VFAST Transactions on Software Engineering
https://vfast.org/journals/index.php/VTSE@ 2024, ISSN(e): 2309-3978, ISSN(p): 2411-6246
Volume 12, Number 2, April-June 2024 *pp:95-113*

Intrusion Detection Using Machine Learning and Deep Learning Models on Cyber Security Attacks

Irfanullah Khan [1], **Junaid Khan** [1], **Shah Hussain Bangash** [1], **Waqas Ahmad** [1*], **Muhammad Asad Iftikhar** [2], **Khalid Hameed** [2]

[1]Department of Computer Science Iqra National University Peshawar,Pakistan; [2]CECOS University of IT and Emerging Sciences

Keywords: *Machine Learning Algorithms, Deep Learning Algorithms, Network Intrusion Detection, Cyber Security Attacks, Countermeasures Cyber Attacks.*

Journal Info:
Submitted:
April 20, 2024
Accepted:
May 25, 2024
Published:
June 24, 2024

Abstract

To detect and stop harmful activity in computer networks, network intrusion detection is an essential part of cybersecurity defensive systems. It is becoming more difficult for traditional rule-based techniques to identify new attack vectors in the face of the increasing complexity and diversity of cyber threats. Machine learning (ML) and deep learning (DL) models can analyze vast amounts of network traffic data and automatically identify patterns and anomalies, there has been a surge in interest in using these models for network intrusion detection. This paper examines the approaches, algorithms, and real-world applications of machine learning and deep learning techniques for network intrusion detection in order to present a thorough review of the state-of-the-art in countering cyber threats. We assess ML and DL-based intrusion detection systems' effectiveness, strengths, and weaknesses in a range of attack scenarios and network environments by synthesizing current literature and empirical research. Additionally, we talk about new developments, obstacles, and paths forward in the areas of transfer learning, adversarial robustness, and ensemble learning. The understanding gained from this investigation clarifies the potential of ML and DL models in strengthening defenses against changing cyber threats, reducing risks, and protecting vital assets. In deep learning autoencode accuracy 68% less than other models. The performance of the CNN and LSTM algorithm is impressive and outperformed with 100% accuracy on cyber security attacks datasets. Machine learning algorithm accuracy rate of SVM and KNN 100% while logistic regression accuracy is 99% GNB accuracy 80% with training data of the models. The overall models perforamance deep learning increadible accuracy with 100% on the training and testing data.

***Correspondence author email address:** Waqas.ahmad@inu.edu.pk,onlinesoftteach@gmail.com

DOI: 10.21015/vtse.v12i2.1817

1 Introduction

Network attacks pose cybersecurity risks, necessitating intrusion detection systems. Advanced methods like machine learning and deep learning are being explored to address the limitations of traditional rule-based approaches in handling dynamic cyber threats [1].

Machine learning and deep learning models improve intrusion detection by learning patterns from network traffic data, detecting sophisticated attack vectors and constantly adapting to new threats, making them valuable cybersecurity tools [2]. This study reviews network intrusion detection using machine learning and deep learning models, discussing their merits, limitations, and practical consequences, discussing practical difficulties, and offering solutions [3].

However, the machine and deep learning technologies critically examine the effectiveness of ML and DL-based NIDS in various attack scenarios and network topologies, discussing new trends for enhanced intrusion detection systems [4]. The significance of machine learning and deep learning in enhancing network security defences against cyber threats, thereby enhancing resilience, reducing risks, and protecting vital assets [5]. The latest technologies explore deep learning techniques for cyber security intrusion detection, analyzing popular datasets and examining seven deep learning models: deep autoencoders, constrained Boltzmann machines, convolutional neural networks, deep belief networks, deep neural networks, and internet-connected device-based. Additionally, cyberattacks are increasingly targeting Critical National Infrastructures (CNIs), primarily relying on Industrial Control Systems (ICS). Protection of ICSs and CNIs is crucial at national, international, and organizational levels. Europe has implemented laws to secure networks, information, and electronic communications [6]. Intrusion detection systems (IDS) are a crucial second line of protection against cyberattacks, used in conjunction with access control, authentication, and encryption techniques. They differentiate between malicious and benign activity using rules. Data mining aids in implementing IDSs with greater accuracy and robust behavior [7]. The compares deep discriminative intrusion detection methods using deep learning strategies, using new datasets and performance indicators like false alarm rate, accuracy, and detection rate [8]. In the digital age, the internet is crucial for communication and system engineering, making security sensitive due to sensitive data. Network detection aids in system security screening, while intrusion detection aims to launch attacks. Advancements in intrusion detection (ID) have made it the second line of defense after firewalls . Network intrusion detection systems monitor network traffic to identify suspicious activity.

They are widely used for system security, with two types: crowd-based and net-based. Host-based systems use system histories and information to filter equipment and record archives. Intrusion detection investigators have considered machine learning techniques for database searching, suggesting supervised and unsupervised learning. Despite numerous studies, challenges persist in identifying disruptions in system arrival circulation, leading to uneven detection rates and high false positives. The data set includes training data and jobless input attributes [9].

2 STATE-OF-THE-ART

Parasuraman Kumar et.al, proposed study examines the use of DEEP learning neural networks for intrusion detection in cyberattacks. As the internet becomes a crucial communication tool, security becomes a sensitive issue due to sensitive data. Network detection aids in system security screening, with intrusion detection becoming the second line of defense behind firewalls [10]. Zeeshan Ahmad et.al, studied explores deep learning and machine learning techniques for network intrusion detection systems. With the rapid growth of networks and data, new attacks and hackers pose challenges to network security. Intrusion detection systems (IDS) protect networks by analyzing traffic, but researchers struggle to improve detection accuracy and reduce false alarm rates [11]. Niraj Thapa et.al, worked on intrusion detection system (IDS) utilizing deep learning and machine learning models, aiming to improve cybersecurity by achiev-

ing low false alarm rates and high detection rates . Bambang Susilo et.al, researched on deep Learning Algorithm for Intrusion Detection in Internet of Things Networks addresses security challenges in IoT devices. While existing techniques have addressed these issues, there's still room for improvement, and machine learning is a suggested strategy to enhance IoT security [12]. Hamed Alqahtani et.al, focused on increasing complexity of cyber-security due to increased computer connectivity and applications necessitates robust defense against cyberattacks. Machine learning classification techniques have been used to create data-driven intrusion detection systems, potentially contributing to cybersecurity [13]. Devrim Akgun et. A deep learning-based cybersecurity intrusion detection model for DDoS attacks has been developed, utilizing machine learning techniques. The model uses models from LSTM, CNN, and DNN, and is tested on the widely used CIC-DDoS2019 dataset. Preprocessing methods like feature extraction are employed for efficient detection [14]. Saba et.al, reviewed Internet of Things (IoT) aims to improve lives by offering intelligent devices and applications, but security risks remain a major concern. Deep learning model-based anomaly-based intrusion detection systems can improve IoT security by identifying patterns and facilitating smooth detection based on anomalies [15]. Dhanya K. A.a et.al, UNSW-NB15 dataset reveals that Decision Tree classifier outperforms other ensemble models in detecting network attacks, with KNearest Neighbour classifier showing the best results . Srikanthyadav Moraboena et.al deep learning approach for network intrusion detection using a Symmetric Deep Autoencoder (SDAE) for unattended function instruction. It also presents a deep research categorization model using stacked SDAEs, based on classification of Network Security Laboratory's Knowledge Discovery in Databases and Canadian Institute for Cybersecurity's Intrusion Detection System data sets. Zhendong Wang et.al, research develops an integrated deep intrusion detection model based on SDAE-ELM to improve network security by reducing training time and classification accuracy. The model also enhances host intrusion detection accuracy by utilizing DBN-Softmax, a deep neural network used in natural language processing and image identification [16].

2.0.1 Intrusion Detection System (IDS) Challenges in Cyber Security

Challenge 1 Scalability: Due to scalability concerns, deploying IDS across large and complex networks can be difficult. Careful design and resource allocation are necessary to provide consistent coverage and detection efficacy across all network segments and devices[17].

Challenge 2 Adaptability to Changing Threats: As a result of the ongoing evolution of cyber threats, intrusion detection systems must update and modify their detection techniques. This necessitates quick updates to IDS rules and signatures as well as ongoing monitoring of newly developing threats[18].

Challenge 3: Network environments are complex because they are dynamic and heterogeneous, with a wide range of devices, protocols, and settings. IDS needs to be able to function well in a variety of network contexts without producing false alarms or interruptions[19].

Challenge 4: Resource Restrictions: The implementation of IDS necessitates substantial resources, including hardware, software, and human knowledge. It may be difficult for organizations to allocate enough resources.[20]

Challenge 5: Anomaly Detection: Anomaly-based intrusion detection systems (IDS) can effectively discover unknown threats by detecting deviations from typical activity. Nevertheless, they frequently have trouble telling the difference between malicious activity and acceptable deviations, which might result in missed detections or false alarms[21].

Challenge 6 High Data Volume: Due to the enormous volumes of data generated by modern networks, it is difficult for IDS to efficiently monitor and handle all network traffic in real-time. Because of resource limitations, this may lead to missed events or delays in detection[22].

Challenge 7 Encrypted communication: Because encryption is so widely used, especially Transport

Table 2.1 Previous Study Literature Review

Authors	Datasets	Technologies	Drawbacks / Limitations	Data	Methods	Accuracy	Attacks
Mamatha Maddu et.al [20] 2023	InSDN datasets	ResNet152V2, Intrusion Detection	Improve the proposed system by utilizing feature selection and identifying zero-day and low-rate DDoS assaults on IoT systems.	Texture Dataset	Pre-Processing, Augmentation	99.31%	DDos, Spoofing, Dos
Khushnaseeb Roshan et.al [21] 2024	CICIDS-2017 intrusion detection	Machine & Deep Models	To improve to cover important aspects related to NIDS adversarial attacks and its defense mechanism	Texture Dataset	Detection, Augmentation	N/A	black-box white-box adversarial attacks
Bayi Xu et.al [22] 2024	NSL-KDD dataset	BiLSTM, CNN, PSO, Intrusion detection	Further, need to explore model architectures with higher performance and lower resource consumption to enhance the availability of intrusion detection methods.	Texture Dataset	Detection	0.999158	**FGSM JSMA PGD**
Sami Yaras et.al [23] 2023	CICIoT2023' and 'TON IoT	IoT-Based (IDS), Deep Learning	Enhancing them and adding new features will require overcoming obstacles, such as energy constraints and processor limitations.	Texture Dataset	Detection	99.995%	DDos
Vladimir Ciric et.al [24] 2024	CICIDS-2017	Deep Learning, IDS	The lack of real-world testing in the literature is a critical limitation in the realistic perception of AI-driven security solutions.	Texture Dataset	Detection	N/A	Zero-day attacks
Yanfang Fu et.al [25] 2022	NSL-KDD	Deep Learning, IDS	In the future, we plan to apply the DLNID model to an actual, combined network capture module to implement an online intrusion detection model.	Texture Dataset	Detection	90.73%	Viruses, malicious
Yakub Kayode Saheed et.al [26] 2022	UNSW-NB15 dataset	Machine Learning, IDS	IoT is the privacy and security issue resulting from the energy limitations and scalability of IoT devices.	Texture Dataset	Detection	99.99%.	Malicious Attacks

Layer Security (TLS), intrusion detection systems (IDS) have a hard time looking through encrypted communication to look for dangerous content. Attackers may use encryption to conceal their actions from being discovered.

2.1 Discuss the Cyber Security Attacks

Cybersecurity attacks represent serious risks to enterprises, including ransomware, phishing, malware, DDoS, SQL injection, and insider threats. Input validation and web application firewalls are implemented, employees are trained to recognize phishing emails, antivirus software is updated frequently, DDoS mitigation services are deployed, regular data backups are made to reduce the risk of ransomware, and strong access controls are put in place to reduce insider threats[23]. To further protect against any breaches, companies should apply data loss prevention techniques and regularly train staff members on security awareness. By using these countermeasures, companies can strengthen their entire security posture and cyber attack resistance[24].

3 Research Methodology

The design, implementation, and evaluation of efficient intrusion detection systems (IDS) follow a methodical process in the research methodology for network intrusion detection utilizing machine learning (ML) and deep learning (DL) models on cyber security attacks[25]. ML and DL models are chosen based on performance, scalability, and interpretability.The efficacy of the trained models in identifying cyber security threats is assessed by applying the proper validation methodologies. In order to evaluate the efficacy of various models, comparative analysis is performed, taking into account measures like accuracy, precision, recall, and F1-score. In [26]The findings are analyzed in light of the goals of the study and the body of current literature, offering perceptions into the advantages and disadvantages of ML/DL-based intrusion detection systems. Ultimately, recommendations and conclusions are provided for further study and real-world use of network intrusion detection systems[27]. Figure 1 represents the problem that is first specified, along with the kinds of cyberattacks that need to be found and the performance indicators that will be employed in the assessment process[28].

Table 2: Various Attacks Counter-Measurements

Cyber Security Attack	Counter-Measures
Phishing	✓ Training for staff members to recognize phishing emails ✓ Putting email filters into place to identify and stop phishing emails ✓ For accounts that are sensitive, two-factor authentication
Malware	✓ Upgrading anti-malware and antivirus software on a regular basis ✓ Putting endpoint security solutions into practice ✓ Executing routine system updates and virus scans
DDoS (Distributed Denial of Service)	✓ Implementing services for DDoS mitigation ✓ Putting in place traffic filtering and rate-limiting regulations, ✓ Content Delivery networks (CDNs) to absorb traffic
SQL Injection	✓ Web applications: parameterized queries and input validation ✓ Putting web application firewalls (WAF) into practice ✓ Patching and updating web applications on a regular basis
Ransomware	✓ Frequently creating backups of important data and systems ✓ Putting in place strict access restrictions and least privilege ✓ Educating staff members about safe email and internet usage

A thorough assessment of the literature is done to find previous studies, datasets, and methods, which serve as the study's foundation. Data is obtained and preprocessed for model training, with feature selection and engineering techniques used to improve intrusion detection[29].

3.1 The reality mining dataset

The Reality Mining scheme corresponds to the biggest cellular mobile trial yet tried in the academic world. An unparalleled quantity of information on individual performance is gathered and cluster communications that we arrange on any missing and building accessible to the universal educational community[30]. At the end of the trial, this dataset will include more than fifty thousand hours roughly sixty years of uninterrupted information on everyday individual performance[31]. In an editorial on the Reality Mining project in December's matter of New Scientist, famous communal system forecaster and Harvard professor David Laser was referenced saying that this investigation will transform the field of communal system investigation[32].

3.2 Datasets IDS

Datasets are crucial for training and assessing intrusion detection systems, providing network traffic data from various sources. The quality and variety of these datasets significantly impact the system's effectiveness. Common datasets include malware infections, DoS, DDoS, and SQL injections[33]. Researchers preprocess these datasets to manage missing values, normalize features, and balance class distributions. Labeled samples of a variety of cyberattacks, including malware infections, Denial of Service (DoS), Distributed Denial of Service (DDoS), SQL injection, and more, are commonly included in datasets for intrusion detection[34]. NSL-KDD, UNSW-NB15, and CICIDS2017 are a few frequently utilized datasets that offer a variety of attack scenarios and network traffic characteristics.

3.3 Research Challenges During this Research

A number of difficulties could come up while studying how well deep learning and machine learning algorithms work in cyber security. Lack of a systematic dataset: This study brought to light the lack of a current dataset reflecting new attacks on contempo-

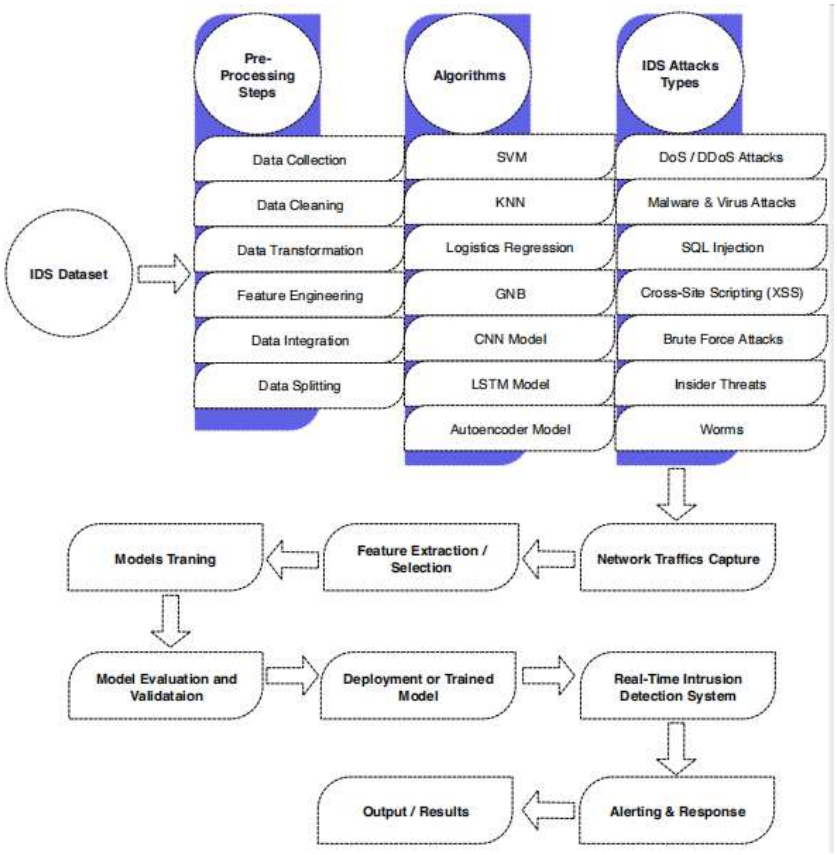

Figure 1. Block Diagram of Intrusion Detection System Counter remeasurements Cyber Security Attacks

rary networks[35]. Because these models were not trained with enough attack kinds and patterns, the majority of the offered approaches were unable to detect zero-day attacks[36]. An effective IDS model must be tested and validated on a dataset containing both older and more recent attacks. The inclusion of the maximum number of attacks specification in a dataset will help the machine learning (ML/DL) model identify more patterns, which will ultimately lead to protection against various sorts of maximum invasions[37]. 3.2.2 Reduced detection accuracy as a result of an unbalanced dataset: The current analysis also reveals that, for some attack types, the majority of the suggested IDS approaches show poorer detection accuracy than the model's overall detection accuracy[38]. The dataset's imbalance is the root cause of this issue. Compared to attacks with more instances, the detection accuracy of attacks in the low frequent attacks class is lower[39]. 3.2.3 Resources consumed by complex models: Nearly 80% of the researcher's suggested IDS approaches are based on extremely complex models that demand a great deal of processing and computational effort. This could lead to additional processing unit overhead, which would ultimately impair IDS performance[40].

4 EXPERIMENTS

To efficiently identify and address cybersecurity threats, intrusion detection systems (IDS) make use of a range of machine learning and deep learning methods. Because machine learning techniques, including Random Forests and Support Vector Machines (SVMs), can identify malicious or benign network traffic based on attributes taken from packet headers or payload data, they are frequently utilized in machine learning applications. Strong and capable of managing high-dimensional data, Random Forests outperform SVMs in defining intricate decision boundaries. Convolu-

tional neural networks (CNNs) and recurrent neural networks (RNNs), two deep learning architectures, have demonstrated potential in improving intrusion detection system (IDS) capabilities. These algorithms enable IDS to automatically learn from and analyze enormous volumes of network data, enabling it to respond to changing cybersecurity threats.

4.0.1 Machine Learning Algorithms

Intrusion Detection Systems (IDS) employ diverse machine learning methods to efficiently identify and counteract cybersecurity attacks. The Random Forest classifier is a frequently used technique that is renowned for its resilience and capacity to handle high-dimensional data. Because Random Forests build many decision trees and aggregate their predictions, they are highly effective at identifying anomalies and categorizing network traffic. Another well-liked IDS tool is Support Vector Machines (SVMs), which have a high degree of accuracy when separating malicious from legitimate network traffic. SVMs can discriminate between malicious and benign network behavior because they can draw complex decision boundaries in high-dimensional domains. The text discusses the trends in the quantity

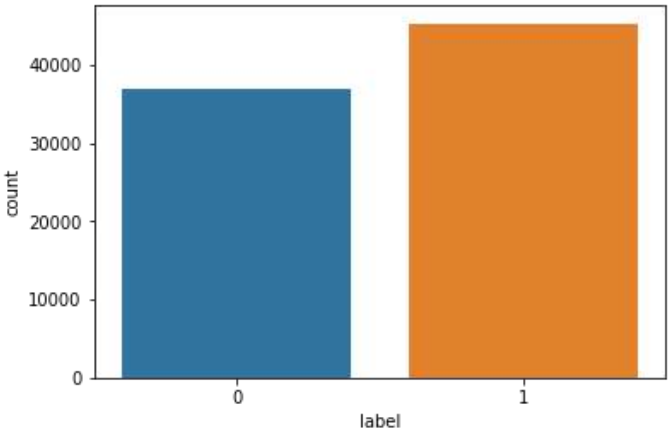

Figure 2. The label represents fake and real news dataset data

of labels and potential causes of these trends figure 4.1. It also discusses the units of labels, such as the number of labels on the y-axis and the time scale on the x-axis. It also mentions the existence of additional details. The label 0 indicates nomal fake news while 1 represents the real news detection.

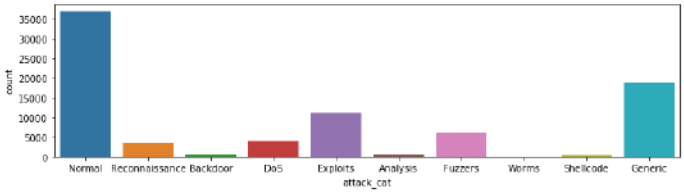

Figure 3. Data Distributed Categorical Plots

4.1 Check Categorial Data Plots of the Dataset

The distribution and correlations among the categorical variables in a dataset can be seen through the use of categorical data charts. They show information on the frequency and distribution of various categories and include bar, count, and box graphs. Exploratory data analysis and feature engineering are aided by these plots, which show patterns, anomalies, and possible relationships within categorical variables. Categorical data distributions can be visually examined by analysts to identify trends, outliers, and problems with data quality. These findings can then be used to inform further data pretreatment and modelling stages for more reliable and accurate analysis. The figure 4.2 represents bar graph with the heading "Attack Categories by Analysis Method" is attached to the file you submitted. The many techniques for analyzing cyberattacks are listed on the x-axis. Normal analysis, reconnaissance, backdoors, exploits, fuzzers, worms, shellcode, DoS (denial-of-service), and generic are some of these techniques. The amount of attacks that, according to the analysis approach, fit into each category is displayed on the y-axis. The "normal analysis" bar, for example, indicates that 35,674,667 attacks were examined by standard procedures. The "reconnaissance" bar indicates that 8,116,642 assaults were found using these techniques.

4.2 Histogram to See the Data Distribution

Data distribution in the picture you submitted, as it is devoid of labels and information about the context

in which it is used. I can, however, describe the general method of visualizing data distribution using histograms. A histogram is a graph that shows how a set of data is distributed. The most frequent value or the middle value in the data set is referred to as the center of the distribution. A histogram's center is usually located at the bin with the tallest bar. The degree of variation among the data points is indicated by the distribution's spread. Figure 4.3 shows that histogram with

Figure 4. Data Distributions Various Plots

a broader spread shows more data points distributed throughout the value range, whereas a histogram with a narrower spread shows more data points clustered at the center. The histogram's form might provide crucial details regarding the data's distribution. A symmetrical histogram, for instance, indicates that the data is dispersed equally around the center. a histogram that is distorted, with lopsided bars The histogram's look can vary depending on how many bins are used. While fewer bins can make it easier to observe the general shape, more bins can offer a more thorough perspective of the distribution. The histogram's appearance may also be impacted by the bin size selection.

4.3 Correletion Matrix

A correlation matrix is an essential analytical tool for finding patterns and links between different network traffic variables or features in the context of Intrusion Detection Systems (IDS) within cybersecurity. The correlation coefficient, which indicates the direction and strength of a linear relationship between two qualities, is represented by each item in the matrix. Analysts can identify characteristics that change together, possibly indicating unusual activity or security risks within the network, by looking at the correlation matrix. In

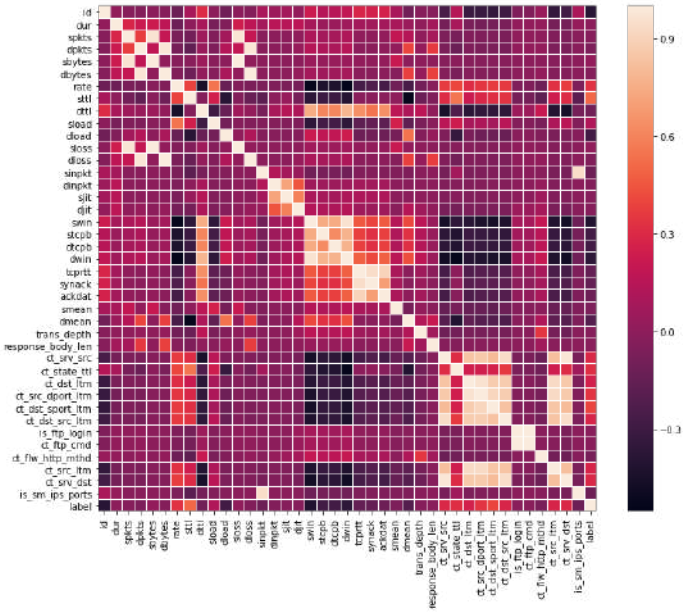

Figure 5. Correletion Matrix of the Dataset IDS

the figure 4.4 represents correlated features, for instance, may indicate coordinated attacks in network traffic analysis, such as a distributed denial-of-service (DDoS) attack coming from several sources. On the other hand, weak or negative correlations may draw attention to a variety of activities or healthy network activity. By focusing on suspicious patterns or events that diverge from typical network activity, security analysts may detect and mitigate cybersecurity risks more effectively thanks to this expertise. Correlation matrices also help with feature selection and dimensionality reduction, which directs the creation

and refinement of machine learning models used in intrusion detection systems. Analysts can increase detection accuracy, simplify the model training process, and improve interpretability by detecting features that are strongly linked or redundant. It is imperative to take into account the constraints of correlation analysis, including its incapacity to identify nonlinear correlations.

4.4 Support Vector Machine (SVM)

The Support Vector Machine (SVM) technique is widely recognized for its effectiveness in classification and regression applications. It performs especially well in high-dimensional spaces and when the number of features exceeds the number of samples. With the use of kernel functions that facilitate the efficient handling of nonlinear decision boundaries, support vector machines (SVMs) search for the ideal hyperplane in the feature space that divides various classes. Despite their strength, support vector machines (SVMs) are less appropriate for noisy data because to their processing expenses, particularly when dealing with huge datasets and their tendency to struggle when classes overlap heavily. The curve indicating that the model

	precision	recall	f1-score	support
0	1.00	1.00	1.00	21938
1	1.00	1.00	1.00	14459
micro avg	1.00	1.00	1.00	36397
macro avg	1.00	1.00	1.00	36397
weighted avg	1.00	1.00	1.00	36397

Figure 6. Results of Support Vector Machine (SVM) Performance Evaluation

may be sacrificing some recall in favor of precision. Recall will rise (the model will find more positive cases) when the threshold for identifying a case as positive is dropped, but precision will fall (some of the cases identified as positive will actually be negative). In contrast, recall will fall (the model will miss more positive examples) when the threshold is raised, but precision will increase (the model will identify fewer cases as positive, but the ones it does classify will be more likely to be positive). The model's recall and precision may be impacted by the categorization threshold selection. The trade-off between recall and precision at various thresholds is represented by the curve. The best applications of the precision-recall curve are in two-class classification issues. Alternative methods of visualization might be more suitable for problems involving multiple classes. The figure 4.6 shows

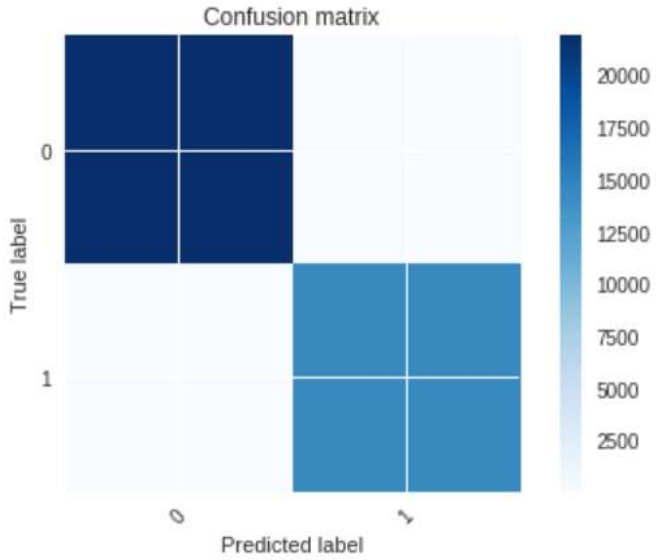

Figure 7. Confusion Matrix Support Vector Machine (SVM) Performance

that classification cccuracy is calculated by dividing the total number of accurate predictions by the total number of predictions made. Greater performance overall is indicated by a higher value. By combining the values on the diagonal of the matrix and dividing the result by the total of all the values in the confusion matrix, you may compute it. It focuses on how well the model can recognize positive cases. By dividing the total number of genuine positives and false positives by the number of true positives, it is computed. This is the ratio of accurately predicted abnormal cases (bottom left cell) to the total number of predicted abnormal instances (bottom row) in the confusion matrix. SVM is a machine learning technique that can be applied to applications involving classification. Finding a hyperplane that divides the data points of one class from another class is how it operates. The percentage of data points that an SVM model properly classifies serves as a gauge for its accuracy.

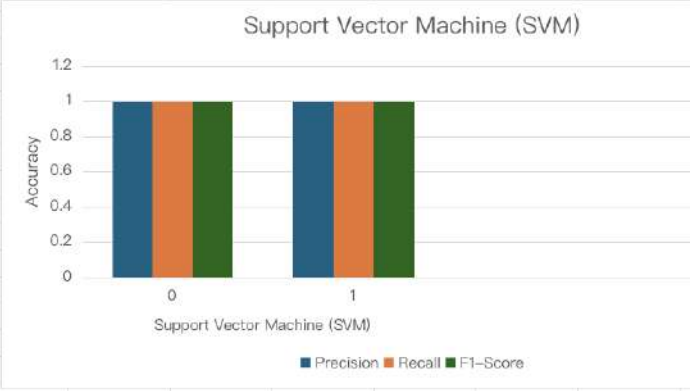

Figure 8. SVM Algorithms Performance Compared Various Cyber Security Attacks

The SVM model's training parameters are represented by the x-axis, most likely. For example, it may display alternative values for the regularization parameter or distinct kernel functions utilized by the SVM. On a scale from 0 to 1, the y-axis shows how accurate the SVM model is. When the model assigns a value of 1, all of the data points are correctly classified.

4.5 KNN Algorithm

KNN algorithm straightforward conceptual structure, K-Nearest Neighbors (KNN) is incredibly useful, particularly when dealing with non-uniform decision limits. KNN is especially useful for pattern identification, anomaly detection, and recommendation systems because it is predicated on the idea that comparable instances typically have similar results. However, it can be limited by its computational requirements during testing, particularly when dealing with large datasets, and its sensitivity to redundant or unnecessary information. The figure 4.8 shows that the percentage of

Classification report:

	precision	recall	f1-score	support
0.0	1.00	1.00	1.00	67343
1.0	1.00	1.00	1.00	67343
accuracy			1.00	134686
macro avg	1.00	1.00	1.00	134686
weighted avg	1.00	1.00	1.00	134686

Figure 9. Results of KNN Algorithm Performance Evaluation

positive forecasts that came true as predicted. When a model has a high precision, it is good at classifying only the relevant cases as positive. The precision for class 0 in the example is 1.00, indicating that all of the data points that were predicted to be class 0 were, in fact, class 0. The percentage of real positive cases that the model successfully detected is represented by this. When a model has a high recall, it is effective in identifying all pertinent cases. The model accurately identified all of the actual class 0 data items in the case, as indicated by the recall of 1.00 for class 0. The confusion matrix appears that the model is doing

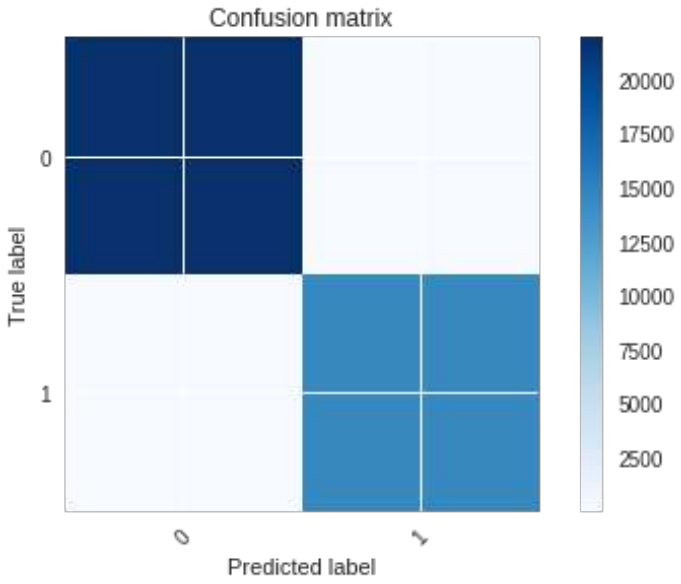

Figure 10. Algorithms Performance Compared Various Cyber Security Attacks

a good job of classifying the data based on the high precision, recall, and F1-score for each class in this case. The quantity of courses: When it comes to multi-class classification challenges involving more than two classes, the study provides further information. The remaining data: The precision, recall, and F1-score for the minority class may be deceptive if the data is unbalanced, meaning that one class has a much higher number of data points than the others. The x-axis, which has the title "Test Number," most likely alludes to the several assessment sets that were used to gauge the effectiveness of the model. Accuracy is the label for the y-axis, which has a range of 0 to 1. The performance improves with a greater value.

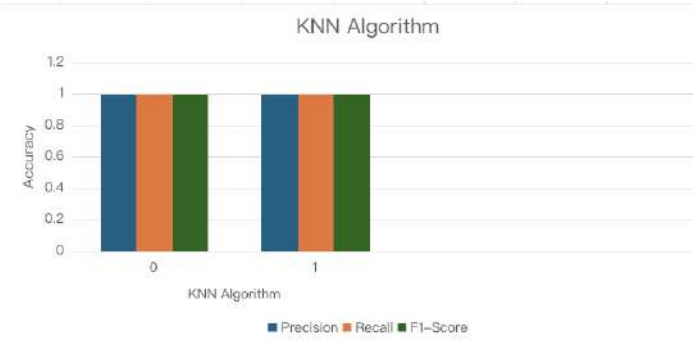

Figure 11. KNNAlgorithms Performance Compared Various Cyber Security Attacks

At about test number 5, this test nearly reaches 1.0, suggesting that it has the highest overall accuracy. It keeps up a high level of accuracy throughout all of the assessments. Compared to Test 1, this test's overall accuracy is lower. Accuracy seems to vary more over the course of the evaluations, rising and falling with varying test numbers.

4.6 Logistic Regression

When there is a linear relationship between the target variables and the characteristics, logistic regression, a mainstay of classification algorithms, performs exceptionally well. It is extremely useful in industries like credit scoring and healthcare analytics since it can provide probability for outcomes. Its simplicity does have a drawback, though, as it is limited to linear decision limits and has trouble handling complex data linkages.

	precision	recall	f1-score	support
0	0.99	0.99	0.99	21938
1	0.99	0.99	0.99	14459
micro avg	0.99	0.99	0.99	36397
macro avg	0.99	0.99	0.99	36397
weighted avg	0.99	0.99	0.99	36397

Figure 12. Results of Logistics Regression Algorithm Performance Evaluation

The figure 4.11 x-axis of the curve represents the recall, which is the proportion of positive cases that were correctly identified by the model; the y-axis represents the precision, which is the proportion of the model's predicted positive cases that were actually positive. An ideal precision-recall curve would be a straight line in the upper left corner of the graph, indicating that the model is able to correctly classify all positive cases (high recall) and all of the cases that the model classified as positive are actually positive (high precision). The model accurately categorizes positive cases in the upper left corner, but trades precision and recall. A good model has a high precision and recall curve. A statistic known as the area under

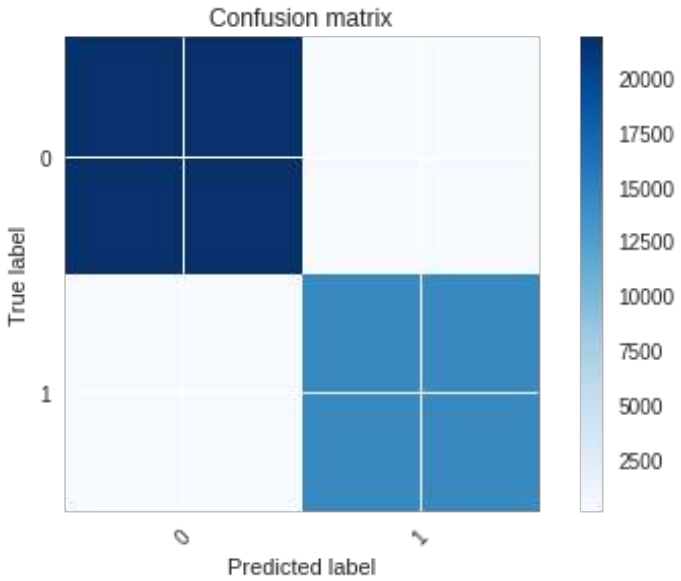

Figure 13. KNN Algorithms Performance Compared Various Cyber Security Attacks

the curve (AUC) can be used to summarise a model's overall performance. A better model is one with a higher AUC. The precision and recall of the model can be impacted by the categorization threshold selection. The precision versus recall trade-off at various levels is represented by the curve. Logistics Regression algorithms represents 0 and 1 based of confusion matrix. The models show thier performance on various types of data of cyber security attacks dataset of intrusion detection. Logistic regression techniques' performance varies depending on the data type and the quality of features. It's most effective in linearly separable data and basic decision boundaries, but may be less effective in high-dimensional data or complex attacks. The training dataset and features also impact its effectiveness.

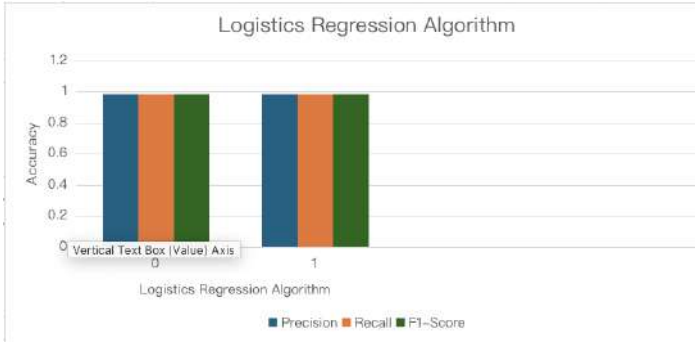

Figure 14. Logistics Regression Algorithms Performance Compared Various Cyber Security Attacks

4.7 GNB Algorithms

Gaussian Naive Bayes (GNB) is a simple and effective algorithm that finds use in classification applications, especially those that involve high-dimensional data. Its efficacy in numerous applications, ranging from text classification to spam filtering, is undeniable, despite the assumption of feature independence, which may not always hold true in real-world data. Gaus-

	precision	recall	f1-score	support
0	0.88	1.00	0.94	21938
1	0.99	0.80	0.89	14459
micro avg	0.92	0.92	0.92	36397
macro avg	0.94	0.90	0.91	36397
weighted avg	0.93	0.92	0.92	36397

Figure 15. GNB Algorithm Performance Evaluation

sian Naive Bayes (GNB) algorithm is a probabilistic classification method based on Bayes' theorem. GNB algorithm performance show the accuracy precision 0.88, recall 1.00 and f1-score 0.89 resprectively. GNB is straightforward, it has shown to be successful in a variety of classification problems, particularly when the feature space is Gaussian distributed and continuous. The probability density function of the Gaussian distribution for each characteristic is used in GNB to determine the likelihood of a sample falling into a given class. GNB's performance on the Confusion Matrix depends on the type of cyber security attack. Its efficiency and simplicity make it suitable for high-dimensional data. However, it can deteriorate with complex features or non-Gaussian distributions.

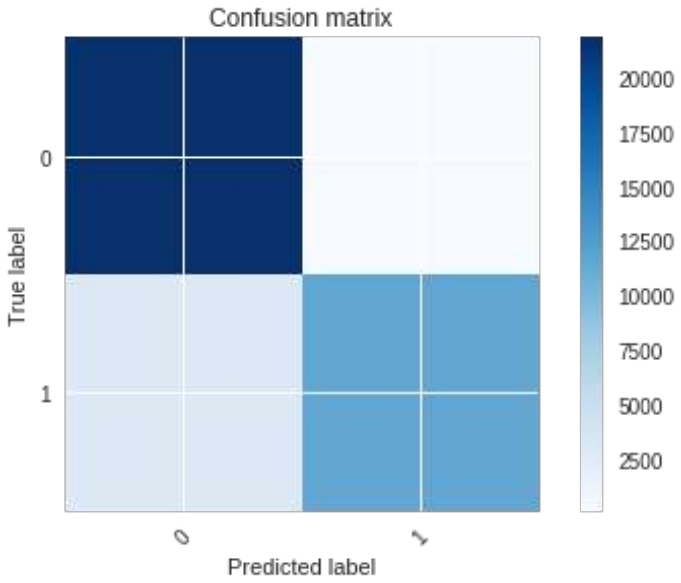

Figure 16. GNB Algorithm Confusion Matrix Performanc

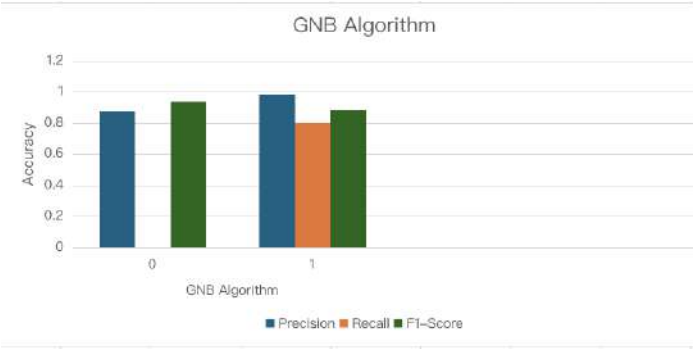

Figure 17. GNB Algorithms Performance Compared Various Cyber Security Attacks

The performance of Gaussian Naive Bayes (GNB) algorithms varies depending on the type of cyberattack. Due to its ease of use and effectiveness, GNB is a good fit for managing high-dimensional data, which is frequently encountered in cyber security applications. But with coupled or non-Gaussian distributed features, its performance may be affected by the assumption that features are independent, which may not always hold true. When attack patterns are discernible and classes are well-separated, GNB typically performs well. However, it might not be able to withstand extremely complex attacks or those with minute variances.

4.8 Deep Learning Algorithms

4.8.1 CNN Model

In the field of deep learning, convolutional neural networks (CNNs) have become a mainstay, especially because of their exceptional performance in image-related tasks. Using a sequence of convolutional layers, CNNs automatically extract hierarchical information from input images and identify patterns and spatial correlations. CNNs are very good at tasks like object detection, picture segmentation, and image classification because of this hierarchical feature extraction process. Together with innovations like transfer learning, their capacity to automatically learn representations from raw data has enabled breakthroughs in a variety of industries, including autonomous driving and healthcare. CNNs are quite powerful, but they need a lot of labeled data to train, and their intricate structures might cause overfitting, which means you have to use cautious regularization strategies and architectural design decisions. Convolutional Neural Network (CNN)

	precision	recall	f1-score	support
0	1.00	1.00	1.00	21938
1	1.00	1.00	1.00	14459
micro avg	1.00	1.00	1.00	36397
macro avg	1.00	1.00	1.00	36397
weighted avg	1.00	1.00	1.00	36397

Figure 18. CNN Model Performance Evaluation

models are evaluated for performance using metrics such as accuracy, precision, recall, and F1-score. CNNs are excellent at tasks like object detection, segmentation, and picture classification because they can automatically learn hierarchical features. Crucial assessment methods encompass confusion matrix analysis, which sheds light on classification errors, and cross-validation, which guarantees generalization across various datasets. Furthermore, methods such as precision-recall curves and ROC curves aid in the selection and fine-tuning of models by visualizing the trade-offs between true positive rate and false positive rate. It is imperative to conduct routine performance monitoring and validation to guarantee that CNN models remain resilient and efficient in a range of application scenarios. The Confusion Matrix of

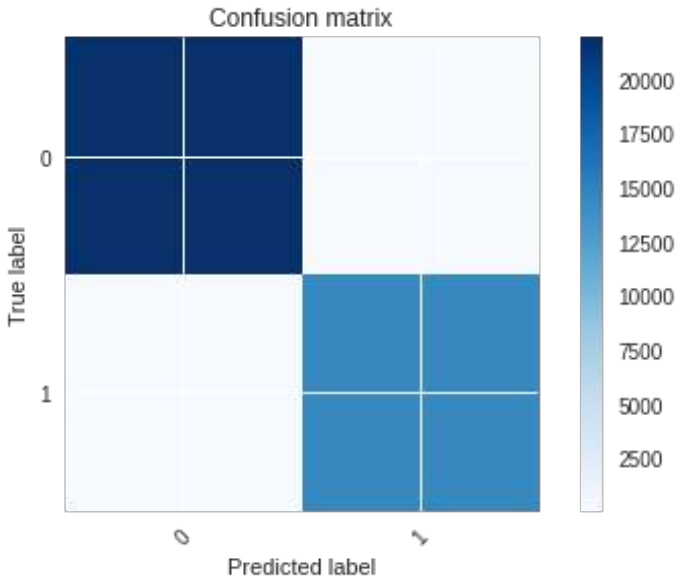

Figure 19. CNN Model Confusion Matrix

Convolutional Neural Network (CNN) models provides a comprehensive evaluation of their classification accuracy and error types, allowing stakeholders to identify areas for improvement, fine-tune model parameters, and enhance their effectiveness in tasks like object detection, semantic segmentation, and picture recognition. The above diagram represents

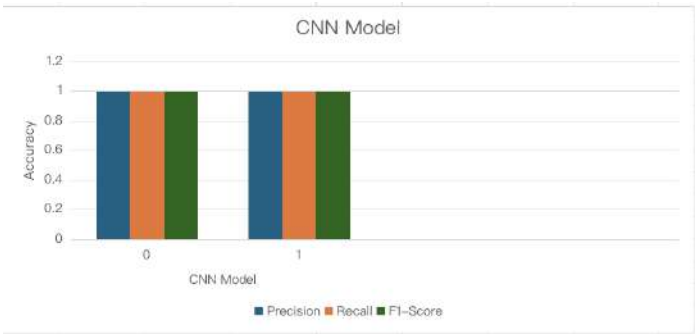

Figure 20. CNN Model Performance Compared Various Cyber Security Attacks

the CNN model performance on confusion matrix. CNNs also show promise in identifying anomalies in network traffic patterns, highlighting peculiar behaviors that could indicate possible attacks such as

denial-of-service (DoS) attacks or attempts at data exfiltration. CNNs are incredibly flexible instruments for cyber security protection measures because of their versatility and capacity to recognize complex patterns.

4.8.2 LSTM Model

Recurrent neural networks (RNNs) have been modified to create Long Short-Term Memory (LSTM) networks, which are meant to capture long-term dependencies in sequential data and solve the vanishing gradient issue that conventional RNNs have. In order to accomplish this, LSTMs integrate memory cells with gating mechanisms, which over time selectively preserve or delete information. They become crucial in tasks like speech recognition, time series forecasting, and natural language processing (NLP) because of their ability to efficiently model temporal dependencies. LSTMs are a key tool in the field of sequential data analysis because of their capacity to handle sequences of different lengths and capture context over long time spans. Long Short-Term Memory (LSTM) models

	precision	recall	f1-score	support
0	1.00	1.00	1.00	21938
1	1.00	1.00	1.00	14459
micro avg	1.00	1.00	1.00	36397
macro avg	1.00	1.00	1.00	36397
weighted avg	1.00	1.00	1.00	36397

Figure 21. LSTM Model Performance Evaluation

are evaluated by measuring their F1-score, accuracy, precision, and recall. Natural language processing, time series prediction, and anomaly detection are just a few of the applications where LSTMs shine. These tasks involve the examination of sequential data. Evaluation methods include confusion matrix analysis to comprehend classification errors and cross-validation to guarantee robustness across various datasets. Furthermore, methods like precision-recall curves and receiver operating characteristic (ROC) curves help to visualize trade-offs between true positive rate and false positive rate, which helps with model selection and optimization. Frequent performance review guarantees that LSTMs continue to be effective and flexible in a variety of cyber security and other applications. Furthermore, methods like precision-

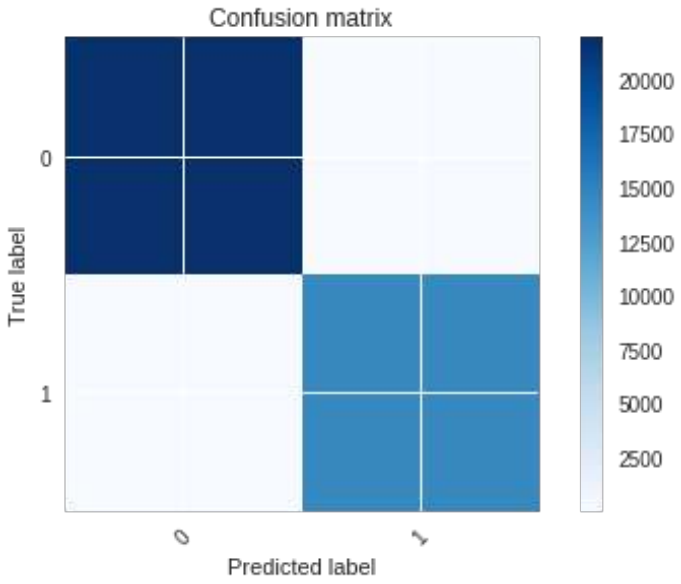

Figure 22. LSTM Model Confusion Matrix

recall curves and receiver operating characteristic (ROC) curves help to visualize trade-offs between true positive rate and false positive rate, which helps with model selection and optimization. Frequent performance review guarantees that LSTMs continue to be effective and flexible in a variety of cyber security and other applications. Long Short-Term Memory

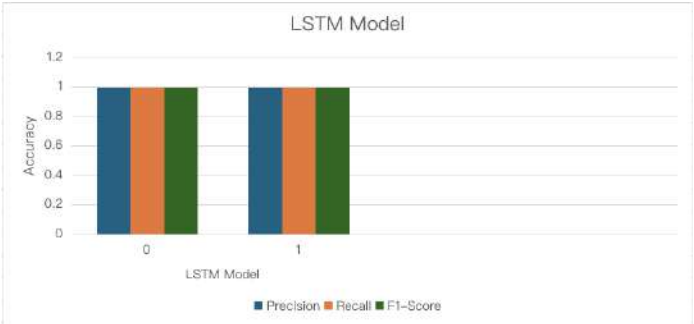

Figure 23. LSTM Model Performance Compared Various Cyber Security Attacks

(LSTM) models effectively identify threats through a comparative diagram comparing their performance across various cyber security attacks. They can identify trends and abnormalities, aiding stakeholders in

making informed decisions about defense strategies and threat mitigation efforts. This visual comparison highlights their strengths and limitations.

4.8.3 Autoencoder Model Performance

Neural networks classified as autoencoders are employed for unsupervised learning tasks, specifically in denoising, data compression, and feature learning. They are made up of a decoder network that uses the latent space representation created by the encoder network to recover the original input, and an encoder network that compresses the input data. Autoencoders enable effective data compression and visualization by facilitating dimensionality reduction and feature extraction through the learning of a compact representation of the input data. Moreover, autoencoders can be trained to rebuild clean samples from noisy inputs, thereby denoising corrupted data. Their adaptability and capacity to derive meaningful representations from unlabeled data make them indispensable in a number of fields, such as recommendation systems, anomaly detection, and image generation. The graph shows the total number

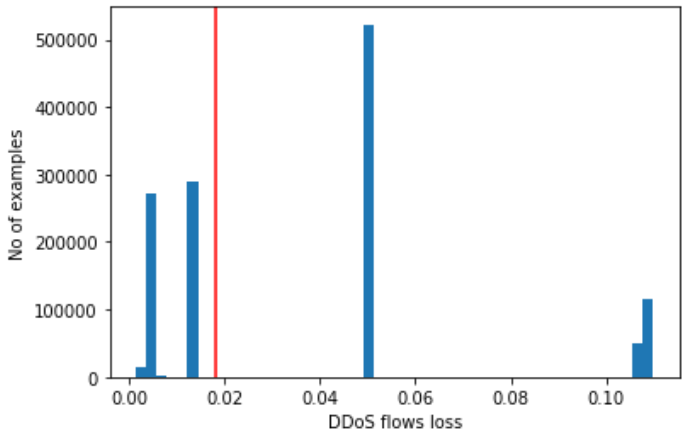

Figure 24. Autoencoder Detect DDoS Flows Loss

of DDoS attacks lost over time, with a sharp rise in DDoS flows at the start and a fall at the end of the time interval. The graph's y-axis displays the quantity of DDoS flows lost, and the x-axis represents time. Although the x-axis scale is unlabeled, it seems to span a little time interval—possibly seconds or milliseconds. The graph displays a sharp rise in the quantity of DDoS flows lost at the start of the time interval, followed by a fall. It's hard to interpret the graph precisely without more details. It's possible, nevertheless, that the graph illustrates how successful a DDoS mitigation system is. The abrupt spike in DDoS flows lost can be a sign that a DDoS attack was detected and stopped by the system. The attack may have ended if the loss of DDoS flows decreased. It looks as though the

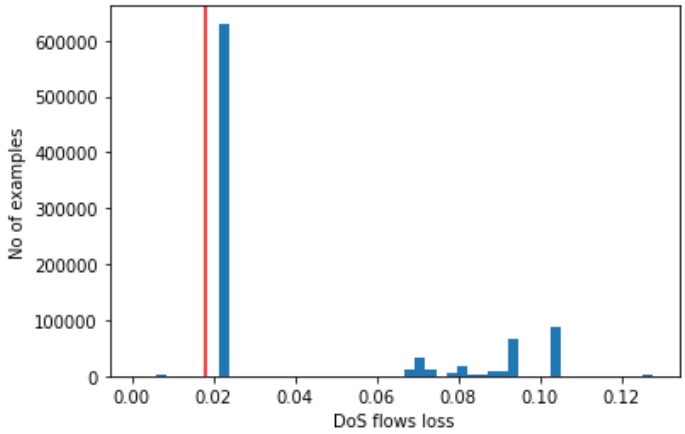

Figure 25. Autoencoder Detect DoS Flows Loss

y-axis extends from 0 to 400,000. With values rising at a progressively faster rate from left to right, the x-axis seems to be non-linear. On the graph, a single line is drawn. From left to right, the line tends upward, but it seems to flatten out near the higher y-axis. The

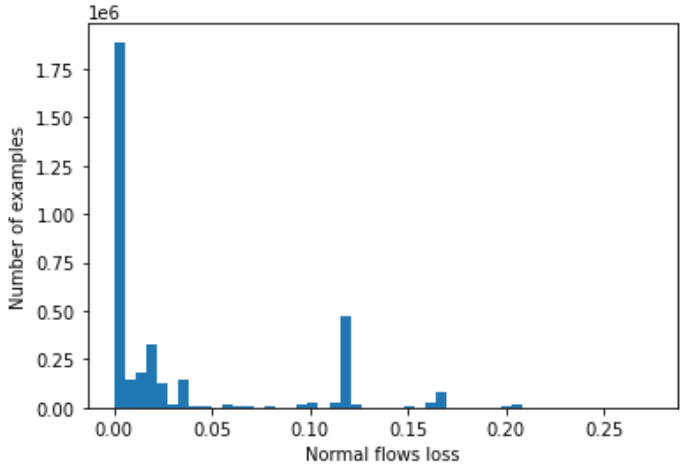

Figure 26. Autoencoder Detect DDoS Flows Loss

graph shows the total number of mistakes made

during training, with a declining trend indicating less mistakes as training progressed. The y-axis represents errors, with labels likely multiples of 100,000. This indicates the model is becoming more proficient and picking up new skills. A confusion matrix is a table

	precision	recall	f1-score	support
0	0.90793	0.68565	0.78129	3567467
1	0.33448	0.69441	0.45149	811664
accuracy			0.68727	4379131
macro avg	0.62121	0.69003	0.61639	4379131
weighted avg	0.80164	0.68727	0.72016	4379131

AUC: 69.0%

Figure 27. Autoencoder Model Performance Evaluation

that displays how well an algorithm performs while classifying various classes. It is applied to statistics and machine learning. The actual classes are represented by the rows in the confusion matrix you submitted, and the anticipated classes are represented by the columns. The number of data points in each category is indicated by the numbers in the table. For instance, the number of data points that were both class 0 in reality and class 0 in the algorithm's prediction is 3,567,467 in the top left cell. The amount of accurate forecasts is displayed on the table's diagonal. In this instance, more class 0 data points (3,567,467) than class 1 data points (811,664) were predicted by the model. The model's performance is further detailed by looking at the metrics at the bottom of the table: accuracy, precision, recall, and F1 score. The indicator of a model's ability to discriminate across classes is called AUC, or Area Under the Curve. Its AUC is 69.0% in this scenario. The confusion matrix is a tool used in autoencoders to assess an error in the reconstruction of initial input data. It represents the degree to which the autoencoder can reconstruct the data, with actual labels in rows and predicted labels in columns. The data points in the table are classified as either abnormal or normal, with 68.6% of them showing effective rebuilding. Reconstructions are categorized using a threshold; however, the precise threshold value is not given. The autoencoder's capacity to reconstruct the original data for every class is evaluated by the confusion matrix. Autoencoder

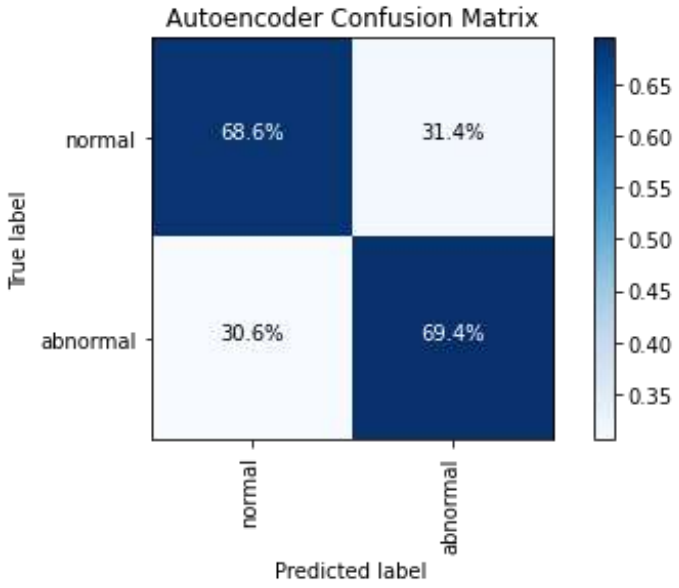

Figure 28. Autoencoder Model Confusion Matrix

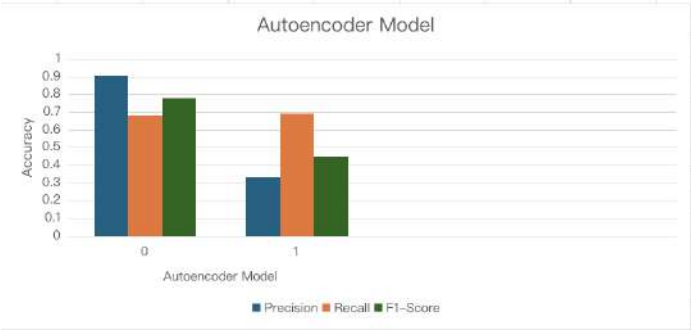

Figure 29. Autoencoder Model Performance Compared Various Cyber Security Attacks

confusion matrices measure reconstruction error, not classification accuracy. Threshold dependence affects interpretation, with lower thresholds indicating more successful reconstructions but potentially introducing noise.

5 Conclusion and Future Direction

Intrusion Detection Systems (IDS) employ an array of machine learning and deep learning techniques to proficiently identify and address cybersecurity threats. Because they can identify malicious or benign network traffic based on attributes taken from packet headers or payload data, machine learning techniques like Random Forests and Support Vector Machines (SVMs)

are commonly utilized. Random Forests are resilient and effective with high-dimensional data, whereas Support Vector Machines are superior at drawing intricate decision borders. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs), two deep learning architectures, have demonstrated potential in improving intrusion detection system (IDS) capabilities. CNNs are useful for tasks like detecting anomalies in network traffic patterns or recognizing virus signatures in packet payloads because they are skilled at extracting spatial information from network traffic data. Because RNNs especially Long Short-Term Memory (LSTM) network are good at capturing temporal dependencies, they can identify minute, time-varying patterns that could be signs of cyberthreats. These algorithms enable IDS to automatically learn from and analyze enormous volumes of network data, enabling it to respond to changing cybersecurity threats. Deep learning models CNN and LSTM accuracy rate is highest as compare to all the algorithms. Machin learning some models poor performance on the testing data of cyber security attacks dataset.

Author Contributions

Irfanullah Khan, Waqas Ahmad,Shah Hussain Bangash: Conceptualization, Methodology, Software **Waqas Ahmad , Junaid Khan, Shah Hussain Bangash**: Data curation, Writing- Original draft preparation. **Irfanullah Khan , Junaid Khan, Khalid Hameed**: Visualization, Investigation. **Irfanullah Khan, Muhammad Asad Iftikhar, Khalid Hameed**: Supervision.: **Waqas Ahmad, Muhammad Asad Iftikhar**: Software, Validation. **Muhammad Asad Iftikhar, Shah Hussain Bangash**: Writing- Reviewing and Editing

Compliance with Ethical Standards

It is declared that all authors don't have any conflict of interest. It is also declared that this article does not contain any studies with human participants or animals performed by any of the authors. Furthermore, informed consent was obtained from all individual participants included in the study.

References

[1] H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: A survey," *Applied Sciences*, p. 4396, 2019.

[2] L. Ashiku and C. Dagli, "Network intrusion detection system using deep learning," *Procedia Computer Science*, pp. 185, 239–247, 2021.

[3] P. Kumar, A. A. Kumar, C. Sahayakingsly, and A. Udayakumar, "Analysis of intrusion detection in cyber attacks using deep learning neural networks," *Peer-to-Peer Networking and Applications*, vol. 14, pp. 2565–2584, 2021.

[4] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Transactions on Emerging Telecommunications Technologies*, vol. 14, p. e4150, 2021.

[5] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *Journal of Information Security and Applications*, vol. 50, p. 102419, 2022.

[6] I. F. Kilincer, F. Ertam, and A. Sengur, "Machine learning methods for cyber security intrusion detection: Datasets and comparative study," *Computer Networks*, vol. 188, p. 107840, 2021.

[7] N. Thapa, Z. Liu, D. B. Kc, B. Gokaraju, and K. Roy, "Comparison of machine learning and deep learning models for network intrusion detection systems," *Future Internet*, vol. 12, p. 167, 2020.

[8] M. A. Ferrag, L. Maglaras, H. Janicke, and R. Smith, "Deep learning techniques for cyber security intrusion detection: A detailed analysis," in *6th International Symposium for ICS & SCADA Cyber Security Research 2019*, pp. 110, 102817, 2019.

[9] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. 7, pp. 41525–41550, 2019.

[10] B. Susilo and R. F. Sari, "Intrusion detection in iot networks using deep learning algorithm," *Information*, vol. 11, p. 279, 2020.

[11] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, "A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions," *Electronics*, vol. 9, p. 1177, 2020.

[12] L. Liu, P. Wang, J. Lin, and L. Liu, "Intrusion detection of imbalanced network traffic based on machine learning and deep learning," *IEEE Access*, vol. 9, pp. 7550–7563, 2020.

[13] N. Saeed, W. Ahmad, and D. M. S. Bhatti, "Localization of vehicular ad-hoc networks with rss based distance estimation," in *2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, pp. 1–6, 2018.

[14] I. H. Sarker, Y. B. Abushark, F. Alsolami, and A. I. Khan, "Intrudtree: a machine learning based cyber security intrusion detection model," *Symmetry*, vol. 12, p. 754, 2020.

[15] W. Ahmad, G. Husnain, S. Ahmed, F. Aadil, S. Lim, *et al.*, "Received signal strength-based localization for vehicle distance estimation in vehicular ad hoc networks (vanets)," *Journal of Sensors*, 2023.

[16] M. Imran, N. Haider, M. Shoaib, I. Razzak, *et al.*, "An intelligent and efficient network intrusion detection system using deep learning," *Computers and Electrical Engineering*, vol. 99, p. 107764, 2022.

[17] S. H. Bangash, D. Khan, A. Ishtiaq, M. Imad, M. Tahir, W. Ahmad, G. Husnain, and L. Jan, "Integrating machine learning and deep learning approaches for efficient malware detection in iot-based smart cities," *Journal of Computing & Biomedical Informatics*, vol. 05, pp. 280–299, 2023.

[18] W. Ahmad, S. Ahmed, N. Sheeraz, A. Khan, A. Ishtiaq, and M. Saba, "Localization error computation for rssi based positioning system in vanets," in *2019 International Conference on Advances in the Emerging Computing Technologies (AECT)*, pp. 1–6, 2020.

[19] D. Akgun, S. Hizal, and U. Cavusoglu, "A new ddos attacks intrusion detection model based on deep learning for cybersecurity," *Computers & Security*, vol. 118, p. 102748, 2022.

[20] T. Ullah, E. G. Hussnain, W. Ahmad, G. Sikander, and M. Ashfaq, "An efficient machine learning based multiclass cyber attacks classification and prediction," *The Sciencetech*, vol. 4, 2023.

[21] R. Khan, L. Jan, S. Khan, M. H. Zafar, W. Ahmad, and G. Husnain, "An effective algorithm in uplink massive mimo systems for pilot decontamination," *Results in Engineering*, p. 101873, 2024.

[22] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based intrusion detection system for iot networks through deep learning model," *Computers and Electrical Engineering*, pp. 99, 107810, 2022.

[23] M. S. Elsayed, N.-A. Le-Khac, S. Dev, and A. D. Jurcut, "Ddosnet: A deep-learning model for detecting network attacks," in *2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, pp. 391–396, 2020.

[24] I. Ullah, M. Yasir, I. U. Haq, G. Husnain, S. U. Islam, W. Ahmad, and S. Rizwan, "Performance evaluation of secured virtual private network based on dynamic multipoint virtual private network," in *Proceedings of 1st International Conference on Computing Technologies, Tools and Applications*, pp. 26–35, 2023.

[25] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in *2016 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, pp. 258–263, 2016.

[26] Z. Wang, Y. Liu, D. He, and S. Chan, "Intrusion detection methods based on integrated deep learning model," *Computers & Security*, vol. 103, p. 102177, 2021.

[27] G. Kocher and G. Kumar, "Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges," *Soft Computing*, vol. 25, pp. 9731–9763, 2021.

[28] N. A. Awad, "Computers, materials & continua," *Medicine*, vol. 67, 2021.

[29] L. Abualigah and A. J. Dulaimi, "A novel feature selection method for data mining tasks using hybrid sine cosine algorithm and genetic algorithm," *Cluster Computing*, vol. 24, pp. 2161–2176, 2021.

[30] N. Tiwari, N. K. Singh, R. Singh, and R. Rameshwar, "Identifying potential churners through predictive analysis: evaluation using pro-active-attrition management logistic regression," *International Journal of Technology Transfer and Commercialisation*, vol. 18, pp. 439–461, 2021.

[31] P. Edastama, A. Dudhat, and G. Maulani, "Use of data warehouse and data mining for academic data: A case study at a national university," *International Journal of Cyber and IT Service Management*, vol. 1, pp. 206–215, 2021.

[32] R. Hou, X. Ye, H. B. O. Zaki, and N. A. B. Omar, "Marketing decision support system based on data mining technology," *Applied Sciences*, vol. 13, p. 4315, 2023.

[33] Y. Fu, Y. Du, Z. Cao, Q. Li, and W. Xiang, "A deep learning model for network intrusion detection with imbalanced data," *Electronics*, vol. 1, p. 898, 2022.

[34] H. Su, H. Sun, J. Zhu, S. Wang, and Y. Li, "Bat: Deep learning methods on network intrusion detection using nslkdd dataset," *IEEE Access*, 2020.

[35] F. Ateş *et al.*, "Determination of vehicle type by image classification methods for a sample traffic intersection in isparta province," in *Proceedings of the International Conference on Artificial Intelligence and Applied Mathematics in Engineering*, 2021.

[36] S. Rawat *et al.*, "Intrusion detection systems using classical machine learning techniques vs integrated unsupervised feature learning and deep neural network," *Internet Technology*, vol. 5, 2022.

[37] P. L. S. Jayalaxmi *et al.*, "Machine and deep learning solutions for intrusion detection and prevention in iots: A survey," *IEEE Access*, vol. 10, pp. 121173–121192, 2022.

[38] Y. K. Saheed *et al.*, "A machine learning-based intrusion detection for detecting internet of things network attacks," *Alexandria Engineering Journal*, vol. 12, pp. 9395–9409, 2022.

[39] V. Dutta *et al.*, "A deep learning ensemble for network anomaly and cyber-attack detection," *Journal of Sensor*, vol. 20, p. 4583, 2020.

[40] H. Yang, L. Cheng, and M. C. Chuah, "Deep-learning-based network intrusion detection for scada systems," in *IEEE Conference on Communications and Network Security*, 2019.