Efficient Intrusion Detection system in Cloud Computing environment using Deep Learning Algorithms

MSc Research Project
Cloud Computing

Vishnu Vardhan Ponnada
Student ID: x21182671

School of Computing
National College of Ireland

Supervisor: Aqeel Kazmi

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Vishnu Vardhan Ponnada
Student ID:	x21182671
Programme:	Cloud Computing
Year:	2023
Module:	MSc Research Project
Supervisor:	Aqeel Kazmi
Submission Due Date:	14-08-2023
Project Title:	Efficient Intrusion Detection system in Cloud Computing environment using Deep Learning Algorithms
Word Count:	7086
Page Count:	23

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Vishnu Vardhan Ponnada
Date:	14th August 2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Efficient Intrusion Detection system in Cloud Computing environment using Deep Learning Algorithms

Vishnu Vardhan Ponnada
x21182671

Abstract

As the digital landscape evolves, the challenges faced by network specialists in the realm of cloud communication and information intensify. The critical concern revolves around detecting malicious behaviors originating from individual hosts and spreading across interconnected cloud networks. Intrusions, representing unauthorized breaches within cloud resources, have catalyzed the demand for efficient Intrusion Detection Systems (IDS). Administrations and organizations have turned to creative remedies to counter these risks, and one particularly promising strategy is the employment of deep neural network algorithms. The current research focuses on applying deep learning algorithms to identify and categorize various security attacks in the cloud computing environment. A possible address is provided by deep learning, which is recognized for its capacity to uncover complicated patterns within big datasets. Several algorithms were used in this work Among tested models, the Autoencoder displayed superior performance, exhibiting an accuracy of 99.56% in identifying and categorizing malicious and Benign attacks within cloud environments. Further enhancing the study's contribution to cloud security, a real-time web application has been developed using Flask. This application adeptly detects security threats by meticulously analyzing network packets in real-time. The findings of this study contribute significantly to the realm of cloud security, furnishing valuable insights and establishing a robust framework for enhancing threat detection and mitigation tactics within cloud environments.

1 Introduction

The progress and evolution of cloud computing in the past few years is colossal and immeasurable. Considered to be one of the most effortlessly accessible avenues, Cloud offers tremendous opportunities for data and resource sharing to users across different domains, owing to its high-performing, flexible, and on-demand nature. It also plays a pivotal role in reducing infrastructure investment and operational costs of businesses and organizations as it offers popular on-demand services like pay-as-you-go, which proves to be one of the most effective data solutions. The rapidly increasing popularity of cloud computing has resulted in a drastic increase in data being stored in it on a day-to-day basis. Along with this, the volume and challenges associated with the data also increase. With the eventual increase in the quantity of data, it also possesses a gap for advanced and complex threats. Although the cloud's effectiveness and security have significantly increased, so have the malware threats. Over the past few years, both the cloud service providers as well as the users have witnessed a radical increase in the happening of security threats, which commonly happen in the form of malware attacks, phishing, manipulation of data servers, compromised data integrity and user confidentiality. The distributed structure outline and publicly accessible architecture of the cloud base are observed to be the prime reason for the happening of such attacks. Also, with the continuous progression in the technological world and with the rise of advanced tools, cyber-attacks have become very progressive and stealthy. It has also potentially propagated a vulnerable loophole for cyber attackers to penetrate the cloud. This grey area has put the users as well as the Cloud Service Providers in a helpless and vulnerable position, making the cyber attackers use it as an opportunity. To avoid these issues, cloud service providers have been using the technique of encryption to safeguard the data in the cloud and establish confidentiality. However, it has been deemed necessary to have a proper protection system in place that synchronously work with the cloud service providers as well as the users to avoid or prevent such disastrous cyber-attacks from happening.

Cloud computing revolved around cloud data centres. The service rendered by the cloud service providers also keeps the data centres as a focal point to improve their applications and better their working. Here different cloud data centres and warehouses are used to host these said applications. These are of high value and any intrusion or anomaly found in this space can pose a serious threat to the environment or the application as a whole. It also has a chance of higher escalations and surging network or application failures. In the last decade, various protocols and approaches have been implemented in the cloud environment to detect and prevent the happening of such anomalies and cyber-attacks. The concept of anomaly or intrusion detection is widespread and can not only be restricted to the domain of cloud computing. The majority of the previous examples deal with the detection process that is related to hardware failure, but not specifically to the cloud environment. Also, traditional intrusion detection systems are solely based on rule-based or signature-based approaches, which may have a lot of fallbacks and limitations in dealing with modern and new-age cyber-attacks. These conventional approaches only work well if the patterns or signatures of such attacks are known prior. The techniques cannot keep up with the ever-evolving technology and modern anomalies. So, employing these traditional intrusion detection techniques fails to detect novel cyber-attacks leaving the network, cloud service providers and users with a security breach in the cloud environment.

Another important factor that should be considered is the scalable and dynamic nature of the cloud computing infrastructure. These attributes of the cloud make it very complicated and challenging for the conventional intrusion detection system to find and stop the presence of anomalies in the network. Also, the traditional IDS find it very difficult to detect the presence of anomalies with the immense network traffic and high volume of data. Additionally, the distributed framework along with the resource allocation processes make the detection process further intricate and problematic. The conventional intrusion detection approaches find it difficult to become accustomed to these dynamic contexts, which increases the number of false positives and false negatives and reduces the system's complete efficacy.

In order to resolve the issues, Previous research works employed machine learning techniques to detect the presence of anomalies have shown tremendous scope. Since it offers excellent real-time prediction and swift processing, it is ideal. However, with the machine learning algorithms, extensive training samples needed to be logged in to avoid the data imbalance in the cloud. This takes us to the next step of using a higher classification model when compared to machine learning, which can render a higher level of accuracy. This is where the need for deep learning comes into the picture. This paper suggests using deep learning techniques for intrusion detection to alleviate the drawbacks of conventional IDS in the cloud computing context. We aim to create an IDS that can successfully identify and mitigate intrusions in the cloud computing environment by utilizing the capabilities of deep neural networks.

1.1 Aim of Study

The main objective of this study is to create an intrusion detection system that is more effective and reliable than current approaches. The proposed deep learning model will be able to perform real-time detection, minimize false positives and negatives detection, and detect majority of the cyber-attacks. We seek to improve both the accuracy and adaptability of intrusion detection in the complex and dynamic cloud computing environment by combining deep learning techniques.

1.2 Research Objectives

The research objectives for the study on cloud security using deep learning models can be outlined as follows:

- To evaluate the present state of cloud security, pinpointing the gaps and vulnerabilities that malicious entities might exploit.
- To explore the potential of deep learning models, particularly the Autoencoder model, in enhancing cloud security measures.
- To design a system, possibly utilizing a web UI, that can provide real-time analysis of cloud traffic, distinguishing between benign and malicious activities.

1.3 Research Question

The following research question aim to provide clarity on the potential of deep learning in strengthening cloud security, guiding the research towards meaningful insights and impactful solutions.

- How effective are deep learning models, especially the Autoencoder, in detecting and categorizing malicious activities in cloud environments? Can a real-time monitoring system be developed to identify and categorize cloud traffic as benign or malicious promptly using a Deep learning algorithm?

2 Related Work

This section of the research paper deals with analysing and assessing existing research works in the domain of intrusion detection systems. It presents conventional IDS approaches, machine learning, and deep learning-based IDS models.

2.1 Signature-based Conventional Intrusion Detection System in Cloud Computing

An existing research work that presents a complete inspection and assessment of the signature-based anomaly detection system as a whole is presented by the authors' Masdari and Khezri (2020). It also includes the data and machine learning techniques for the process of detection. The advantages and fallbacks of this approach are clearly discussed and analysed in this work. All the attributes of comparison are carefully evaluated to derive the end note. From the outcomes, it is evident that the signature-based traditional methods can't justify the dynamic requirements of the cloud environment. This research thesis also opens up the scope for future research in the same and allied fields. Another insightful research work that deals with the intrusion detection process using the signature and pattern-based approach is carried out here Sangeetha et al. (2015). This research is carried out to find the presence of anomalies in the virtual network applications with the data of identical anomaly samples. The rules of semantics are also applied in this thesis to derive cordial results. The signature and rule-based samples are checked with the model and if the result comes as a mismatch, then it is detected as malicious. The limitation of this research is that it falls short in analysing large samples and datasets. A research thesis that portrays the rule and signature-based IDS in the cloud setting using a fog-related framework is presented here in this paper Wang et al. (2018). To prevent overall threats, a collaborative approach is carried out. A lot of factors like data size, analysing patterns, attributes, locational aspects as well as signature models are employed in this paper to arrive at desirable results. The outcomes of this research clearly showcase the advantages as well as limitations of this model. The fog approach is the pivotal factor in this thesis. The share resources are also taken into consideration here. The outcomes depict a lot of room for improvement and show inadequacies on a large scale.

Most conventional research work related to signature and rule-based intrusion detection systems focuses primarily on a specific kind of anomaly detection. The same thought is clearly established in the work tagged here Rajendran et al. (2019). In this research, the authors target detecting the presence of DoS attacks in the cloud setting. To realise this model, a rule-based smart strategy is employed. The developed classification system seems to work well with the stipulated detection process. It is also coupled with feature selection algorithms to give accurate results. The only drawback is that this approach cannot detect the evolving and other anomalies present in the network. Another related analysis done in the same domain is formulated and published by the authors' Kumar et al. (2020). A very strong narrative about the inadequacy of conventional rule and signature-based approach's performance in real-time online data is clearly portrayed in this model. Here the author uses decision trees and a massive dataset for analysis. From the research outcomes, it is evident that the performance of this technique works very accurately in the offline data set compared to the real-time one. But no improvement was observed in the reduction of false negative and positive ratios. It is only capable of detecting multiple anomalies in the offline dataset. That is why there is a need for a better IDS system that can keep up with the dynamic evolution of cloud settings and progressing anomalies Alam et al. (2019).

2.2 Machine Learning-based Intrusion Detection System in Cloud Computing

As already mentioned, several researchers clearly convey the effectiveness of machine learning algorithms in the detection of anomalies in the cloud environment. The research done here Suman and Kumar (2023), proves the same statement in the most effective manner. To convey the essence of the research, the authors carry out both theoretical and analytical approaches to deepen their claims. This model is designed to detect various kinds of cyber-attacks that the could possibly face. The only issue is that the authors employ a vast amount of training samples to achieve their desired results. The DDoS attack is especially concentrated in this research. The outcomes observed are proven to be effective and productive. In a detailed review carried out by Subramanian and Tamilselvan (2019), the authors present a detailed synopsis of the efficacy of machine learning techniques in the detection of cyber-attacks. They also lay emphasis on how this classification algorithm influences the future of cloud security in a very positive manner. Here, the Support Vector Machines (SVM) and linear regression algorithms are used. Again, there is a need for a huge training sample set in this proposed model to make machine learning effective. The authors also consider a complete approach when it comes to cloud security. The outcomes of the research are evaluated with the existing research works. In the work presented by Chkirbene et al. (2020), the main issues of imbalance in the cloud because of the usage of extensive training samples are discussed. The ultimate goal of this assessment is to figure out a novel approach that works well in the cloud environment and has the capability to adapt to changing anomalies. A classifier is used in this analysis to help the model tell the difference between the cyber-attacks that are taken into consideration which is then allocated in a separate database. The model detects correctly, and the overall accuracy and effectiveness of the approach are improved but there is a need for a huge training sample.

The effectiveness of machine learning in detecting the anomalies and other cyber threats present in the cloud environment is clearly presented in the paper formulated by Srivastava et al. (2022). The aim of the investigation is to increase the flexible and scalable nature of the cloud. Various machine learning algorithms like decision trees and support vector machines are utilised in this research here. The analysis is carried out on both the offline and online data samples and the accuracy is calculated. From the outcomes, we can see the performance in the offline samples are considered to have performed well when compared to the online ones. Another original approach in the same domain of intrusion detection system developed for the identification of anomalies in the cloud using machine learning is drafted by Attou et al. (2023). Here, the authors take their ultimate goal as to strengthen and fortify the cloud computing network. The approach is to regulate the data traffic and dynamicity in the network to make the machine learning algorithms effective and well working. However, the task is found to be very arduous and ongoing. Several data mining techniques and machine learning algorithms are employed here to get optimal results. The performance and precision are overall good. Another comprehensive approach presents the strategy to devise a very efficient system using machine learning to detect anomalies in the cloud Aldallal and Alisa (2021). A specific type of genetic algorithm combined with the support vector machine is utilised in this research work. Two different datasets are taken for comparison purposes. The increase in accuracy range is found to be around 5% but there isn't any significant decrease in the production of false positives and false negatives.

2.3 Deep Learning-based Intrusion Detection System in Cloud Computing

From the literature comparison, it is evident that the employment of deep learning algorithms in detecting anomalies is quite effective. The same is clearly established in the work done by Vinolia et al. (2023). Here, the authors compare both the machine learning as well as deep learning algorithms to test and analyse the accuracy and effectiveness of both in the different stages of model drafting. A myriad of computing and data mining techniques are employed in this research. From the outcomes, it is very precise and clear that the deep learning unsupervised approach tends to perform well than the machine learning algorithms. This model was able to achieve a supreme accuracy of around 99%. A very similar research work close to the proposed approach is carried out here Parampottupadam and Moldovann (2018). In this thesis, the authors plan to devise a deep learning-based intrusion detection system that works on real-time cloud computing methodology. Popular algorithms neural networks, naïve Bayes, random forest, logistic regression and support vector machine is employed here. The outcomes of this paper prove that the deep learning method is the best to arrive at promising results in the detection of anomalies in real-time networks. A cumulative accuracy of around 99.5% is found in the outcomes of this model. The training data sample also has an accuracy of around 83%. A brief approach of deep learning combined with a hybrid approach is formulated by Garg et al. (2019). The author employs a consecutive technique to effectively detect the presence of collective anomalies in the cloud environment. The convolutional neural network (CNN) and the hybrid technique of grey wolf optimization (GWO) are easily utilised as the prime algorithms of this research. Working in two different phases, this model consists of both natural and synthetic datasets which are very extensive and all-inclusive. This cloud-based detection proved to be much superior to the others with an overall improvement in accuracy of 9%.

The potential of neural network in prediction and detection applications are already well established. The research work of Hizal et al. (2021), shows us the capacity of the same in detecting anomalies in the cloud. The motive of this research is to identify the presence of cyber-attack and to negate that threat from happening again. The authors employ both convolutional neural networks (CNN) and recurrent neural networks (RNN) to formulate this model. The KDD dataset is used here. This model exhibits around 99% accuracy in the proceeded classifications. Optimising the cloud environment is also equally necessary to keep it stable from cyber-attacks. Bhingarkar et al. (2022) presented a comprehensive research work that presented an optimised model to detect the presence of malware in the cloud network. The author employs deep learning algorithms like neural networks, max-min, etc. to ideate the process. The integration of several optimization algorithms like a chimp and autoregressive chimp plays a pivotal role in this research thesis. The accuracy of this work is found to be around 94% and the sensitivity around 95%. An intrusion detection system that specifically revolves around neural networks is developed and published by Joshi et al. (2018). Various techniques come in cohesion to present this approach to detect the presence of anomalies in the cloud network. Both the convolutional neural networks and recurrent neural networks are the prime methods used in this analysis. From the outcomes, the efficiency and the outcomes of the deep learning algorithms in detecting anomalies are clearly observed. The precision and accuracy of this deep learning-based IDS are found to be on a higher scale compared to the conventional approaches.

3 Methodology

Online fraud activity in the sphere of cloud security underscores the vulnerabilities in our cloud infrastructure. These vulnerabilities can lead to breaches of protected intellectual property, failures in cloud equipment, degradation of cloud-based sensitive data, and a compromise of individual privacy, trustworthiness, and credibility within the cloud environment. In light of these challenges, it's paramount to deploy an IDS (intrusion detection system) specifically tailored for cloud systems, ensuring their integrity against a vast array of threats. IDS's functionality becomes indispensable for organizations operating in the cloud, defending against covert and elusive attacks by analyzing network traffic attributes within the cloud to detect malicious patterns. Thus, the primary objective of this work is to design an IDS optimized for cloud security. With the help of deep learning algorithms in this research, the Intrusion Detection system can enhance cloud security. Following Methodology is used in order to enhance the cloud security using Intrusion detection system as shown in Figure 1.

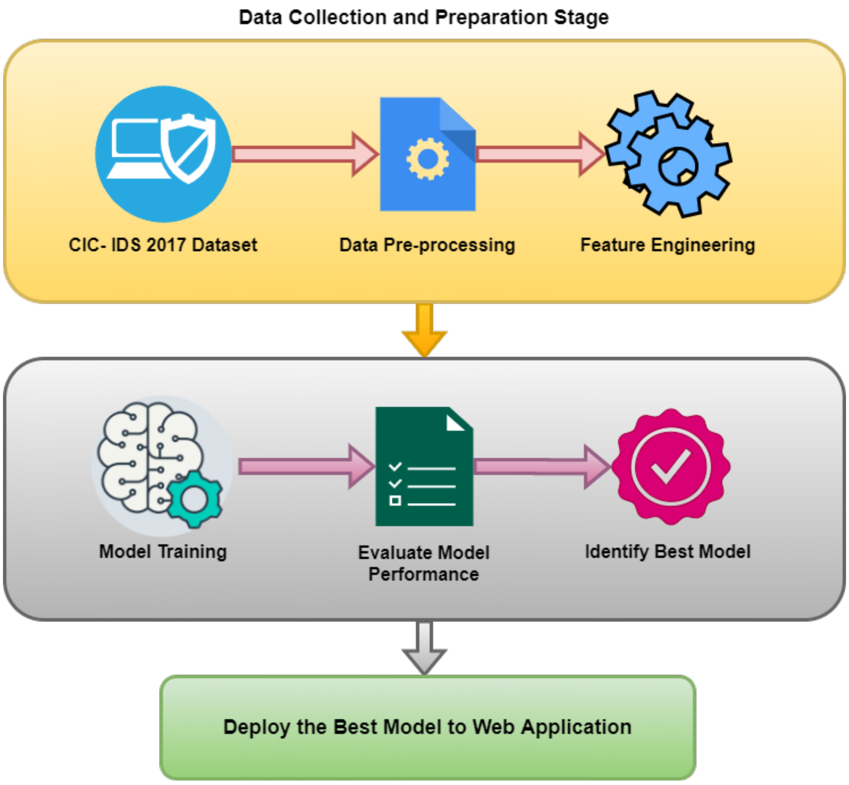

Data Collection and Preparation Stage
CIC- IDS 2017 Dataset
Data Pre-processing
Feature Engineering
Model Training
Evaluate Model Performance
Identify Best Model
Deploy the Best Model to Web Application

Figure 1: Methodology Diagram for Intrusion Detection System

3.1 Dataset Description

The CIC-IDS2017 dataset, sourced from the CIC data repository, is instrumental in the realm of deep-learning for cyber security. It serves as a foundation for training, validation, and testing of intrusion detection algorithms. This dataset encapsulates a myriad of cyber-attacks, including DDoS, DoS, benign FTP, and STP. Despite its comprehensive nature, only one file offered a balanced data distribution for our research. This particular subset contains 225,745 samples, each characterized by 79 distinct features. Analyzing this data offers invaluable insights into crafting effective IDS systems.

3.2 Data Preprocessing

A vital stage around the development of deep learning models is preparing the data, allowing us to guarantee that the information being collected is of excellent quality and appropriate for the investigation and training of models. Multiple significant preprocessing operations was carried out in this research. First, to understand the essence of the attributes, the data formats for every column were examined. This understanding is useful for choosing the right techniques for preprocessing and for comprehending the data. The data were then statistically described, offering general statistics like average, standard deviation, maximum, minimum, etc. These figures give an overview of the data's dispersion and variation. The following phase included removing possible empty or NaN (Not a Number) entries from the raw data in order to correct any discrepancies. The result helps to eliminate data items that are absent or that are insufficient, which might have a negative impact on the effectiveness of the assessment and modeling. In this instance, it turned out that the information set had no null values. Additionally, it was discovered that particular fields had infinite values. To address this, NaN values were used to substitute the endless values. By using this method, any problems that can result from the existence of innumerable values are avoided and the data is guaranteed to stay intact. Furthermore, multiple columns were found to have only one distinctive value in them. These columns don't offer any useful data for reviewing or building models. Therefore, the 8 features/columns were removed from the resulting dataset. These preprocessing procedures lay the groundwork for generating precise and dependable outcomes in the development phases that follow.

3.3 Data Analysis and Visualisation

In order to fully comprehend the dataset & its fundamental trends, as well as acquaintances, analysis of data and visualization, are necessary for deep learning initiatives. Data visualization along with analysis are crucial because they aid in comprehending the dataset's properties, spotting prospective patterns or deviations, and directing toward the choice of suitable characteristics for the training of models. To start with, a probability density histogram was plotted for the "Destination port" column. This plot as shown in Figure 2 helps in understanding the distribution of destination ports in the dataset. From this figure 2, it is visible that 0-499 destination ports have the highest density for both benign and DDoS attacks while the density lowers as the destination port increases.

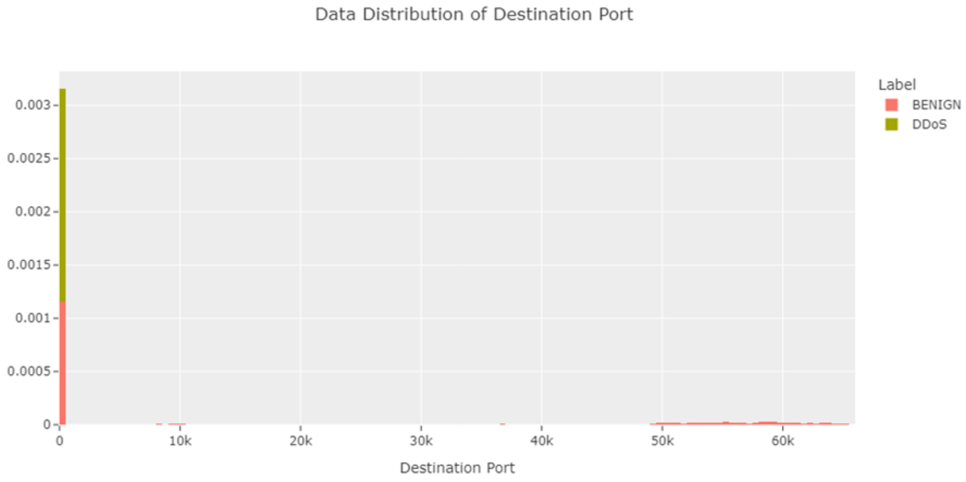


Figure 2: Data Distribution of Destination Port

Following that, line plots were generated to analyze the data distribution of the "active mean" and "Idle mean" columns, providing insights into the behavior of these features as shown in Figures 3 From Figure 3, it is depicted that for active means the DDoS usually ranges between 25k-170k while benign have more density in 0 to 24k or 180k-200k, and for ideal means the value count for each is high and similar behavior is also observed.

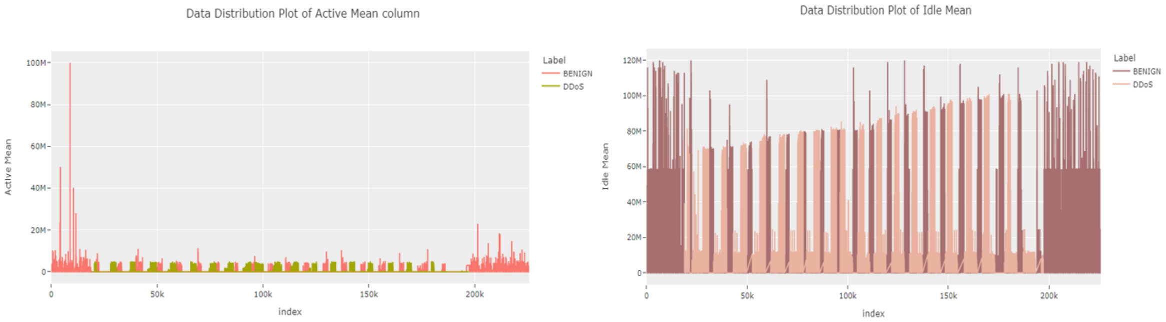


Figure 3: Data Distribution of Active Mean and Idle Mean Column

Histogram plots were then used to examine the distribution of the "ECE Flag Count" and "SYN Flag Count" columns, shedding light on the occurrence and frequency of these flag counts as shown in Figures 4 it is analyzed that the data distribution for both labels is approximately the same while SYN Flag depicts that for benign the counts of SYN Flag Count is more than than DDoS attacks.

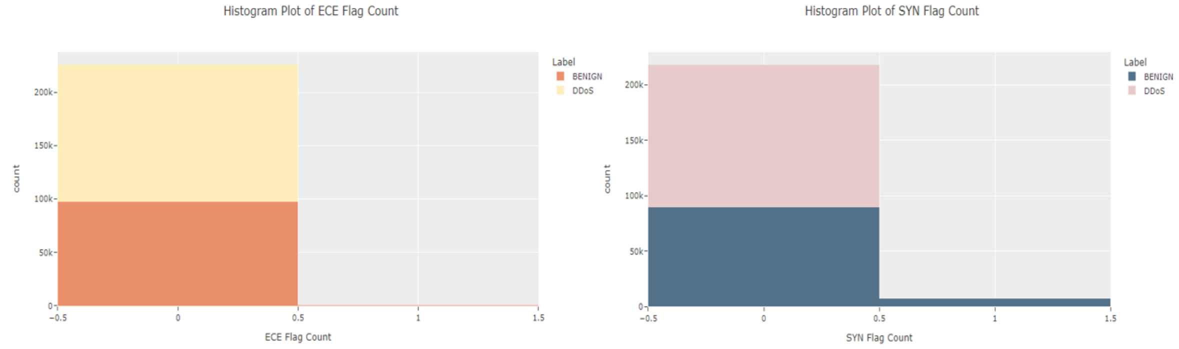


Figure 4: Histogram plot for ECE and SYN Flag Count

Density-wise outliers and data analysis were performed on the ”PSH Flag Count” column using a violin plot, which helps in visualizing the distribution, central tendency, spread, and potential outliers of the ”ACK Flag Count”. as shown Figure 5. After analyzing Figure 5 we found that no outliers are present but for DDoS density is very low while for benign while ACK flag counts are the same for both attacks and have no outlier in data.

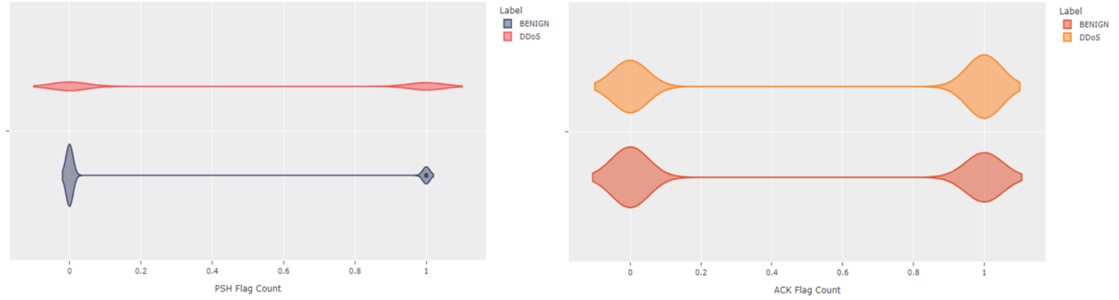


Figure 5: Violin Plot of PSH Flag and ACK Flag Count

A pie plot was generated to explore the different values of the ”Down/Up Ratio” column, providing a visual representation of the ratio distribution as shown in Figure 6.

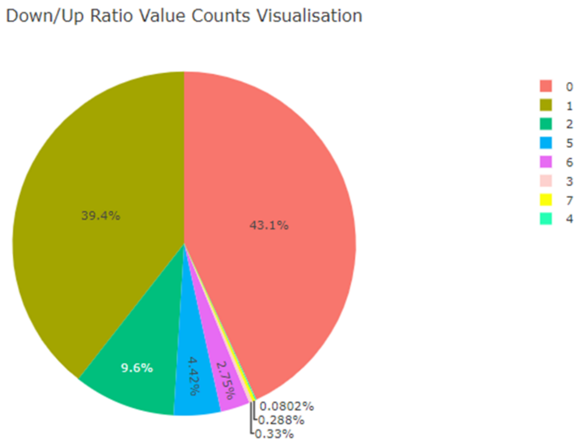


Figure 6: Down/Up Ratio Value Counts

Scatter plots were utilized to analyze the relationships between various columns and the target variable (”Label”). Specifically, scatter plots were created to examine the associations between ”Total Fwd Packets” and ”Total Backward Packets” with attacks as shown in Figure 7, From Figure 7 it is observed in DDoS attacks very few ”Total Fwd Packets” and ”Total Backward Packets” but benign attacks have both Fwd packets and Backward packets.

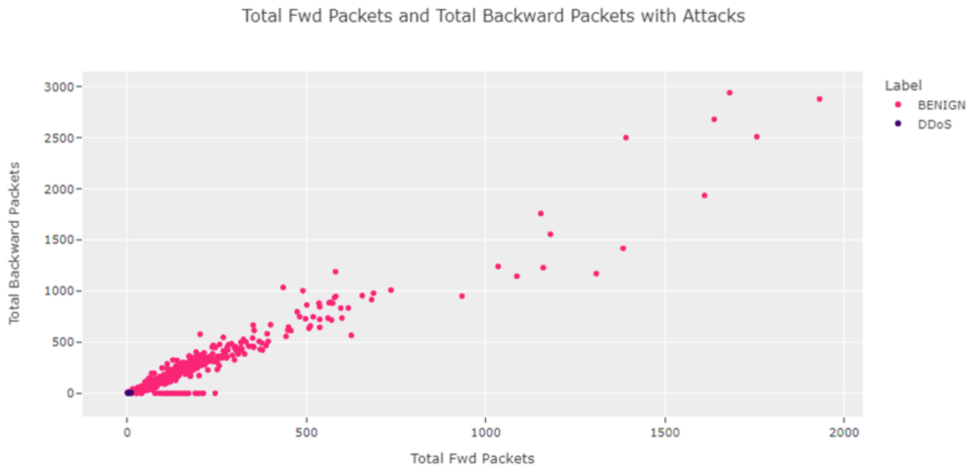


Figure 7: Distribution of Total FWD and BWD packets with Attacks

Insights into the pattern of distribution of destination ports, the behavior of mean values, the regularity of flag counts, the existence of outliers, the proportional distribution, and the associations among multiple characteristics and incidents are all accessible via these different plots, granting the dataset a deeper understanding and guiding subsequent processes.

3.4 Feature Engineering

Regarding deep learning tasks, feature engineering is generally a critical stage that entails converting and structuring the data for improved performance of the model. Numerous feature engineering strategies were used in this endeavor. For the purpose of avoiding data leaking throughout the modeling process, the intended column, particularly the 'label' column, had originally been removed. A simple imputer using the most frequent strategy was employed to deal with data that was missing. Using this method, every column's most frequently encountered entry is used to substitute any empty entries. The synthetic minority over-sampling technique (SMOTE) was subsequently utilized as an oversampling technique to balance the imbalanced dataset as depicted in Figures 8.

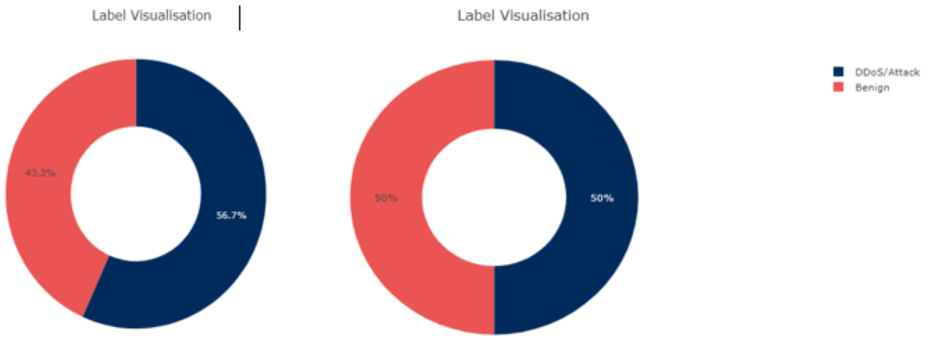


Figure 8: Imbalanced Dataset and Balanced Dataset after SMOTE

The incorporation of the Min-Max Scalar to standardize the data. Principal Component Analysis (PCA) was also executed to reduce dimensionality because the dataset included a high number of columns. With the use of the PCA dimensionality reduction approach, a high-dimensional dataset has been converted into a lower-dimensional depiction while still retaining the most crucial data. 18 components were determined to be enough in this endeavor to acquire 99% of the data. The chosen components were visualized using a line plot as shown in Figure 9. To verify their effectiveness in capturing the variance. Following the application of PCA, the data's shape was altered to (256054, 18), indicating a decrease in the total quantity of features while maintaining the data that is of greatest importance. In conclusion, feature engineering approaches were used to prepare the data for further modeling, including deleting the target column, managing missing values, correcting class imbalance by oversampling normalization, and reducing dimensionality using PCA.

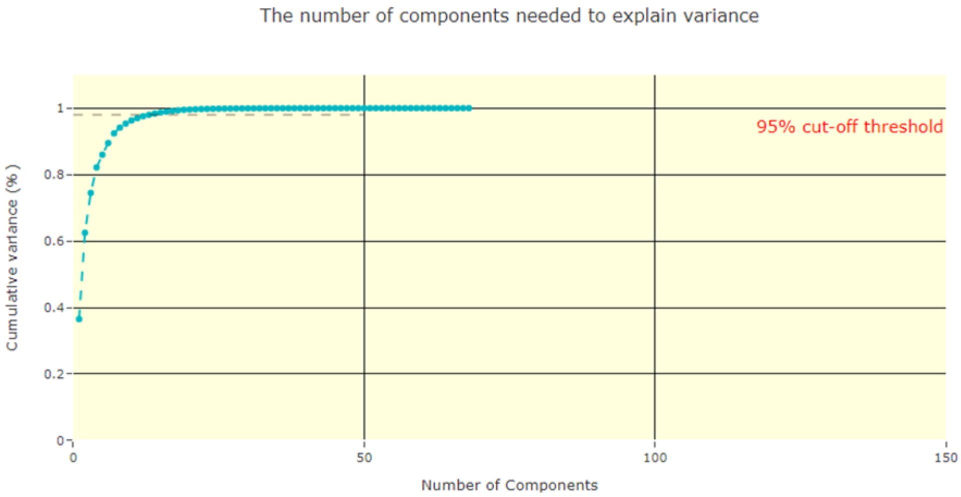


Figure 9: Principle Component Analysis

3.5 Model Training

Particularly in the discipline of cybersecurity, where reliable models are necessary for identifying and categorizing diverse attacks, training models are an important phase in deep learning initiatives. In this endeavor, deploying three sophisticated deep learning models, including RNN (Recurrent Neural Network), GRU (Gated Recurrent Unit), and autoencoders. The data is splitted into train and test data in the ratio of 80 to 20. Each deep learning model was built with different configurations, involving various numbers of neurons and layers. These configurations were chosen based on prior knowledge, experimentation, and the specific requirements of the problem. The CICIDS-2017 dataset, which is frequently characterized by time-sensitive and changing threats, was used to identify temporal relationships using the RNN and GRU models, which are recognized for their capacity to interpret sequential data. On the contrary, autoencoders were used because of their ability to minimize errors in reconstruction while learning usable mathematical models for the input data. The algorithms can improve their performance to generate precise predictions on unobserved data by modifying the weights and biases that are used during training.

3.6 Model Evaluation

When evaluating the success rate and efficiency of deep neural network models for binary categorization tasks like identifying and categorizing benign and DDoS attacks within the sector of cybersecurity, the assessment of models is an important stage. A number of assessment criteria, including accuracy, recall, precision, and F1-score, have been employed in this study. The test data, which had been isolated from the data for training, was utilized to assess the algorithms. The efficiency of the model was evaluated by generating forecasts on the test data and evaluating how successfully it sorted incidents into the appropriate categories. Understanding the models' abilities and drawbacks is revealed during the model assessment process, allowing for better model selection and advancement. This evaluation procedure is essential for determining if the models are appropriate for use in practical applications and for determining whether they possess the acceptable levels of precision, dependability, and robustness necessary for successful cloud security solutions.

4 Design Specification

In this section, we will be discussing the working mechanism of intrusion detection in a cloud computing environment. The overall architecture of the Deep learning-based intrusion detection system is shown in Figure 10. As per our architecture the first component of the system is user, which Initiates requests to access cloud services via the internet. Internet is responsible for connecting the user to the desired cloud service, facilitating data exchange.

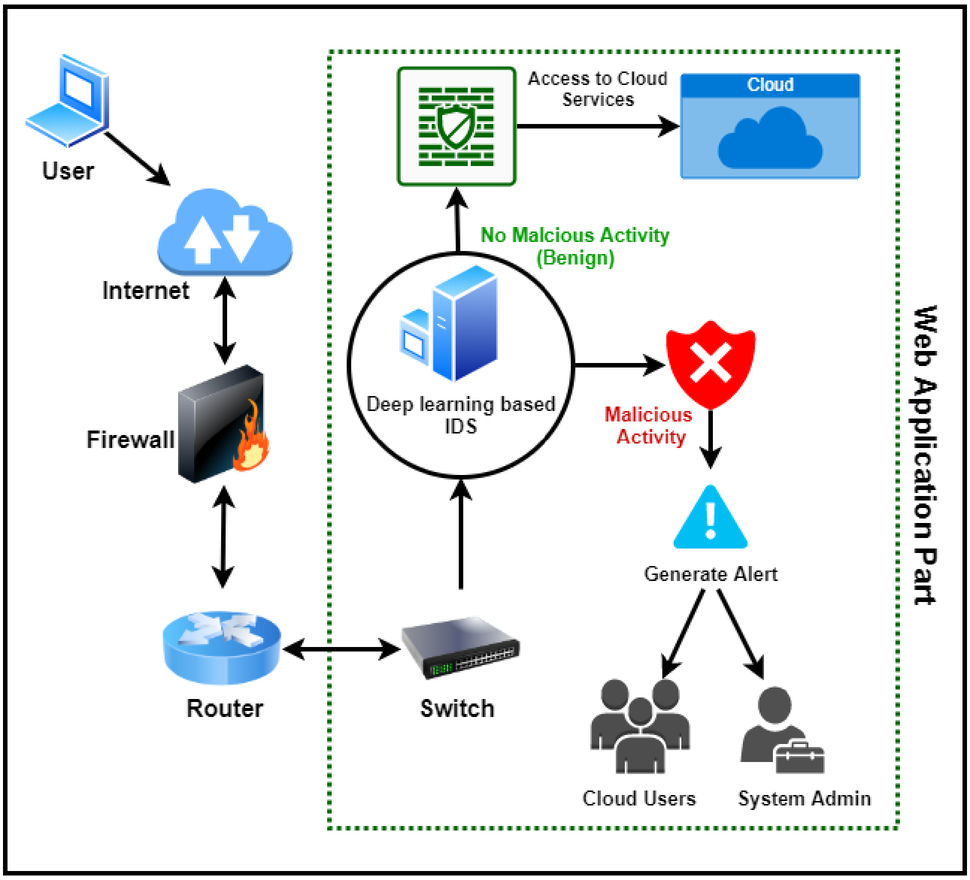


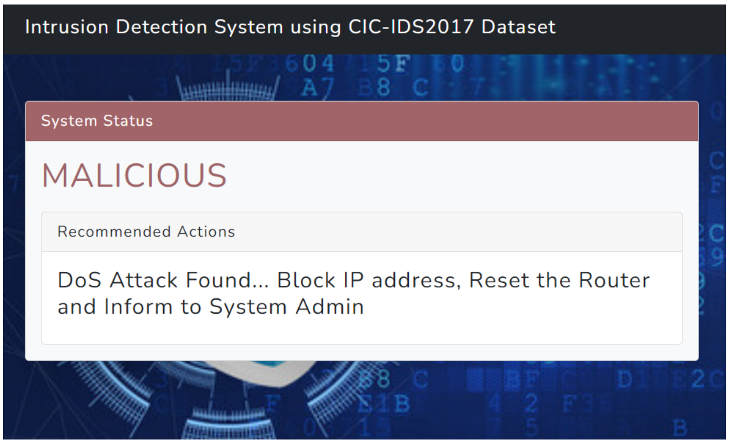
Figure 10: Working Mechanism of Deep Learning based Intrusion detection System in Cloud Computing Environment

A firewall is one of the important components of the system, which adds an additional layer of network security. It inspects and filters incoming and outgoing traffic based on predefined rules. Only traffic that adheres to these rules is allowed through. After the filtration of network packets with a firewall it is transmitted to a router. The router, directs incoming and outgoing data packets, ensuring they reach the correct destination within the network or on the internet. Whereas, Switch is responsible for receiving data packets from the router and forwarding them to the appropriate device or system in the network. After the switch, each network packet has to be passed through an intrusion detection system, where we have employed a deep learning algorithm to continuously monitor system activity. Where it examines data packets to predict potential security threats. IDS Differentiates between benign and malicious activities. Benign activities allow users to continue accessing cloud services. If malicious activity is detected, the IDS classifies the type of security threat. If a security attack is identified by the IDS, an alert is automatically generated. This alert is promptly sent to both cloud users and administrators, ensuring rapid awareness and response. To help the user and cloud administrator a WebUI has been developed, which provides a user-friendly interface that provides real-time analysis of cloud computing traffic. Displays traffic nature (either malicious or benign) in real-time.

5 Implementation

This work was implemented in a step-by-step process using a variety of Python packages and functions. The procedures were executed utilizing Python programming, including data collection through model training and assessment. The CIC-IDS2017 dataset was accessed from the CIC data repository during the data collection procedure. The Pandas package, which offers features to easily manage and modify the data, was used to import the dataset. To maintain uniformity of data, data preparation methods included eliminating null and NaN values utilizing the ”dropna” function. The most prevalent approach was used for dealing with values that were missing employing the SimpleImputer function provided by the scikit-learn module. To deal with the class imbalance, the imbalanced-learn library’s ”SMOTE” function was used, which implements the SMOTE oversampling method. The MinMaxScaler method obtained from the scikit-learn library typically adjusts the data to a particular range and was then applied to normalize the data. The LabelEncoder method included in the sci-kit-learn package was used to do categorical target column encoding. Principal Component Analysis (PCA) was carried out with the PCA module included in the sci-kit-learn module to decrease the dataset’s dimensionality. The dataset was processed to capture the number of elements that would capture 99% of the data.

Three sophisticated deep learning models—RNN, GRU, and autoencoders—were created utilizing the Keras and TensorFlow frameworks for model training. To investigate various architectural configurations, these models were set up with varying amounts of neurons and layers. The Adam optimizer, a favored deep-learning optimization technique, was used to train the models. For binary classification tasks, the loss function was set to binary cross-entropy. Ten epochs, or the number of full iterations across the dataset, were utilized for training the algorithms. Various categorization standards, including accuracy, recall, precision, and F1-score, have been employed in evaluating the models. The testing data set, which was previously separated from the primary dataset utilizing the train_test_split method of the sci-kit-learn module, was used for the outcome analysis. The Python language for programming, together with the pandas, sci-kit-learn, imbalanced-learn, Keras, and TensorFlow libraries, were all used during the development approach. These libraries provide strong capabilities and resources for data handling, preprocessing, building models, training, and assessment, making it easier to carry out the research task in an efficient and prompt way. After successful training of models and evaluating their performance, the most optimal models have been identified to be used as an Intrusion detection system in the cloud computing environment. A web UI has been developed with the help of the Flask framework in order to provide a user interface for continuously monitoring the abnormal activity of the system. Our web-UI detects network attacks in real-time with the help of an autoencoder deep learning algorithm. Our system follows the Client-server architecture, where the client sends the packet to the server and the IDS inside the cloud server analyses the network packet and classifies the packet as Malicious or Benign. The Screenshot of developed web application using flask detecting Maclious and Benign attack is shown in Figure 11 and Figure 12.



Intrusion Detection System using CIC-IDS2017 Dataset

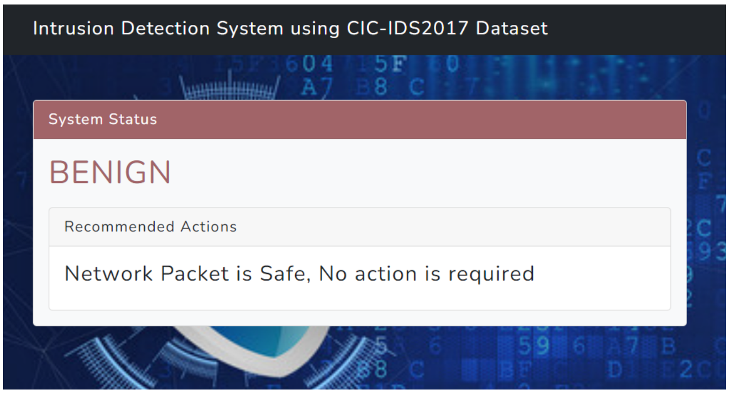
System Status

MALICIOUS

Recommended Actions

DoS Attack Found... Block IP address, Reset the Router and Inform to System Admin

Figure 11: Web Application detecting the Malicious attack using Deep learning based IDS in Real-time and Recommending Actions



Intrusion Detection System using CIC-IDS2017 Dataset

System Status

BENIGN

Recommended Actions

Network Packet is Safe, No action is required

Figure 12: Web Application detecting the Normal attack using Deep learning based IDS in Real-time and Recommending Actions

6 Evaluation

An IDS in cloud security may recognize breaches by analyzing assault behaviors or retrieving signatures generated from network packets. This technique is often referred to as anomaly-based intrusion detection. Deep learning, especially in the context of cloud environments, is particularly effective in this capacity, as it has demonstrated proficiency in anomaly identification. The importance of a potent IDS in maintaining data integrity across global organizations, and safeguarding customer information, cannot be overstated. In this work, three deep learning algorithms – RNN, GRU, and Autoencoders – are specifically tailored to the cloud environment and trained on the authenticated data from the CIC-IDS2017 dataset. Post-training, each model undergoes extensive evaluation using various classification metrics to ensure unbiased model selection. The model showing the highest accuracy, F1 score, precision, and recall will be deemed the best for deployment against potential cloud-based cybercrimes. Different experimentation strategies have been utilized both in the construction and evaluation stages, with a detailed evaluation of each model to be discussed in further subsections.

6.1 Evaluation based on Accuracy

As an assessment metric, accuracy offers a general indicator of how well the algorithms predict the intended outcome. Over epochs, the RNN model's accuracy rose from 97.18% initially to 98.84% in the end. The GRU model also showed improvement, beginning at 98.01% and concluding at 98.96%. Meanwhile, the Autoencoder began with a higher accuracy of 99.34% and slightly decreased to 98.81% in the final epoch. Despite this decline, the Autoencoder model still surpassed the RNN and GRU models in overall accuracy, indicating its superior capability in identifying and classifying threats. In summary, when focusing solely on accuracy, the Autoencoder was the top performer in this study. This performance is visually represented in the accompanying Figure. 13.

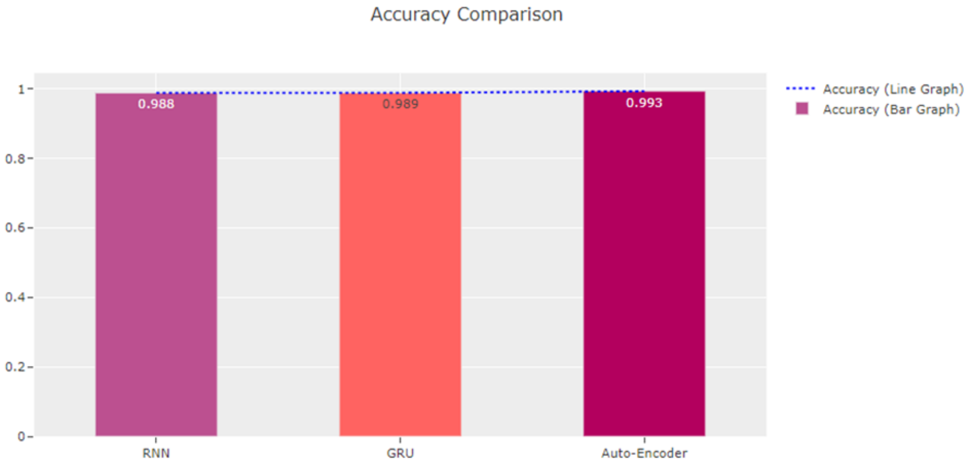


Figure 13: Accuracy Comparison of Models

6.2 Evaluation based on Precision

The fraction of accurately anticipated positive occurrences among all instances projected as positive is measured by precision, which is a crucial assessment parameter, especially when performing binary classification jobs. The precision of the RNN model was 0.9886. The degree of precision was constant from the first to the last epoch, showing that the model continuously produced reliable positive forecasts for the attacks via DDoS in the dataset. The precision of the GRU model was 0.9888. The precision was maintained constant during the training phase, much like the RNN model, proving the model's capacity to precisely anticipate positive cases, such as attacks involving DDoS. A substantial precision of 0.9934 was shown by the Autoencoder approach. Throughout all epochs, the precision kept consistently excellent, demonstrating the algorithm's competence at correctly detecting positive events. When the precision scores for the three models were compared, the Autoencoder model had the highest precision. It pushed both the RNN and GRU algorithms by properly forecasting DDoS incidents, with a precision of 0.9934. The Autoencoder approach for the current endeavor performed exceptionally well on the basis of the assessment that focused on precision. The comparison of employed models based on precision is illustrated in Figure 14.

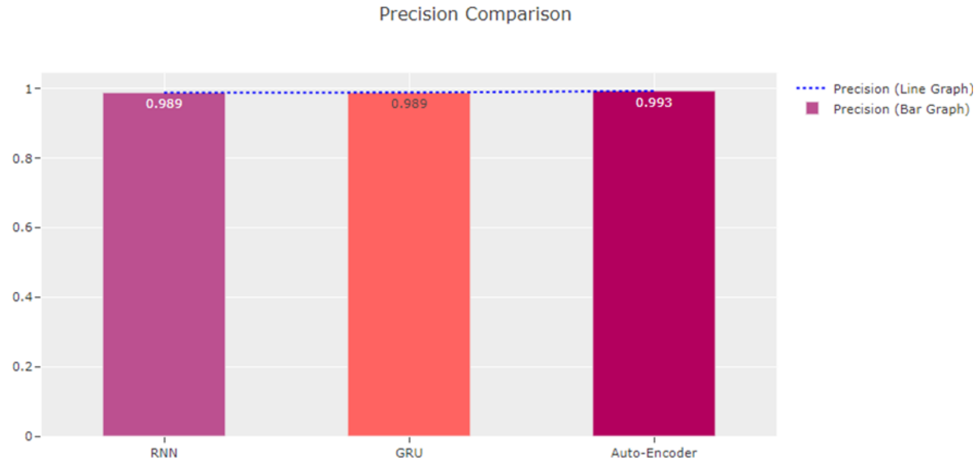


Figure 14: Precision Comparison of Models

6.3 Evaluation based on Recall

Recall, frequently referred to as the real positive rate, quantifies a model's capacity to distinguish DDoS assaults from the real positive cases found in the dataset. The recall for the RNN model was 0.9884. The rate of recall continued high throughout the very first epoch to the last epoch, showing that the algorithm continuously detected a significant part of genuine DDoS assaults in the dataset. The recall for the GRU model was 0.9886. The recall maintained an elevated level during the training procedure, much like the RNN model. The recall for the Autoencoder model was 0.9933. The model's capacity to reliably capture a sizable fraction of the true positive events is shown by the recall being high throughout all epochs. The Autoencoder model had the highest recall out of the three when the recall scores were compared. It topped the RNN and GRU models, alongside a recall of 0.9933. Due to its high recall, which shows that it can accurately identify a sizable part of real DDoS hits, it is a useful model for identifying such incidents in a security measures setting. The comparison of employed models based on Recall is illustrated in Figure 15.

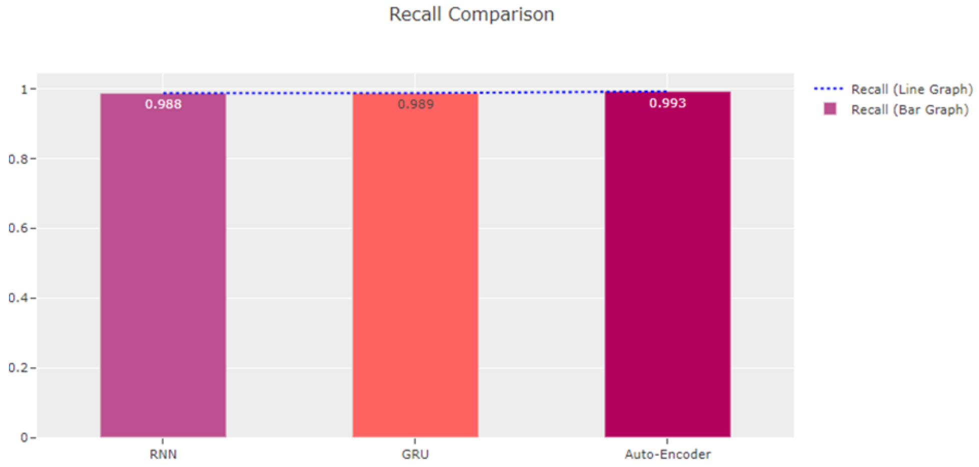


Figure 15: Recall Comparison of Models

6.4 Evaluation based on F1-Score

A metric that takes into account precision and recall, the F1-score offers a fair assessment of an algorithm's ability. The F1 score for the RNN model was 0.9884. The F1-score for the GRU model was 0.9886. The F1 score demonstrated an excellent equilibrium between recall and precision through the training period, comparable to the RNN approach. The F1-score for the Autoencoder model was a fantastic 0.9933. Throughout all epochs, the F1 score was still remarkably high. This demonstrates the algorithm's capacity to detect DDoS assaults with high accuracy and few false positives or negatives. When comparing the three models' F1 results, the Autoencoder model came out on top. It surpassed the RNN and GRU models when it came to obtaining an appropriate efficiency across recall and precision, achieving an F1-score of 0.9933. The comparison of employed models based on the F1-score is illustrated in Figure 16.

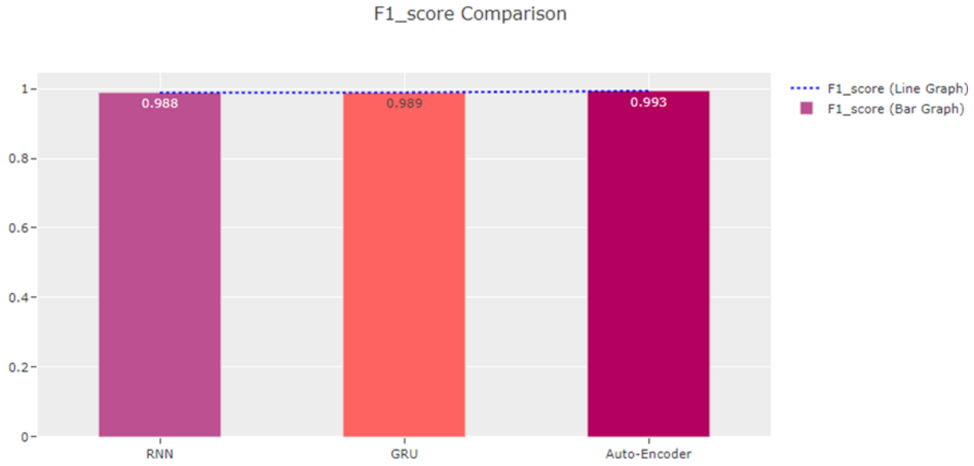


Figure 16: F1-Score Comparison Of Models

6.5 Discussion

Considering the likelihood of using one zero-day vulnerability every single day, the losses brought on by hackers are predicted to amount to as much as four trillion in the future decades. Additionally, in the near future, the volume of data retained in private and public clouds hosted by data-driven businesses will double two hundredfold. Consequently, there is a rise in the need for security systems with more sophistication. The number of victims for putting attacks on the network has expanded due to flaws in computer systems, weak security measures, and ignorance of incidents and offenses. Using common security measures like firewalls and anti-virus programs, networked attacks like the threat of ransom, data theft, theft of identities, disruption of customer service, and zero-day malware is challenging to track down. In order to recognize potential harmful behaviors created by attackers, an IDS (intrusion detection system) is employed to analyze the information moving across the computer system and to trigger an alert. Deep learning algorithms may thus be a solution to the necessity of having an efficient intrusion detection system since the discussion emphasizes the study of the outcomes attained from the adopted procedures and models. The Autoencoder model, which attained a high accuracy of 99.56%, precision of 0.9934, recall of 0.9933, and F1-Score of 0.9933, stood out as the top-performing model among the ones used. When it comes to precision, recall, accuracy, and F1 score, this model fared better than the RNN and GRU approaches. There are a number of possibilities behind the enhanced efficiency of the Autoencoder model. It begins with an Autoencoder structure, which was successfully used to capture primary trends and interpretations in the dataset and is particularly created for unstructured learning and extracting features. The model correctly classified benign and DDoS attacks owing to its ability to reassemble the input data and spot abnormalities. Additionally, the performance of the Autoencoder model was improved by the use of deep learning approaches, such as several layers and the Adam optimizer's capability of optimization. The model was able to learn from the training process across 10 epochs and modify its biases and weights in order to perform at its best. Additionally, it is noted that although slightly inferior to the outputs, the results achieved by the other two methods are likewise noteworthy. The preparation procedures used, including data cleaning, normalization, oversampling, and dimensionality reduction using PCA, are also associated with the achievement of the Autoencoder model and other algorithms. These methods enhanced the model's capacity to generalize and generate precise predictions on untried data while also assisting in the preparation of the data for efficient learning. These findings highlight the importance of strong models and thorough data preparation for precise and trustworthy results, and they offer insightful information on identifying and categorization of various cyberattacks.

7 Conclusion and Future Work

The major contribution of this study is to provide an expansive framework for deep learning-based attack detection and categorization within cloud systems. The insights and conclusions drawn from this research could fortify cloud security defenses, minimize potential threats, and protect essential cloud networks and systems. It has paved the way for further innovations and enhancements in cloud security and the creation of an effective IDS system, contributing to a more secure online space for individuals, businesses, and communities. In this study, the emphasis was on detecting and categorizing different incidents within cloud environments using deep learning methods. Among the explored models, the Autoencoder demonstrated the best performance, achieving an impressive accuracy of 99.56%, precision of 0.9934, recall of 0.9933, and F1-Score of 0.9933. This model illuminated the potential of deep neural networks in the field of cloud security, adeptly identifying and categorizing malicious and benign activities. Currently, our research utilizes the Public dataset from CIC-IDS. However, the real data of IDS and Cloud Systems is much more complex than this, where deep learning models can not be much accurate such data can be collected and predictions can be performed in order to safeguard the cloud user data. Also, incorporating innovative deep learning architectures like Transformer algorithms and deep ensemble models. Such advancements could further enhance the recognition and classification of cloud-based attacks. Continuous streaming data and learning techniques would enhance the algorithms' adaptability to ever-changing attack patterns. Furthermore, the continuous retraining of models with the latest datasets is vital to maintain their efficacy, given the evolving nature of cloud-related threats.

References

Alam, S., Shuaib, M. and Samad, A. (2019). A Collaborative Study of Intrusion Detection and Prevention Techniques in Cloud Computing, *in* S. Bhattacharyya, A. E. Hassanien, D. Gupta, A. Khanna and I. Pan (eds), *International Conference on Innovative Computing and Communications*, Lecture Notes in Networks and Systems, Springer, Singapore, pp. 231–240.

Aldallal, A. and Alisa, F. (2021). Effective Intrusion Detection System to Secure Data in Cloud Using Machine Learning, *Symmetry* **13**(12): 2306. Number: 12 Publisher: Multidisciplinary Digital Publishing Institute.
URL: *https://www.mdpi.com/2073-8994/13/12/2306*

Attou, H., Guezzaz, A., Benkirane, S., Azrour, M. and Farhaoui, Y. (2023). Cloud-Based Intrusion Detection Approach Using Machine Learning Techniques, *Big Data Mining and Analytics* **6**(3): 311–320. Conference Name: Big Data Mining and Analytics.

Bhingarkar, S., Revathi, S. T., Kolli, C. S. and Mewada, H. K. (2022). An effective optimization enabled deep learning based Malicious behaviour detection in cloud computing, *International Journal of Intelligent Robotics and Applications* .
URL: *https://doi.org/10.1007/s41315-022-00239-x*

Chkirbene, Z., Erbad, A., Hamila, R., Gouissem, A., Mohamed, A. and Hamdi, M. (2020). Machine Learning Based Cloud Computing Anomalies Detection, *IEEE Network* **34**(6): 178–183. Conference Name: IEEE Network.

Garg, S., Kaur, K., Kumar, N., Kaddoum, G., Zomaya, A. Y. and Ranjan, R. (2019). A Hybrid Deep Learning-Based Model for Anomaly Detection in Cloud Datacenter Networks, *IEEE Transactions on Network and Service Management* **16**(3): 924–935. Conference Name: IEEE Transactions on Network and Service Management.

Hizal, S., ÇAVUŞOĞLU, and AKGÜN, D. (2021). A new Deep Learning Based Intrusion Detection System for Cloud Security, *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pp. 1–4.

Joshi, P., Prasad, R., Mewada, P. and Saurabh, P. (2018). A New Neural Network-Based IDS for Cloud Computing, *in* P. K. Pattnaik, S. S. Rautaray, H. Das and J. Nayak (eds), *Progress in Computing, Analytics and Networking*, Advances in Intelligent Systems and Computing, Springer, Singapore, pp. 161–170.

Kumar, V., Sinha, D., Das, A. K., Pandey, S. C. and Goswami, R. T. (2020). An integrated rule based intrusion detection system: analysis on UNSW-NB15 data set and the real time online dataset, *Cluster Computing* **23**(2): 1397–1418.
URL: *https://doi.org/10.1007/s10586-019-03008-x*

Masdari, M. and Khezri, H. (2020). A survey and taxonomy of the fuzzy signature-based Intrusion Detection Systems, *Applied Soft Computing* **92**: 106301.
URL: *https://www.sciencedirect.com/science/article/pii/S1568494620302416*

Parampottupadam, S. and Moldovann, A.-N. (2018). Cloud-based Real-time Network Intrusion Detection Using Deep Learning, *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, pp. 1–8.

Rajendran, R., Santhosh Kumar, S. V. N., Palanichamy, Y. and Arputharaj, K. (2019). Detection of DoS attacks in cloud networks using intelligent rule based classification system, *Cluster Computing* **22**(1): 423–434.
URL: *https://doi.org/10.1007/s10586-018-2181-4*

Sangeetha, S., Gayathri devi, B., Ramya, R., Dharani, M. K. and Sathya, P. (2015). Signature Based Semantic Intrusion Detection System on Cloud, *in* J. K. Mandal, S. C. Satapathy, M. Kumar Sanyal, P. P. Sarkar and A. Mukhopadhyay (eds), *Information Systems Design and Intelligent Applications*, Advances in Intelligent Systems and Computing, Springer India, New Delhi, pp. 657–666.

Srivastava, N., Chaudhari, A., Joraviya, N., Gohil, B. N., Ray, S. and Rao, U. P. (2022). A Review of Machine Learning-Based Intrusion Detection Systems on the Cloud, *in* U. P. Rao, S. J. Patel, P. Raj and A. Visconti (eds), *Security, Privacy and Data Analytics*, Lecture Notes in Electrical Engineering, Springer, Singapore, pp. 303–317.

Subramanian, E. K. and Tamilselvan, L. (2019). A focus on future cloud: machine learning-based cloud security, *Service Oriented Computing and Applications* **13**(3): 237–249.
URL: *https://doi.org/10.1007/s11761-019-00270-0*

Suman, O. P. and Kumar, M. (2023). Machine Learning Based Theoretical and Experimental Analysis of DDoS Attacks in Cloud Computing, *2023 International Conference on Device Intelligence, Computing and Communication Technologies, (DICCT)*, pp. 526–531.

Vinolia, A., Kanya, N. and Rajavarman, V. (2023). Machine Learning and Deep Learning based Intrusion Detection in Cloud Environment: A Review, *2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pp. 952–960. ISSN: 2832-3017.

Wang, Y., Meng, W., Li, W., Li, J., Liu, W.-X. and Xiang, Y. (2018). A fog-based privacy-preserving approach for distributed signature-based intrusion detection, *Journal of*

Parallel and Distributed Computing **122**: 26–35.
URL: *https://www.sciencedirect.com/science/article/pii/S0743731518305057*