. The SVM classification technique use a hyperplane to distinguish between positive and negative class variables, using the principle of structural risk minimization.

Benchmarked Datasets: Utilizing benchmarked datasets like KDD99, NSL-KDD, or CIC-IDS2017 is essential for evaluating the performance of DL models in network attack detection. An exceptionally effective data mining technique is the Random Forests algorithm, which integrates ensemble approaches for classification and regression. A variety of applications have extensively used the random forests approach. It has been used for calculating probability and formulating forecasts. As its name suggests, RF constructs a forest comprised of several decision trees. No accuracy is lost despite the significant absence of data. Derived from the Shallow Neural Network (SNN), Deep Neural Networks (DNN) have lately been a primary focus of research in the field of intrusion detection. In the realm of simulating intricate models, DNN surpasses its competitors significantly. Thirimanne et al. assert that the capacity of DNNs to accurately characterize data and provide viable solutions is extensive. The ReLU activation function, characterized as a piecewise linear function, outputs the input value when the input is positive; if not, it yields zero. The nodes triggered by this function are referred to as rectified linear activation units. The Sigmoid function was used to activate the output layer since it can convert any real number into a range between zero and one.

IV. 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. The NSL-KDD dataset also includes a wide variety of attack types, categorized into four major classes which are DoS. Attempts to

make a machine or network resource unavailable to its intended users. Probe: Attempts to gather information about a network or system, often as a precursor to an attack. R2L. This diversity makes the dataset suitable for training models that can detect and classify different types of network attacks.

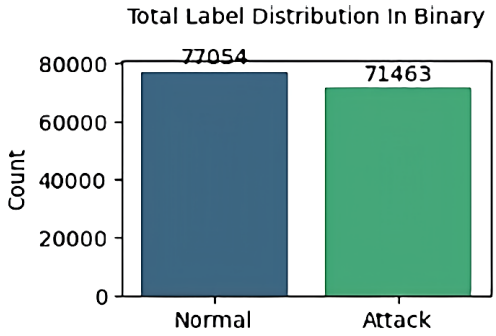


Fig.1. Binary classification in training set and test set.

TABLE I. BINARY CLASSIFICATION IN TRAIN AND TEST

Category	Train	Test	Total
Normal	61,643	15,411	77,054
Dos	42,708	10,677	53,385
R2L	2999	750	3749
U2R	202	50	252
Probe	11,261	2816	14,077
Total	**118,813**	**29,704**	**148,517**

As the above Table I shows in binary classification from total dataset, 77,054 were classified as normal whereas 71,463 were classified as attack. Revealed on the binary classification from the total dataset normal 77,054 and 71,463 attack classes, 15,411 and 14,293 used as normal and attack for test respectively. The total number of data which incorporated in this experiment is 148,517 records the dataset utilized were divided into normal and attack categories. In this study, 80 % of data dataset is used for the training and 20 % of data for testing. With this dataset binary classification and multi-class classification were trained and tested.

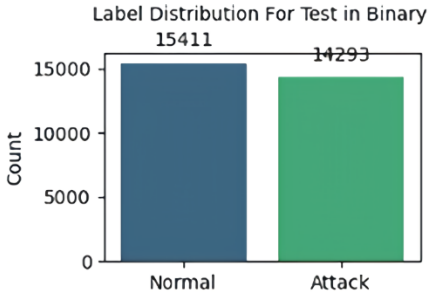


Fig. 2. Binary classification label distribution for test dataset.

1) *Network Attack in terms of multi classification*

NSL-KDD was used in experiments which dived into two categories. It is train category and test category. We used 80% and 20% of total dataset for training and testing respectively, while test data is used make up of create new instance which is not found in the train data and use to create a model. The number of data used in NSL-KDD train and NSL-KDD test were shown in Table II below.

TABLE II. MULTI CLASSIFICATION IN TRAIN AND TEST USING 80 % AND 20% DATASET SPLIT

Category	Train	Test	Total
Normal	61,643	15,411	77,054
Attack	57,170	14,293	71,463
Total	118,813	29,704	148,517

The total number of data used in these experiments was 148,517 with train accounting for 80% and test accounting for 20%. There are 118,813 instances in the train data. (Normal is 61,643, Dos attack 42,708, R2L attack is 2999, U2R attack is 202, and Probe attack is 11,261) where as there are 29,704 instances in test data which are (Normal 15,411, Dos attack 10,677, R2L attack 750, U2R attack 50 attack Probe attack 2816) in test dataset split.

Normal and Dos have large instance across datasets used for testing and training. As indicated in the Table IV, next to probe, R2L and U2R have small instances in both train and test dataset. From the dataset we split into five labels which means normal labels 77,054 Dos 53,385, Probe 14,077, R2L 3749 and U2R 252 network is more affected by Dos and Probe respectively. From these we used for test 15,411, 10,677, 2816, 750, 50 normal, DoS Probe, R2L, U2R respectively as it is shown on the figures.

The following are the class or category that attacks in train and test instances mapped to:

DOS: Appache, back, land, mail, bomb, netpune, pod, processtable, smurf, teardrop, udpstorm.

R2L: ftp-write, Guess password, Internet Message Access Protocol (IMAP), mult hop, named, phf, send mail, Snmpget attack, Snmp guess, spy, warez, client, warez master, worm, X lock, X snoop.

U2R: Buffer overflow, laodmodule, perl, rootkit, httptunnel, ps, sqlattack and xterm.

Probe: IP sweep, Mscan, Namp, Port sweep, saint.

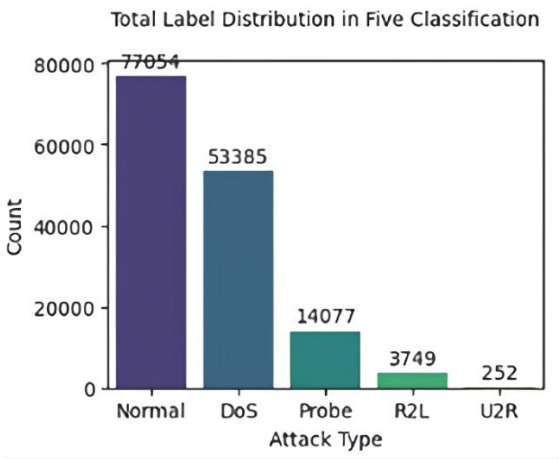


Fig.3. Total distribution of normal and attack types.

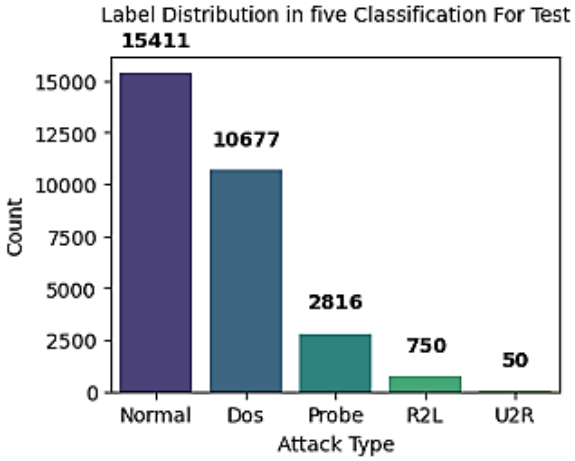


Fig.4. Distribution of normal and attack types for test.

2) HYPER PARAMETERS USED FOR ALL MODELS IN THIS RESEARCH

An epoch is one complete pass of the training dataset in the algorithm. This epoch number is important hyper parameters for the algorithm. It shows how many full iterations or the whole set of training data undergoing during the algorithm training or processing. Training will come to conclusion at the time number of iterations surpasses number of epochs. When trained by minimum error, with the maximum number of iterations. Batch size is the number of samples that pass through to the network at one time. As it is shown the Table III, we used 50, 100 epochs and batch size is 512 with Bayesian optimized algorithm for binary and multi classification respectively.

TABLE III. HYPER PARAMETERS USED IN BOTH BINARY AND MULTI CLASSIFICATION

Models	Epochs		Batch Size
	For binary classification	For multi classification	
DNN	50	100	512
CNN	50	100	512
LSTM	50	100	512
BiLSTM	50	100	512
GRU	50	100	512

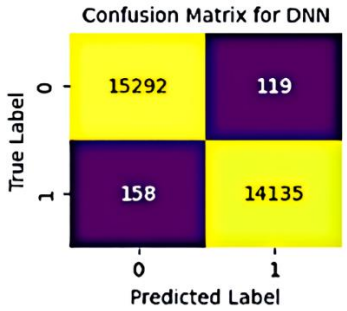


Fig.5. Confusion matrix in DNN for binary classification.

The above Fig. 5 shows the classification report of the performance classification outcome for DNN utilizing the binary classes' a confusion matrix the counts of TP, TN, FP, and TN for each class are displayed in the above classification confusion matrix norma1(0) and attack(1). For each class the model produced results which are true positive and true negative out of the normal test samples (15,411), 15292 are correctly categorized as normal, 119 normal samples are mistakenly categorized as attack and from 14293 attack samples, 14135 are correctly classified as attack whereas 158 instances incorrectly classified as normal.

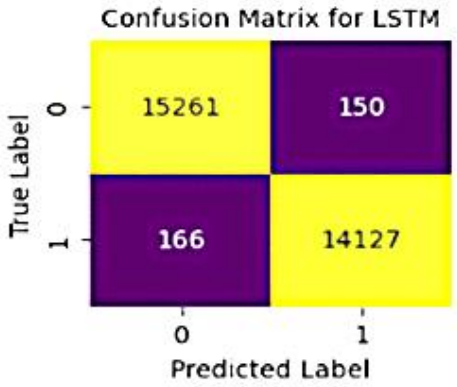


Fig.6. Confusion matrix in LSTM for binary classification.

According to the above Fig. 6 show the report of performance classification outcome for LSTM utilizing the binary classes' confusion matrices shows each class's TP, TN, FP, and TN counts norma1(0) and attack(1). For each class the model produced results which are true positive and true negative out of the normal test samples (15,411), 15261 are correctly categorized as normal, 150 normal samples are mistakenly categorized as assault and from 14293 attack samples, 14127 are correctly classified as attack whereas 166 instances incorrectly classified as normal.

Classification Report for DNN

	Precision	recall	f1-score	support
0	0.99	0.99	0.99	15411
1	0.99	0.99	0.99	14293

Accuracy			0.99	29704
Macro avg	0.99	0.99	0.99	29704
Weighted avg	0.99	0.99	0.99	29704

Classification Report and Confusion matrix in CNN for binary classification

Classification Report for CNN:

	Precision	recall	f1-score	support
0	0.99	0.99	0.99	15411
1	0.99	0.99	0.99	14293
Accuracy			0.99	29704
Macro avg	0.99	0.99	0.99	29704
Weighted avg	0.99	0.99	0.99	29704

The report above shows the performance classification outcome for CNN utilizing the binary classes' confusion matrices the counts of TP, TN, FP, and TN for every class norma1(0) and attack(1).

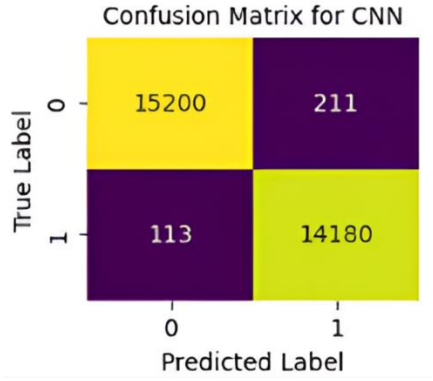


Fig.7. Confusion matrix for CNN classification.

	Precision	recall	f1-score	support
0	0.99	0.99	0.99	15411
1	0.99	0.99	0.99	14293
Accuracy			0.99	29704
Macro avg	0.99	0.99	0.99	29704
Weighted avg	0.99	0.99	0.99	29704

According to the above Fig. 7 shows the performance classification outcome for CNN utilizing the binary classes' confusion matrices the counts of TP, TN, FP, and TN for every class norma1(0) and attack(1). For each class the model produced results which are true positive and true negative out of the normal test samples (15,411), 15200 are correctly categorized as normal, 211 normal samples are mistakenly categorized as assault and from 14293 attack samples, 14180 are correctly classified as attack whereas 113 instances incorrectly classified as normal.

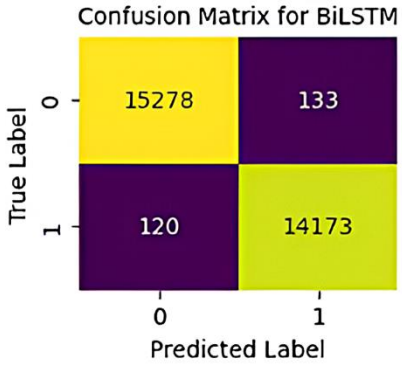


Fig.8. Confusion matrix in BiLSTM in terms of binary classification.

Classification Report for BiLSTM:

	Precision	recall	f1-score	support
0	0.99	0.99	0.99	15411
1	0.99	0.99	0.99	14293
Accuracy			0.99	29704
Macro avg	0.99	0.99	0.99	29704
Weighted avg	0.99	0.99	0.99	29704

As it could be seen from the above report, the performance classification outcome for BiLSTM utilizing the binary classes' confusion matrices the counts of TP, TN, FP, and TN for every class norma1(0) and attack(1). For each class the model produced results which are true positive and true negative out of the normal test samples (15,411), 15,278 are correctly categorized as normal, 133 normal samples are mistakenly categorized as attack and from 14,293 attack samples, 14,173 are correctly classified as attack whereas 120 instances incorrectly classified as normal as in shown in Fig.8.

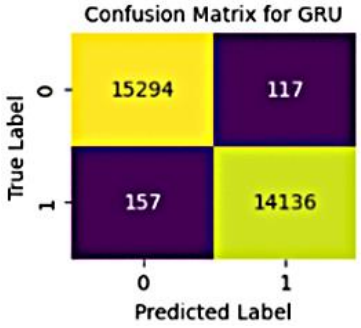


Fig.9. Confusion matrix in GRU for binary classification.

Classification Report for GRU:

	Precision	recall	f1-score	support
0	0.99	0.99	0.99	15411
1	0.99	0.99	0.99	14293
Accuracy			0.99	29704
Macro avg	0.99	0.99	0.99	29704
Weighted avg	0.99	0.99	0.99	29704

The above confusion matrix and classification report shows the performance classification outcome for GRU utilizing the binary classes' confusion matrices the counts of TP, TN, FP, and TN for every class norma1(0) and attack(1).

For each class the model produced results which are true positive and true negative out of the normal test samples (15,411), 15,294 are correctly categorized as normal, 117 normal samples are mistakenly categorized as attack and from 14,293 attack samples, 14,136 are correctly classified as attack whereas 157 instances incorrectly classified as normal as in shown in Fig. 9.

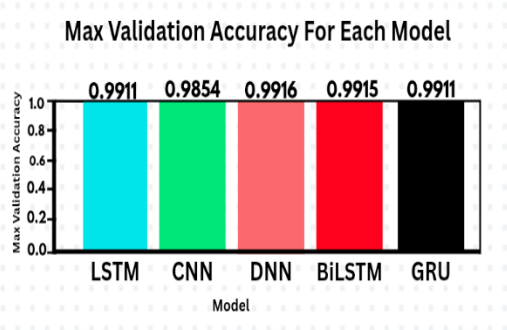


Fig. 10. Max validation accuracy in binary for each model.

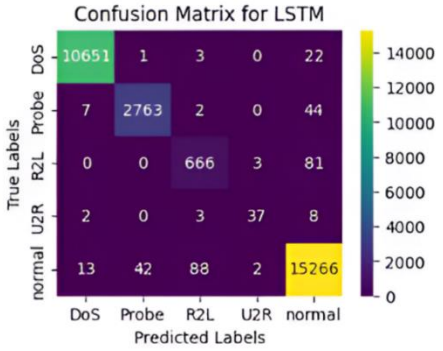
Among models used in this study, BiLSTM scored 99.23% validation accuracy during training while LSTM, GRU, DNN and CNN scored 99.21%, 99.17%, 99.16%, and 99.07% respectively for binary classification as shown in Fig. 10.

Classification Report and Confusion Matrix in DNN for Multi Classification

Classification Report for DNN:

	Precision	recall	f1-score	support
DoS	1.00	1.00	1.00	10677
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	15411
Accuracy			0.99	29704
Macro avg	0.95	0.92	0.93	29704
Weighted avg	0.99	0.99	0.99	29704

The confusion matrix above 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 and U2R and normal respectively. Among the total Probe (2816) sample, 2744 sample are correctly classified as Probe whereas 4, 1, 1, 66 Probe sample are incorrectly classified as Dos, R2L, U2R and normal respectively. In the R2L class from test sample (750), 697 sample correctly classified as R2L whereas 1, 0, 2, 50 samples of R2L wrongly classified as DoS, Probe, U2R and normal respectively.



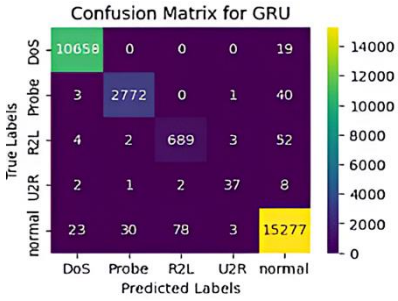
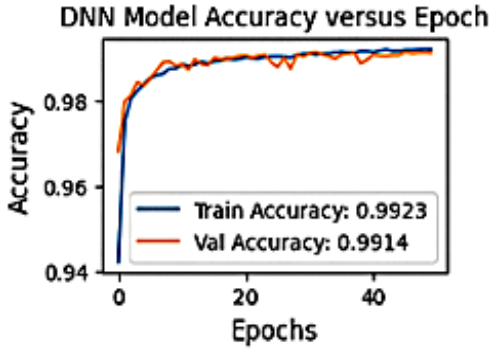


Fig. 11. Confusion matrix in CNN for Multi classification. Fig. 12. Confusion matrix in GRU for multi classification.

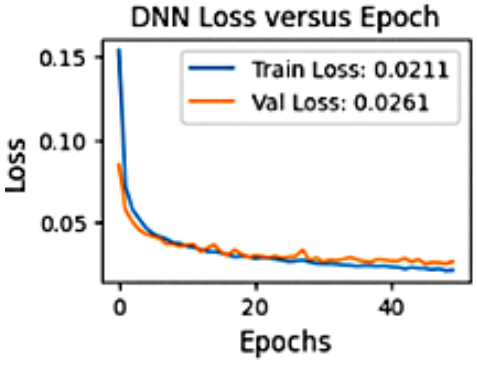
Classification Report for GRU:

	Precision	recall	f1-score	support
DoS	1.00	1.00	1.00	10677
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	15411
Accuracy			0.99	29704
Macro avg	0.94	0.93	0.93	29704
Weighted avg	0.99	0.99	0.99	29704

Finally, the above confusion matrix shows the performance classification outcome for GRU 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), 10,658 are correctly classified as DoS whereas 0, 0, 0, 19 of DoS samples are incorrectly classified as probe, R2L and U2R and normal respectively. Among the total Probe (2816) sample, 2772 sample are correctly classified as Probe whereas 3, 0, 1, 40 Probe sample are incorrectly classified as Dos, R2L, U2R and normal respectively. In the R2L class from test sample (750), 689 sample correctly classified as R2L whereas 4, 2, 3, 52 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, 1, 2, 8 U2R sample are incorrectly classified as Dos, Probe, R2L and normal respectively. In the normal class from test sample (15,411), 15,277 sample are correctly classified as normal whereas 23, 30, 78, 3 of normal sample are incorrectly classified as Dos, Probe, R2L and U2R respectively as shown in the Figures.



(a)



(b)

Fig. 13. Accuracy versus Loss with their corresponding epochs for binary classification using DNN

According to Fig. 13 shows, which the train and validation progress of the suggested CNN model, the training accuracy value line begins nearly 93% while the validation accuracy value begins at nearly 95.5%. The validation accuracy value rapidly increases until the 50th epoch, surpassing and overlapping the values of the training accuracy line as it began to climb with decreases and increase until the final epoch. When it both reach 99.07% and around 99.01% during the 50th epoch, there is 0.003 percent gaps between training accuracy and validation accuracy. The start point of training and validation loss curves are mentioned as 0.20 and 0.13 respectively. The validation loss value goes down then experience nearly straight decrease and training loss value also decrease.

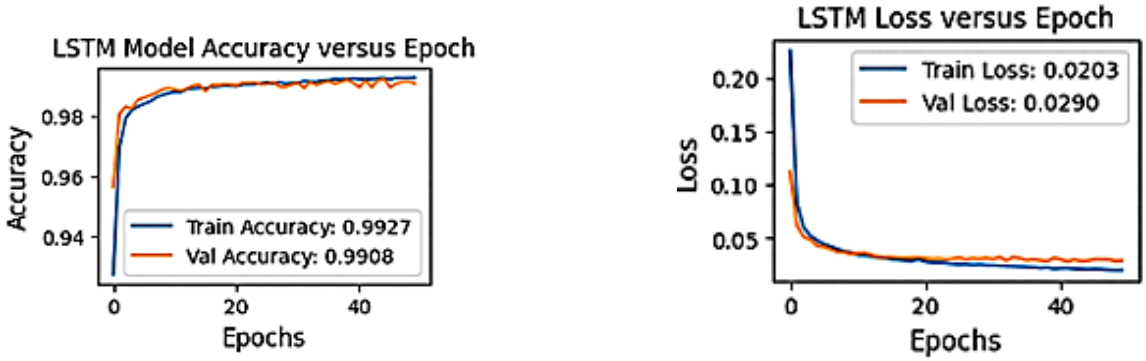
(a) (b)

Fig. 14. Accuracy versus Loss with their corresponding epochs for binary classification using CNN.

According to the following Fig. 14 (a) and (b) shows, which the train and validation progress of the suggested LSTM model, the training accuracy value line begins nearly 91% while the validation accuracy value begins at nearly 96%. The validation accuracy value rapidly increases and decreases until the 50th epoch, sometimes surpassing and being below the values of the training accuracy line as it began to climb with decreases and increase until the final epoch.

When it both reach 99.27% and around 99.08% during the 50th epoch, there is 0.008 percent gaps between training accuracy and validation accuracy. The start point of training and validation loss curves are shown in Fig. 19 as 0.21 and 0.10 respectively.

The validation loss value goes down then experience nearly straight increase and training loss value also increase.



(a) (b)

Fig. 15. Accuracy versus Loss with their corresponding epochs for binary classification using LSTM

As Fig. 15. shows, which the train and validation progress of the suggested BiLSTM model, the training accuracy value line begins nearly 92% while the validation accuracy value begins at nearly 97%. The validation accuracy value rapidly increases until the 50th epoch, surpassing the values of the training accuracy line as it began to climb with decreases and increase until the final epoch.

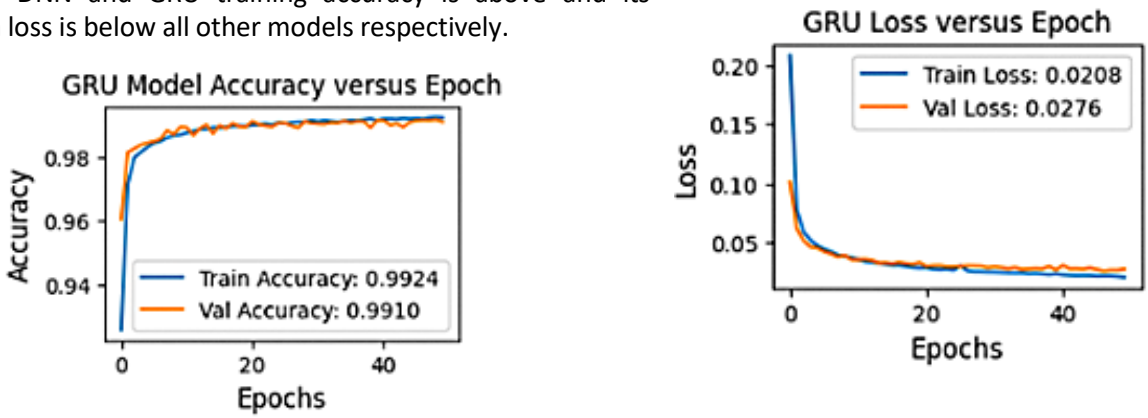
When it both reach 99.31% and around 99.21% during the 50th epoch, there is 0.006 percent gaps between training accuracy and validation accuracy. The start point of training and validation loss curves are shown in Fig. 20 as 0.20 and

0.10 respectively. The validation loss value goes down then experience nearly straight decrease and training loss value also decrease.

(a) (b)

Fig. 16. Accuracy versus Loss with their corresponding epochs for binary classification using BiLSTM.

According to Fig. 16 (a) and (b) shows which the train and validation progress of the suggested GRU model, the training accuracy value line begins nearly 91% while the validation accuracy value begins at nearly 96%. The validation accuracy value rapidly increases until the 50th epoch, surpassing the values of the training accuracy line as it began to climb with decreases and increase until the final epoch.When we sum up these above analyses according to the following, DNN and GRU training accuracy is above and its validation loss is below all other models respectively.



(a) (b)

Fig. 17. Accuracy versus Loss with their corresponding epochs for binary classification using GRU.

According to Fig. 17 (a) and (b) which shows the train and validation progress of the suggested GRU model, the training accuracy value line begins nearly 85% while the validation accuracy value begins at nearly 90%. The validation accuracy value rapidly increases then when reaches above 99.38% it decreases until some epochs and again increases and finally increased but below training accuracy until the final epoch.

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 BiLSTM could be the best model for both binary and multi classification of network attack. The following Table VI , which shows the test result of each model.

TABLE IV. ACCURACY, RECALL, PRECISION AND F- SCORE FOR BINARY CLASSIFICATION

Models	Accuracy	Recall	Precision	F1-score

DNN	99.07%	99.16%	99.17%	99.03%
CNN	98.91%	98.53%	98.53%	98.87%
LSTM	98.94%	99%	98.95	98.89
BiLSTM	99.15%	99.07%	99.07	99.12
GRU	99.08%	99.17%	99.18	99.04

As the Table IV it could be seen in terms of test accuracy from all models we used for our study, in case of binary classification BiLSTM is the best performed model Which Scored 99.15%, 99.07%, 99.07%, 99.12%, Precision, Accuracy, Recall and F1-Score Respectively.

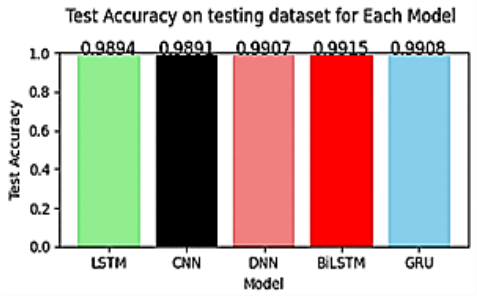


Fig. 18. Test accuracy for binary classification.

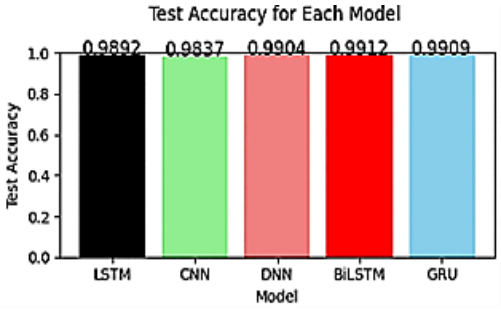


Fig. 19. Test accuracy for multi classification.

As the Fig. 18 also shows, BiLSTM 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%.

TABLE V. TEST ACCURACY FOR BOTH BINARY AND MULTI-CLASSIFICATION

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

As the Table V above shows BiLSTM model scored best accuracy for both binary and multi classification which is 99.15% and 99.12% respectively. Therefore, this shows that BiLSTM 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, BiLSTM outperformed other models.

CONCLUSION

A network assault happens when an individual obtains an unauthorized access to a network is known as a network attack. This includes any attempt to shut down or interfere with the network, which might have catastrophic results. Most businesses rely on well-established network infrastructure security solutions, such as antivirus software, firewalls, and encryption. These tactics do, however, provide some protection against viruses and more complex attacks. Two key ideas in artificial intelligence, machine learning (ML) and deep learning (DL), became well-known during the turn of the century. By teaching computers to think like humans, these approaches' emphasis on data and statistical procedures may significantly increase processing capacity. Computer scientists began using intelligent network security solutions to solve the shortcomings of non-intelligent systems. many deep learning and machine learning techniques.

These methodologies' focus on data and statistical processes may greatly boost computing power by educating computers to think like people. In order to address the drawbacks of non-intelligent systems, computer

scientists started employing intelligent network security solutions. This article thoroughly examines a number of deep learning and machine learning methods for attack detection and classification.

Declarations : **Ethical Approval**: Not applicable , **Competing interests**: No conflicts of interest,
Availability of data and materials: Online datasets can be downloaded from the NSL-KDD Web.
Funding Information: The authors have not received any financial support

REFERENCES

[1] Abbas, S., Bouazzi, I., Ojo, S., Al Hejaili, A., Sampedro, G. A., Almadhor, A., & Gregus, M. (2024). Evaluating deep learning variants for cyber-attacks detection and multi-class classification in IoT networks. *PeerJ Computer Science*, *10*, 1–23. https://doi.org/10.7717/peerj-cs.1793

[2] Aftergood, S. (2017). The Cold War Online. *Nature*, *547*, 30–31. https://www.nature.com/articles/547030a

[3] Ahmad, I., Imran, M., Qayyum, A., Ramzan, M. S., & Alassafi, M. O. (2023). An Optimized Hybrid Deep Intrusion Detection Model (HD-IDM) for Enhancing Network Security. *Mathematics*, *11*(21). https://doi.org/10.3390/math11214501

[4] Al-shehari, T., & Alsowail, R. A. (2021). An insider data leakage detection using one-hot encoding, synthetic minority oversampling and machine learning techniques. *Entropy*, *23*(10). https://doi.org/10.3390/e23101258

[5] Alzubaidi, L., Zhang, J., Humaidi, A. J., Al-Dujaili, A., Duan, Y., Al-Shamma, O., Santamaría, J., Fadhel, M. A., Al-Amidie, M., & Farhan, L. (2021). Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. In *Journal of Big Data* (Vol. 8, Issue 1). Springer International Publishing. https://doi.org/10.1186/s40537-021-00444-8

[6] Anwer, M., Umer, M., Khan, S. M., & Waseemullah. (2021). Attack Detection in IoT using Machine Learning. *Engineering, Technology and Applied Science Research*, *11*(3), 7273–7278. https://doi.org/10.48084/etasr.4202

[7] Bai, Y. (2022). RELU-Function and Derived Function Review. *SHS Web of Conferences*, *144*, 02006. https://doi.org/10.1051/shsconf/202214402006

[8] Boehmke, B., & Greenwell, B. (2019). Hands-On Machine Learning with SKLerni, Keras and TensorFlow. In *Hands-On Machine Learning with R*.

[9] Bonaparte, Y. (2024). Global Financial Stability Index. In *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2753667

[10] Butun, I., Morgera, S. D., & Sankar, R. (2014). A survey of intrusion detection systems in wireless sensor networks. *IEEE Communications Surveys and Tutorials*, *16*(1), 266–282. https://doi.org/10.1109/SURV.2013.050113.00191

[11] Chalapathy, R., & Chawla, S. (2019). *Deep Learning for Anomaly Detection: A Survey*. 1–50. http://arxiv.org/abs/1901.03407

[12] Chatterjee, A., & Ahmed, B. S. (2022). IoT anomaly detection methods and applications: A survey. *Internet of Things (Netherlands)*, *19*(October 2021), 100568. https://doi.org/10.1016/j.iot.2022.100568

[13] Churcher, A, Ullah, R, Ahmad, J, Ur Rehman, S, Masood, F, Gogate, M, Alqahtani, F, Nour, B & Buchanan, WJ 2021,An experimental analysis of attack classification using machine learning in IoT networks', Sensors, vol. 21, no. 2, p. 446.

[14] Das, H. P., & Spanos, C. J. (2022). Improved dequantization and normalization methods for tabular data pre-processing in smart buildings. *BuildSys 2022 - Proceedings of the 2022 9th ACM International Conference on Systems for Energy-Efficient Buildings, Cities, and Transportation*, 168–177. https://doi.org/10.1145/3563357.3564072

[15] De Lucia, M., Maxwell, P. E., Bastian, N. D., Swami, A., Jalaian, B., & Leslie, N. (2021). *Machine learning raw network traffic detection*. *April*, 24. https://doi.org/10.1117/12.2586114

[16] Hartwig, R. P., & Wilkinson, C. (2014). Cyber Risks : the Growing. *Insurance Information Institute*, *June*, 1–27. https://doi.org/10.1726/IJNRD.17046

[17] G Ajeetha and G Madhu Priya. Machine learning based ddos attack detection. In 2019 Innovations in Power and Advanced Computing Technologies (i-PACT), volume 1, pages 1–5. IEEE, 2019.

[18] Hsu, C. M., Hsieh, H. Y., Prakosa, S. W., Azhari, M. Z., & Leu, J. S. (2019). Using long-short-term memory based convolutional neural networks for network intrusion detection. In *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST* (Vol. 264). Springer International Publishing. https://doi.org/10.1007/978-3-030-06158-6_9

[19] Hutchison, D. (2017). Barocchetto. In *Oxford Art Online*.

https://doi.org/10.1093/gao/9781884446054.article.t006431
[20] Ieracitano, C., Adeel, A., Morabito, F. C., & Hussain, A. (2020). A novel statistical analysis and autoencoder driven intelligent intrusion detection approach. *Neurocomputing*, *387*, 51–62. https://doi.org/10.1016/j.neucom.2019.11.016
[21] Iung, B. (2013). Cœur et grossesse. *EMC - Traité de Médecine AKOS*, *8*(2), 1–4. https://doi.org/10.1016/s1634-6939(13)59289-1
[22] Judith, A., Kathrine, G. J. W., Silas, S., & J, A. (2023). Efficient Deep Learning-Based Cyber-Attack Detection for Internet of Medical Things Devices †. *Engineering Proceedings*, *59*(1). https://doi.org/10.3390/engproc2023059139
[23] Kamyab, M., Liu, G., & Adjeisah, M. (2021). Attention-Based CNN and Bi-LSTM Model Based on TF-IDF and GloVe Word Embedding for Sentiment Analysis. *Applied Sciences (Switzerland)*, *11*(23). https://doi.org/10.3390/app112311255
[24] Kim, A, Park, M & Lee, DH 2020, AI-IDS: Application of deep learning to real-time web intrusion detection', In IEEE Access, vol. 8, pp. 70245-70261.
[25] Konatham, B. R. (2023). *a Secure and Efficient Iiot Anomaly Detection Approach Using a Hybrid Deep Learning Technique*.
[26] Kumar, R. (2023). *An Overview of Computer Networking As an Introduction OF*. *July*.'
[27] Lee, A., Wang, X., Nguyen, H., & Ra, I. (2018). A hybrid software defined networking architecture for next-generation IoTs. *KSII Transactions on Internet and Information Systems*, *12*(2), 932–945. https://doi.org/10.3837/tiis.2018.02.024
[28] Liu, H. (2018). *Feature Engineering for Machine Learning and Data Analytics*. https://doi.org/10.1201/9781315181080
[29] Liu, H., & Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. *Applied Sciences (Switzerland)*, *9*(20). https://doi.org/10.3390/app9204396
[30] Marion Olubunmi Adebiyi, Micheal Olaolu Arowolo, Goodnews Ime Archibong, Moses Damilola Mshelia, and Ayodele Ariyo Adebiyi. An sql injection detection model using chi-square with classification techniques. In 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET), pages 1–8. IEEE, 2021
[31] Mayank Agarwal, Dileep Pasumarthi, Santosh Biswas, and Sukumar Nandi. Machine learning approach for detection of flooding dos attacks in 802.11 networks and attacker localization. International Journal of Machine Learning and Cybernetics, 7:1035–1051, 2016.
[32] Mehmood, F., Ahmad, S., & Whangbo, T. K. (2023). An Efficient Optimization Technique for Training Deep Neural Networks. *Mathematics*, *11*(6). https://doi.org/10.3390/math11061360
[33] Mousa Al-Akhras, Mohammed Alawairdhi, Ali Alkoudari, and Samer Atawneh. Using machine learning to build a classification model for iot networks to detect attack signatures. Int. J. Comput. Netw. Commun.(IJCNC), 12:99–116, 2020.
[34] Md Abdullah Al Ahasan, Mengjun Hu, and Nashid Shahriar. Ofmcdm/irf: A phishing website detection model based on optimized fuzzy multi-criteria decision-making and improved random forest. In 2023 Silicon Valley Cybersecurity Conference (SVCC), pages 1–8. IEEE, 2023.
[35] Ni, M. (2023). A review on machine learning methods for intrusion detection system. *Applied and Computational Engineering*, *27*(1), 57–64. https://doi.org/10.54254/2755-2721/27/20230148
[36] Pang, G., Shen, C., Cao, L., & Hengel, A. Van Den. (2021). Deep Learning for Anomaly Detection: A Review. *ACM Computing Surveys*, *54*(2), 1–36. https://doi.org/10.1145/3439950
[37] Pattawaro, A., & Polprasert, C. (2018). *Anomaly-Based Network Intrusion Detection System through Feature Selection and Hybrid Machine Learning Technique*. https://doi.org/10.1109/ICTKE.2018.8612331
[38] Ramaswamy, S. L., & Chinnappan, J. (2022). RecogNet-LSTM+CNN: a hybrid network with attention mechanism for aspect categorization and sentiment classification. *Journal of Intelligent Information Systems*, *58*(2), 379–404. https://doi.org/10.1007/s10844-021-00692-3
[39] Sarumi, OA, Adetunmbi, AO & Adetoye, FA 2020, Discovering computer networks intrusion using data analytics and machine intelligence', Scientific African, vol. 9.

[40] Salih, A. A., Ameen, S. Y., Zeebaree, S. R. M., Sadeeq, M. A. M., Kak, S. F., Omar, N., Ibrahim, I. M., Yasin, H. M., Rashid, Z. N., & Ageed, Z. S. (2021). Deep Learning Approaches for Intrusion Detection. *Asian Journal of Research in Computer Science*, *June*, 50–64. https://doi.org/10.9734/ajrcos/2021/v9i430229