National College of Ireland

Enhancing the Classification Accuracy of Intrusion Detection system using Auto-encoder Algorithm

MSc Research Project
Data Analytics

Jonah Abhijit Papaiah
Student ID: x20189419

School of Computing
National College of Ireland

Supervisor: Prashanth Nayak

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: ……. Jonah Abhijit Papaiah…….……

Student ID: ……..x20189419.……..……

Programme: …….. Data Analytics…..…… **Year:** ……2023…….

Module: ……MSc Research Project…….……..……

Supervisor: ……Prashanth Nayak…….……..……

Submission Due Date: ……15/12/2022……..……..……

Project Title: ……Enhancing the Classification Accuracy of intrusion Detection system using Auto-encoder Algorithm……..……

Word Count: ……..8402..... **Page Count:** ……..….26……..…..……..

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: ……Jonah Abhijt Papaiah……

Date: ……15/12/2022……

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):	

Enhancing the Classification Accuracy of Intrusion Detection system using Auto-encoder Algorithm

Jonah Abhijit Papaiah
X20189419

Abstract

The development of the internet and commerce has compelled governments and other organizations all over the world to promote new technologies and employ more complex procedures and contemporary networks. For instance, several business organizations allow administrative access to the system via the intranet and actively advocate web services for their partners. However, using such networks brings about a number of security risks that enter the system through connections and these malicious data packets impact the security and integrity of the system as well as the confidential information. Governments and other organizations are being forced to push new technology, use more intricate processes, and utilize cutting-edge networks as a result of the growth of the internet and commerce. For instance, a number of commercial organizations permit partners to use online services and actively promote administrative access to the system via the intranet. But using such networks comes with a variety of security dangers that enter the system through connections and these malicious data packets affect the security and integrity of the system as well as the confidential data. The convincible outrun can be machine learning-based algorithms that are capable of automatically identifying the system invasions such as FTP/ SSH brute force intrusions which have resulted in satisfying outcomes. But nowadays it is observed that generally, deep learning algorithms overcome machine learning algorithms if the data size is large enough therefore four advanced deep learning algorithms are applied in this research work which are CNNs, LSTM, Conv-LSTM, and Auto-Encoders. Since the data source can be different in real-world applications therefore two datasets are accounted for this task. All algorithms are implemented and tested on test data and assessed using various parameters since being developed utilizing KDD CUP-99 IDS dataset and CSE-CIC-IDS2018 datasets. The Auto-Encoder approach, which has been proven to be superior compared to these other algorithms after assessment of parameters like Accuracy, Precision, Recall, and Validation Loss, can be employed to categorize invasion into a variety of forms of obtrusive actions in actual employment.

1 Introduction

1.1 Background of the Study

The current interest and approach in developing “internet and communication” (ICT) technologies during the past few years have converse knowledge on the emergence of network security as one of the most vital research domains. The main establishment of expertise in network security comes with a proper understanding of the application of various tools such as firewalls, different antivirus software and most importantly intrusion detection

systems (IDSs). These tools ensure security for the network system and the associated devices within a specific cyberspace. Among all the above-mentioned network security approaches, the IDS system ensures the detection mechanism for any kind of cyber-attack and provides the necessary security through constant monitoring of the traffic in the network system to detect malicious or suspicious behaviour.

The idea and development of the intrusion detection system (IDS) were first introduced by Jin Anderson, in 1980 (Ahmad et al., 2021). Since its establishment, several IDS-based products have been developed as well as modified for improving network security. It is because of immense advancements in technologies during the past decade, a resultant expansion of network size and the use of different applications have been determined that make the use of network nodes. Hence, it results in the generation of massive important data and their sharing across a wide range of network nodes. Under all these generative processes, ensuring network security has become a challenging factor because of the huge number of cyber-attacks or cyber threats due to mutation or changes in conventional attacks. For the recent few years, the network system is highly vulnerable to these threats and organizations are highly concerned about the security enabling their data and networks. For instance, the compromise, if it happens, in the data nodes and the information it provides can induce a massive impact on the organization, especially on its reputation as well as financial losses (Ahmad et al., 2021). When concerning intrusion detection systems, the existing products typically show inefficiency to detect cyber-attacks alongside zero-day attacks as well as reducing the false positive and negative alarm rates. Therefore, the need for adoption of more efficient, reliable, accurate and cost-effective network intrusion detection systems (NIDS) is necessary to enable strong network security.

The fulfilment of the need to develop an effective IDS system has been proliferate by researchers by gathering knowledge and information on the possibilities being explored with different algorithms. For instance, machine learning and deep learning have received great attention in recent years due to their efficiency and reliability in delivering improved results in every approach. These techniques have gained immense popularity even in the area of developing network security through intrusion detection systems. This popularity in network security is gained mainly with the discovery of one of the most powerful “graphics processing units” (GPUs) (Ahmad et al., 2021). Both machine learning and deep learning have served many research purposes, especially in this network security domain and finally gave a productive result. The ML-based intrusion detection system approach is highly dependent on the feature engineering process that uses productive information based on network traffic. On the other hand, a deep learning-based intrusion detection system automatically excels in understanding the complex features extracted from raw datasets deep in its core structure.

For the past decade, researchers have utilized several machine learning and deep learning-based solutions to enable a safe, efficient, and reliable network intrusion detection system to detect malicious or suspicious attacks. However, the extensive increase in network traffic, as well as network security threats, is a diversified challenge with the NIDS system which therefore leads to failure in detecting malicious intrusions properly. When considering the deep learning method, the explanation drew attention to its early stage of research in the network intrusion detection process and therefore never vast exploration of modern technologies efficiently to detect the intruders present in the network. Regarding the intrusion detection system, this study has explored the recent advancements in technologies based on different algorithms with a continuous exploration of the solutions for network intrusion

detection systems. From the continuous research and exploration of previous findings and also understanding the trend towards future perspectives, this study will help to acknowledge the new inventions with a particular focus on auto-encoder-based deep neural network architecture.

1.2 Aim of the Study

The study has aimed at providing knowledge and information on the recent trends of anomaly-based intrusion detection systems using auto-encoder-based deep neural network architecture. Apparently, the study will focus on other algorithms as well to develop an insight into the approaches made till now.

1.3 Research Objectives

The following research objectives have been considered:

- To identify the efficiency of the anomaly-based intrusion detection systems in detecting malicious intrusions
- To identify the techniques or classified models that have been introduced till now to use accordingly with intrusion detection systems to detect intrusion
- To analyse and evaluate the proposed model when used together with an anomaly-based intrusion detection system in the detection of intrusion
- To determine the credibility of each model in the detection of the intrusion and how the proposed model can be compared with existing models

1.4 Research Questions

- Which algorithm is the most optimal method for the detection of intrusions from network system?

- How efficiently the auto-encoder algorithms detect the anomaly in the system and type of attack as compared to other deep learning algorithms?

1.5 Study Significance

The study has been justified with a proper understanding of the network behaviour that has been observed while studying the intrusion detection system. It has been already discussed earlier that in the past decade, the use of machine learning and deep learning in combination with IDS has been used extensively to detect network traffic and suspicious intruders. However, due to massive data input and output, there has been a wide increase in network traffic which the traditional classifiers have failed to detect. Therefore, this study has purposely taken into consideration the existing techniques that have been explored to detect network intrusion and equally observed the value of the proposed auto-encoder deep neural network architecture model with the anomaly-based network detection system in this detection process.

1.6 Conclusion

Upon completion of this first chapter, it is possible to understand the scenario of the intrusion detection mechanism for the past 10 years under the wing of both machine learning and deep learning-based solutions. From the discussion, it has been noted that due to heavy network traffic and massive data generation, old conventional methods may not be able to detect recent intrusions. Therefore, there is a need for more research and development of advanced solutions in combination with anomaly intrusion detection systems to identify malicious activities more efficiently and accurately. Thus, this chapter has presented a thorough understanding of the approaches till now and will continue to explore further in the next chapter of this study to analyze and compare each classification model in detecting intrusive behavior.

2 Related Work

2.1 Anomaly-based Intrusion Detection System

The intrusion detection system (IDS) is an important consideration when defeating malicious activities in the cyber system. While engaging in this contact, researchers are continuously proposing various methods to detect this intrusion and ultimately developed an anomaly-based intrusion detection system where the deviation from normal network behaviour has been pointed as an intrusion (Resende & Drummond, 2018). Under this consideration, the profiling technique is acknowledged as relevant in establishing a baseline to identify the network behaviour as normal. Various algorithms have been used for the past decade with anomaly-based intrusion detection methods to develop a mechanistic action that can enable a swift detection process. In one of the studies conducted by (Resende & Drummond, 2018), an explanation entails the adaptive approach with a genetic algorithm where feature selection is performed for profiling as well as the parameters to be identified for anomaly-based intrusion detection. The experiment was presented with the use of CICIDS2017 datasets. The result obtained from the experiment shows that the method has achieved a good intrusion detection rate of 92.85% along with a false positive alarm rate, of 0.69% respectively. Based on the result, it can be explained further that the new method is adaptive enough to identify novel attacks more efficiently.

The application of the Internet of Things or IoT has been conceptualized as an emerging response of new technology that can improve people's day-to-day life and also put forward a commitment towards various organizations with smart as well as connected devices. However, there has been a constant challenge to experience cyber-attacks when considering IoT engagement. Deep learning-based methods have been adopted by researchers in recent times to provide a solution and enhance security for this IoT environment (Alsoufi et al., 2021). Even though the deep learning algorithm has succeeded to improve the security system and tackle the challenges in the IoT environment, there have been limitations observed in the signature-based intrusion detection even for zero-day attacks (Alsoufi et al., 2021). Therefore, the consideration of anomaly-based intrusion detection systems has proved to be more efficient and approachable to detect anomalies in network behaviour.

2.2 Machine Learning-based Intrusion Detection System

The intrusion detection system has been used constantly for detecting malicious activities in users' computer systems as well as in the network. When considering this intrusion detection, it explains software which helps in scanning networks and systems to detect distrustful activities. Because of the rapidly growing connectivity among computers, it has become important for the intrusion detection system to enable network activity (Saranya et al., 2020). In this section, consideration has been given to machine learning-based algorithms which have gained much popularity in the past decade in detecting intrusion with the IDS system. Anomaly-based intrusion detection is an optimal approach in recent times due to inefficient results with the signature-based intrusion detection system (Alsoufi et al., 2021). The performance of this IDS method highly depends on the accuracy level where this accuracy is enhanced in reducing the false alarm rates for increasing the rate of detection. Machine learning models such as support vector machine or SVM, decision tree and Naive Bayes have been used in much research and the evaluation has been done on NSL-KDD datasets (Halimaa & Sundarakantham, 2019). The result obtained from the evaluation shows that the SVM approach has more positive outcomes than other classification models and therefore can be used in intrusion detection even in huge network traffic.

2.3 Deep Learning-based Intrusion Detection System

There has been a massive data generation in recent times among different devices as well as communication protocols are increasing security concerns. Therefore, an increased need for developing an advanced or modified intrusion detection system has become mandatory. The anomaly-based intrusion detection system is a convenient intrusion detection process that is used at present to detect network traffic. In this section, the discussion has given attention to the deep learning methods over machine learning due to the high dependency on the latter method of feature selection technique. Compared to machine learning, deep learning can easily integrate huge data and bring success into the detection process (Aldweesh et al., 2020). The deep neural network has been explored by many researchers for developing flexible as well as effective intrusion detection systems (IDS) for detecting and classifying unpredictable cyber-attacks. In recent times with the continuous evolution of network behaviour and the emergence of novel attacks, it has become nearly impossible to evaluate different datasets that have been generated for years by static or dynamic approaches (Vinayakumar et al., 2019). Therefore, the need to adopt a highly scaled IDS system using an advanced framework is necessary for monitoring the network traffic and other events in cyberspace.

Since this section has discussed various approaches to intrusion detection through a deep learning-based model, the above explanation has illustrated a deep neural framework for intrusion detection. The dataset used in the study conducted by (Vinayakumar et al., 2019) is KDDCup-99. The experimental result obtained from the study shows a confirmed high performance with deep neural networks (DNN) in comparison to machine learning classification models. In another study developed by (Almiani et al., 2020), a proposed model has been used with a multi-layered recurrent neural network. The dataset used herein is NSL-KDD and the performance of the model is measured through different metrics. The result obtained shows improved stability as well as robustness based on the performance metrics used for the proposed model.

For the past decade, there has been a wide introduction to both wired as well as wireless network systems due to the deployment of the Internet of Things (IoTs). Huge amounts of

data are enchanted between different devices which thereby increase network traffic and malicious actions. Thus, it has already been discussed how the security system has been enhanced in the past decade through anomaly-based intrusion detection systems. The deep learning models that are classified and used for years in recent times give high accuracies of approximately 99.66% compared to the machine learning classifiers (Kasongo & Sun, 2020). Thus, from the overall discussion, it can be stated that DL-based solutions are more accurate for anomaly-based intrusion detection compared to other classifiers.

2.4 Hybrid Intrusion Detection System

Network attacks have become the most challenging issue in recent times and the vulnerability is highly assembled towards threats to users' computer systems and network. To mitigate the issue, various machine learning and deep learning methods have been adopted to develop essential intrusion detection systems. The development of these new IDS systems can detect malicious threats both automatically and timely. Apart from certain ML and DL-based solutions, researchers have studied other approaches where hybrid classifiers are developed from multiple ML and DL classifiers. In one of the studies conducted by (Khan & Kim, 2020), a hybrid "convolutional recurrent neural network" (CRNN) has been introduced which is developed from both CNN and RNN DL-based framework. The efficacy of the model is determined by experimenting on public ID data collected from CSE-CIC-DS2018 datasets. The simulated outcomes of the proposed model have outperformed other established intrusion detection techniques and shows accuracy of nearly 97.75% for the selected dataset.
Internet of Things or IoT has been considered one of the promising solutions in connecting and accessing devices through the internet. However, due to huge diversification in data size and complexities, a continuous challenging network security issue has risen, making the device vulnerable to network threats. As discussed earlier, apart from several ML and DL classifiers, few hybrid classifiers are also introduced for detecting the network attacks. The most common hybrid classifier introduced is "hybrid convolutional neural network model" (Smys et al., 2020). The model is considered to be a suitable approach in detecting different types of attacks in IoT applications. The research model has been validated as well as compared to existing ML and DL classifiers where the result shows an optimized outcome, given the fact; the model is highly sensitive to the network attacks under the IoT environment.

2.5 Ensemble Intrusion Detection System

The intrusion detection system (IDS) has been considered as the pivotal point in computer security that enables effective discovery as well as repealing of malicious activities within the network system. The anomaly-based intrusion network system typically relies on different classification models which is trained through historical data and helps in discovering the malicious activities. Upon considering the anomaly-based IDS method, various studies have introduced ensemble learning classifiers (Khraisat et al., 2019). In a study conducted by (Tama et al., 2019), a model has been proposed where both "hybrid feature selection technique" and a two-level ensemble classifier has been used in order to minimize the features of the datasets used. For the NSL-KDD dataset, the result obtained shows an accuracy level of 85.8%, thus showing an outperformed simulation compared to other classifiers. For years in the recent decade, several ensemble classifiers have been introduced that have shown effective results with different datasets. The study conducted by (Zhou et al., 2020), has justified the above statement by introducing an ensemble classifier which is a

combination of RF and Forest PA. The outcome obtained from the experiment shows that the ensemble approach has exhibited with better performance compared to previous other approaches under different metrics.

2.6 Other Approaches

The recent approaches to DL and ML-based classifiers in a hybrid or ensemble form in several domains are a highly appreciable consideration. This section has introduced the approaches by various researchers to explore several models in their advanced form. In today's era where ICT technology has made the greatest contribution to mankind, intrusion detection systems (IDSs) served as a greatest potential in network security against the malicious attack in cyberspace; therefore, playing a pivotal role in accomplishing a network infrastructure suitable to perform various internet activities (Khan & Kim, 2020). From various studies it has been established that conventional IDS systems have less potential in detecting the novel attacks of cyber systems. Therefore, new DL approaches such as convolutional autoencoder to detect misuse attack has been developed as an efficient as well as intelligent intrusion detection system. Apart from this other classification such as generative adversarial network is also introduced in recent times as an advanced machine learning (ML) classifier that can detect anomalies with high accuracy (Seo et al., 2018). A study proposed by (Ahmim et al., 2019) has explained about a "novel hierarchical model" for intrusion detection system which is an ensemble of decision tree as well as rule-based models. The experimental result obtained through these approaches provides an outcome which is superior to other "state-of-the-art" models with high accuracy and reduced false-alarm rates.

2.7 Conclusion

The anomaly-based intrusion detection system has gradually optimized the detection process under the recognizable influence of several machine learning (ML) and deep learning (DL) classifiers. Due to limited response towards novel malicious attacks, signature-based intrusion detection is not reliable in recent times where there is a higher degree of network traffic and threats to users' systems. Therefore, in this chapter, several classification models have been discussed through which a specific knowledge has been gathered based on the information. From the overall inclusions, it can be concluded that DL-based classifiers have served higher accuracy compared to ML-based solutions thereby proving more efficient to detect malicious network threats in today's IoT environment.

3 Research Methodology

Technologies are escalated at a rapid rate in the last decade which has resulted in higher use of the internet and intranet-based operable across the various industries, government, and military day-to-day works. This advancement is evolutional but also carries a threat to the security and integrity of the organizations. Intrusions are nothing but steps to carry unusual and unauthorized access to the system. These intrusions affect the integrity of the system and the organizations, such as the leakage of classified documents and other important workflows. In this research project work, the aim is to detect intrusions based on the more

accurate predictions made by advanced deep learning algorithms. The complete workflow to achieve the task is discussed in various sub-sections further.

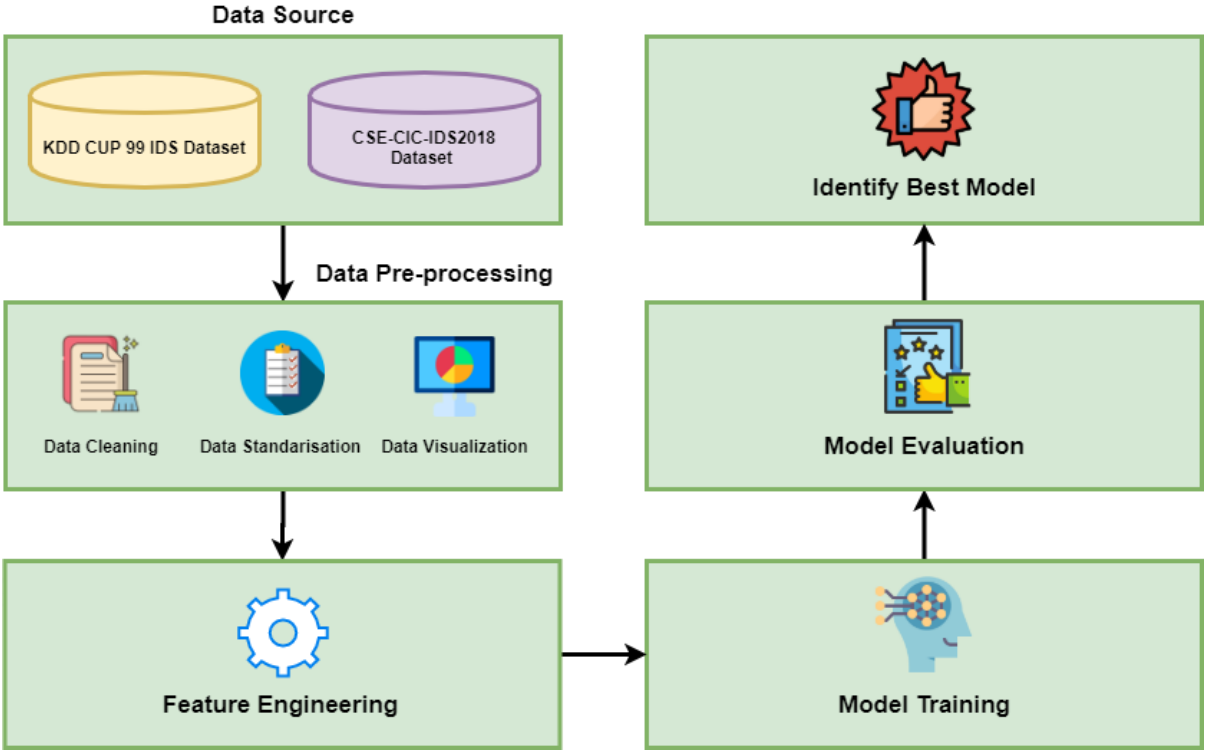

Figure 1 Proposed Methodology for Intrusion Detection System

3.1 Dataset Collections:

Various cybercrimes can be committed through a simple web link. These web links are the intruders and allow to make an intrusion into the victim's system so the intrusions are the first step to committing any cybercrime. Since the application of deep learning algorithms is highly dependent on the quality and the quantity of the dataset therefore a quality dataset with good quantity is important while applying deep learning concepts. In this project work, two datasets are used. Each dataset is collected from a validated data source that provides both quality and good quantity. The first dataset is KDD CUP-99 IDS which is collected from the Kaggle website. This set covers a wide spectrum of modelled incursions into the professional workplace and consistent data that has been audited. Data contains a total of 48,98,431 records and 42 columns. Whereas the label attribute serves as the predicting variable, these 42 attributes provide data on a variety of properties that served as input variables. The total size of data is 753 MB.

As discussed earlier in this task, two datasets are taken under observation because there can be different data sources which can be different so therefore the second dataset is assessed from the University of New Brunswick in order to make predictions on CSE-CIC-IDS2018 data. This authentic data is collected through servers containing Dos invasions for both traffic i.e., forward, and backward traffic. This dataset contains 1048575 records and 80 columns. These large numbers of columns contain information about both forward and backward traffic. In such a large number of columns, the most important columns are Dst Port (Destination port), Protocol, Flow Duration, Tot Fwd Pkts (Total forward packets), Tot Bwd Pkts (Total backward packets), and Label (Label). The size of this dataset is about 400 Mb.

3.2 Data Pre-processing:

The data is gathered from the rightful and undisputed source, but this data is raw in nature. Raw data cannot be inhale directly into the algorithms as this may contain null values, unprocessed features, etc therefore pre-processing is an important step while incorporating deep learning, pre-processing is done to change the data into the necessary format. The first data contains a large number of records that can be processed as these would record large computing resources therefore only 25% of the data is used from the total which is 1266888. While extracting the data it is ensured that minor classes are not dropped After this step, null values are checked and eliminated. The dataset is even further statistically described, and the many labelled attributes are reclassified into the major classes, such as dos, normal, probe, u2r, r2l, etc. Regarding dos, normal, probe, r2l, and u2r, respectively, there are 970670, 243333, 51390, 1425, and 70 distinct values in the labelled column. Some elements are also removed from the label column such as r2l and u2r are quite rare.

The second dataset also contains a reasonable number of rows, but it may contain the null or nan values therefore the null and nan values are eliminated from the data. The Hour column which is in the object data type is changed to Date Time format as per the requirement followed by separating the target and feature columns. After pre-processing the data, the feature engineering is executed on both datasets as discussed in the next section.

3.3 Data Visualization of KDD CUP-99 IDS Dataset (First Dataset):

The input is seen once the cleaning stage has been completed. This representation aids in a thorough interpretation of the data; as a result, deep learning ought to employ it. The frequency numbers of each sort of incursion are displayed in this work's original data, as seen in figure 2. Figure 2 shows that dos incursion frequencies are trailed by normal and probe in terms of priority.

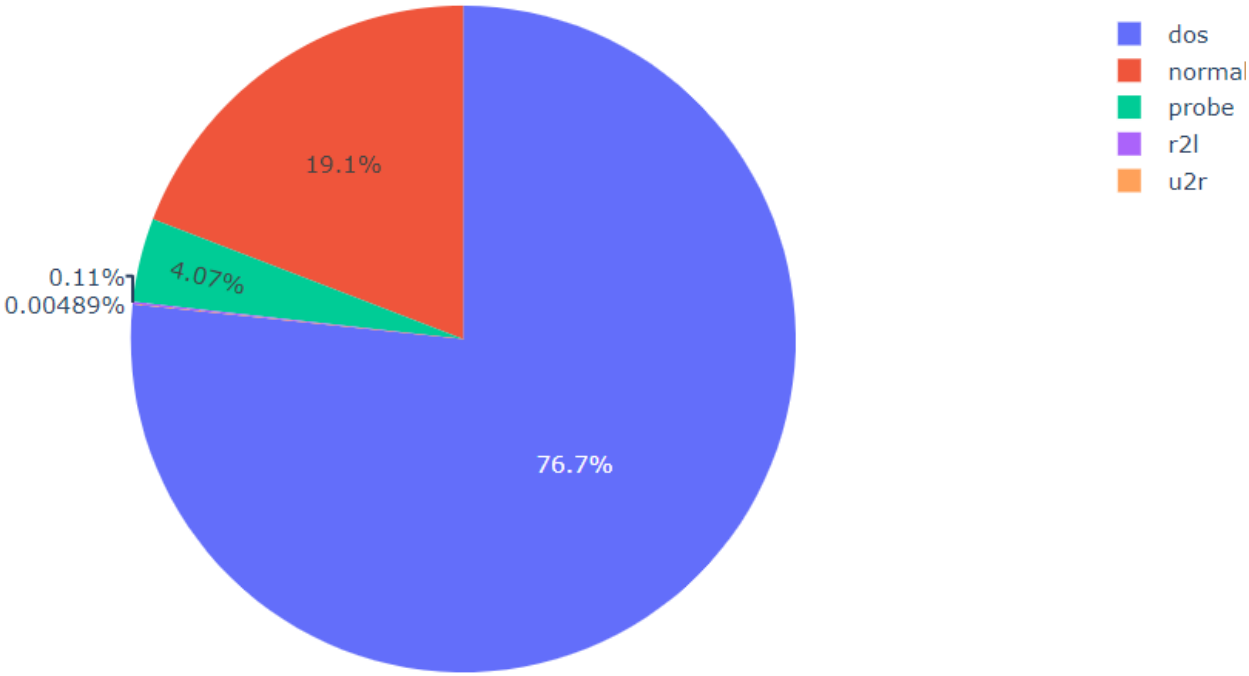

Figure 2 Categories in the Label Feature

The following visualization displays service, protocol, and flag characteristics as bar graphs, as seen in figures 3, 4, and 5 accordingly. The top 10 service elements are represented in the service component plot because they comprise 69 types in total, compared to just three groups for protocol-type elements and 11 groups for flag elements.

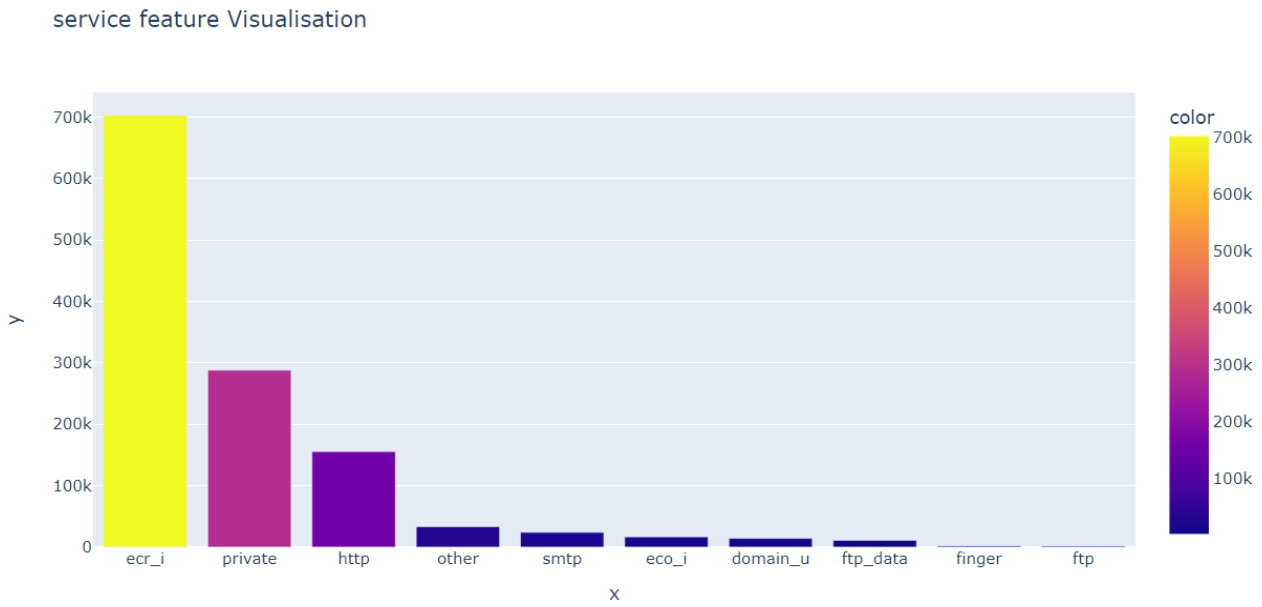

Figure 3 Top 10 categories in service feature

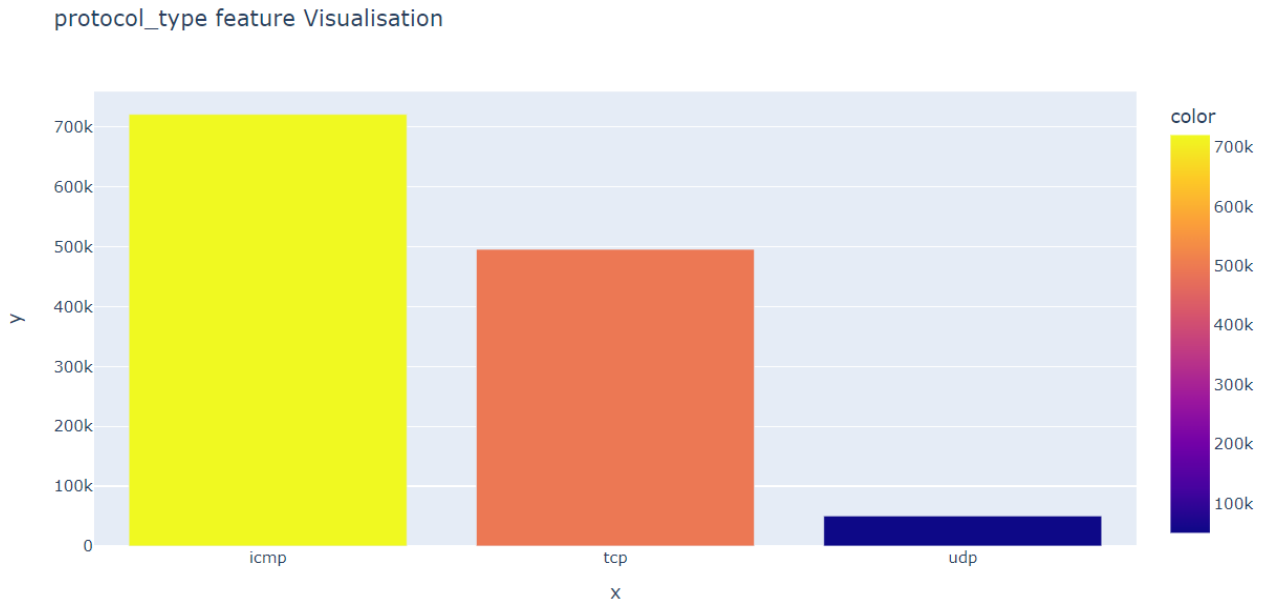

Figure 4 Categories in protocol type feature

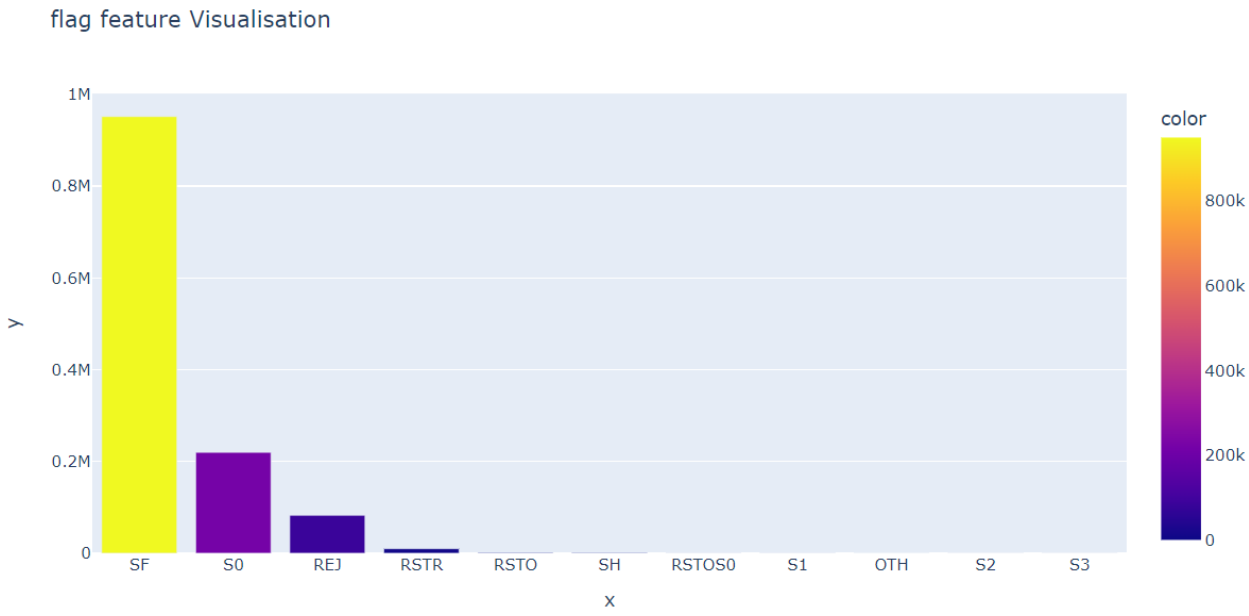

Figure 5 Categories in Flag feature

Figure 6 illustrates a scatter plot for the error rate. This graphic shows that dos intrusion predominates in the serror rate whereas probe intrusion predominates mostly in the rerror rate.

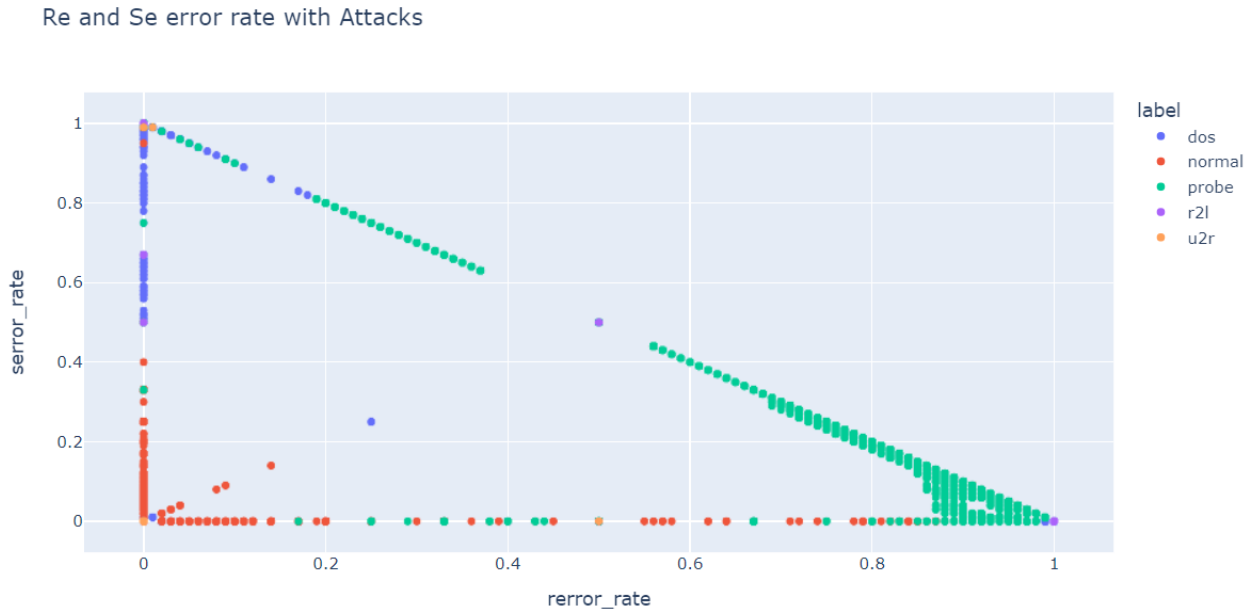

Figure 6 Distribution of types of labels on re and se error rate

3.4 Data Visualisation of CSE-CIC-IDS2018 Dataset (Second Dataset):

In the second dataset, the visualization of the data is executed in order to analyse the data therefore first analysis is made on the number of the Flags raised by the ECE as shown in figure 7. From this figure, we can easily identify that 0.6 M ECE Flags are Benign while the FTP/ SSH Brute force flags are 0.2 M in counts.

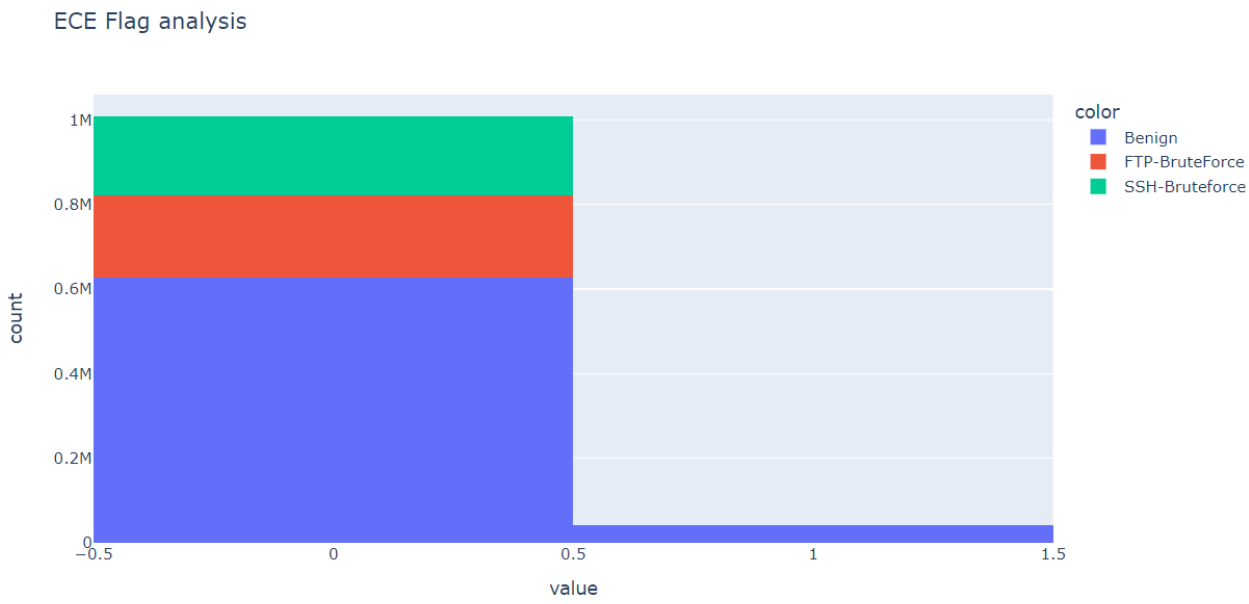

Figure 7 Counts of types of labels

In the next analysis, the hourly count of each class of attacks is visualized as shown in figure 8. This indicates that mostly SSH attacks are in between 2 to 4 Hours while FTP attacks are in 10 to 12 hours.

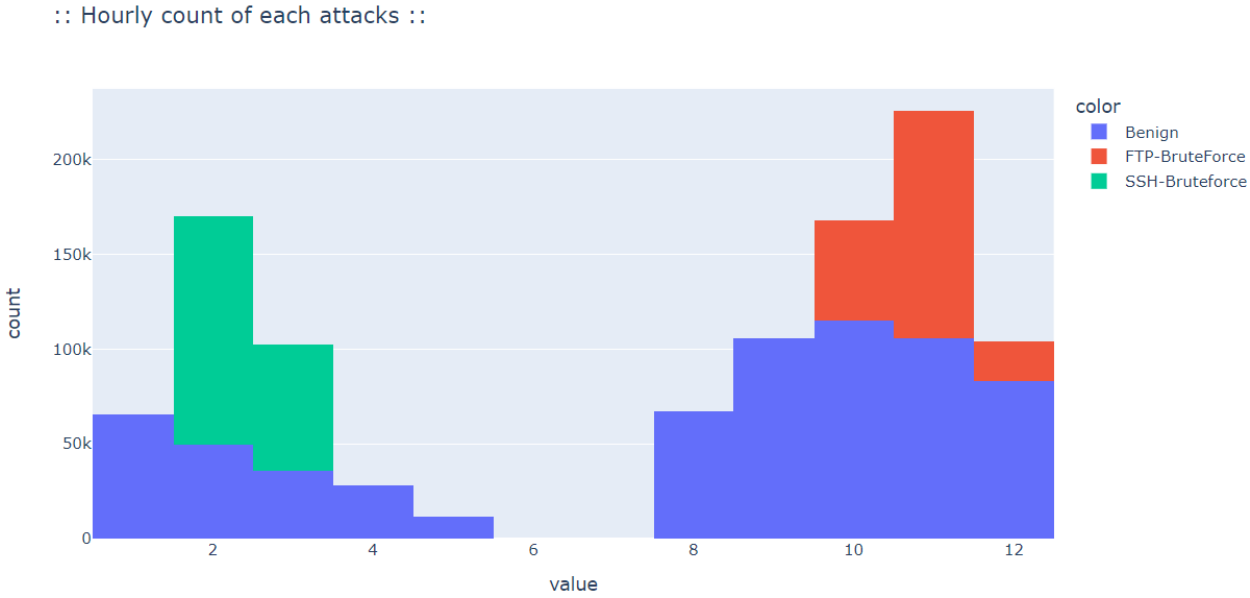

Figure 8 Hourly Count of Each Attack

Next analysis is executed to understand the sub and total flow of forward and backward packets which is shown in Figures 9 and 10. From the figure, it is analysed that there are very few FTP and SSH attacks which exhibits the backward and forward flow of packets. Generally, benign connections exhibit forward and backward packets flow whether it is sub or total.

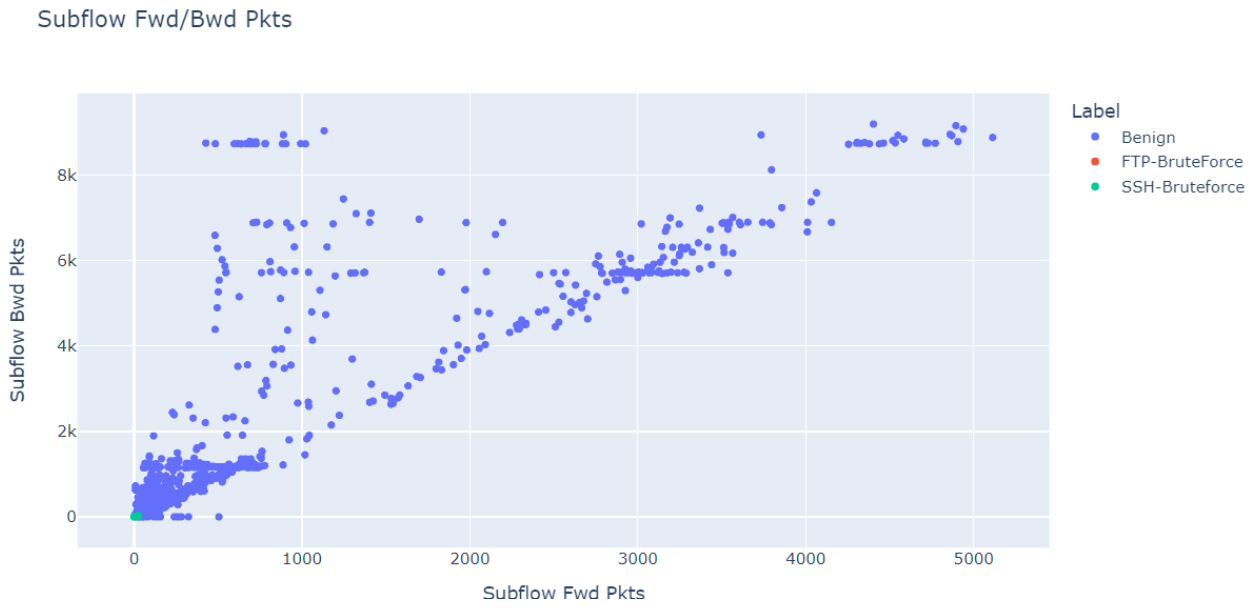

Figure 9 Distribution of Sub flow FWD and BWD packets

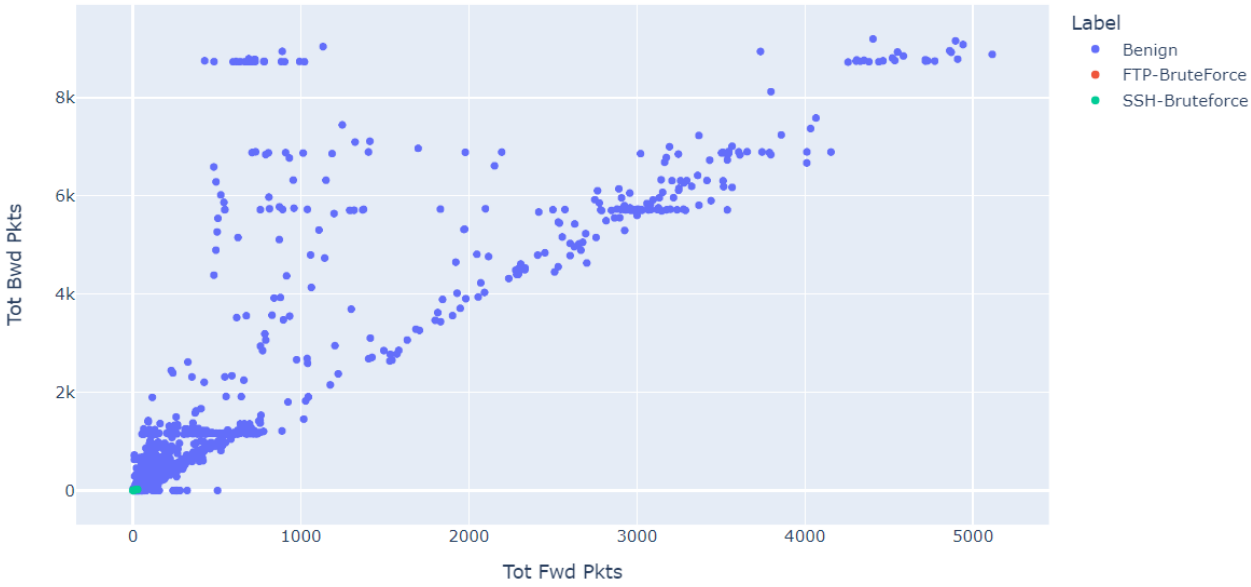

Figure 10 Distribution of Total FWD and BWD packets

3.5 Feature Engineering:

Feature extraction and feature engineering are processes while implementing the deep learning algorithms as the extraction of features having a good correlation with the label column decreases the processing time and the computation resource. This enables the transformation of the columns to a more accurate format. Since the first data contains imbalance therefore random under sampler is applied to balance the dataset. Figure 11 represents the unbalanced classes in the dataset and figure 12 shows the balanced data after the execution of random under sampler. A label encoder is used to transform a categorical column into a numeric form because the data set contains certain categorical elements. One hot encoder is conducted in order to transform the category class of the target column, and restructuring is done as necessary. Standard scalar is used for normalization for the deep learning algorithms.

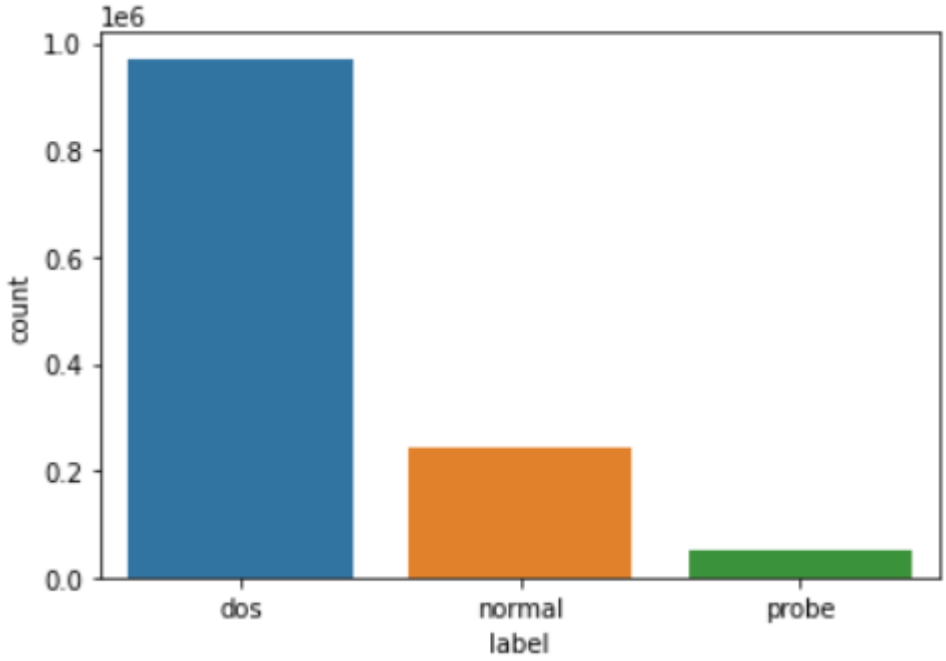

Figure 11 Unbalanced Categories in Label Feature of KDD CUP -99 IDS (Dataset 1)

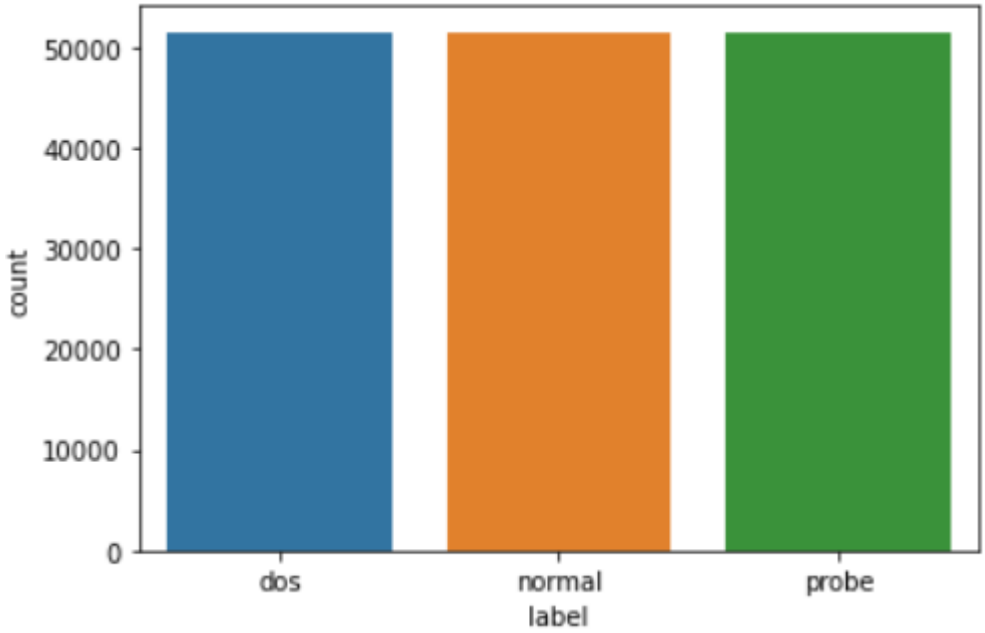

Figure 12 Balanced categories in Label Feature of KDD CUP -99 IDS (Dataset 1)

After pre-processing of the second dataset, feature engineering is performed where first is balancing the dataset if not balanced because it will make a biased prediction. The data contains three class in the target column therefore the under sampled is performed which result in data balancing. The unbalanced data and balanced data are shown in the figure 13 and 14 respectively. Since this data also contains some categorical features therefore the label encoder is executed to make data numerical followed by the application of the min-max scalar in order to normalize the data.

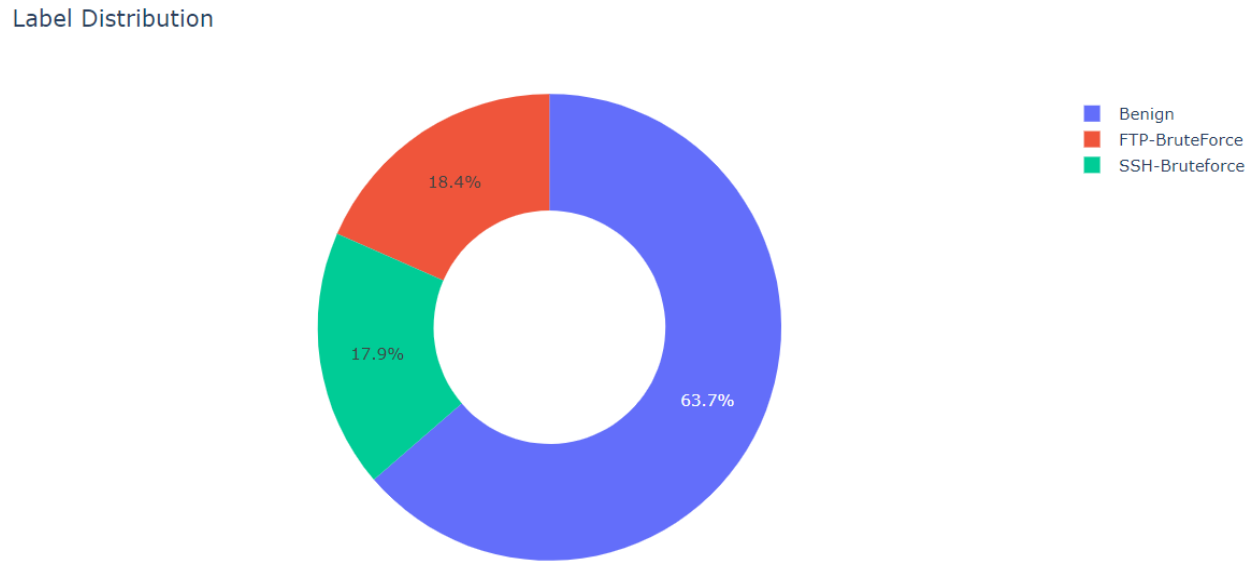

Figure 13 Unbalanced Categories in Label Feature of CSE-CIC-IDS2018 (Dataset 2)

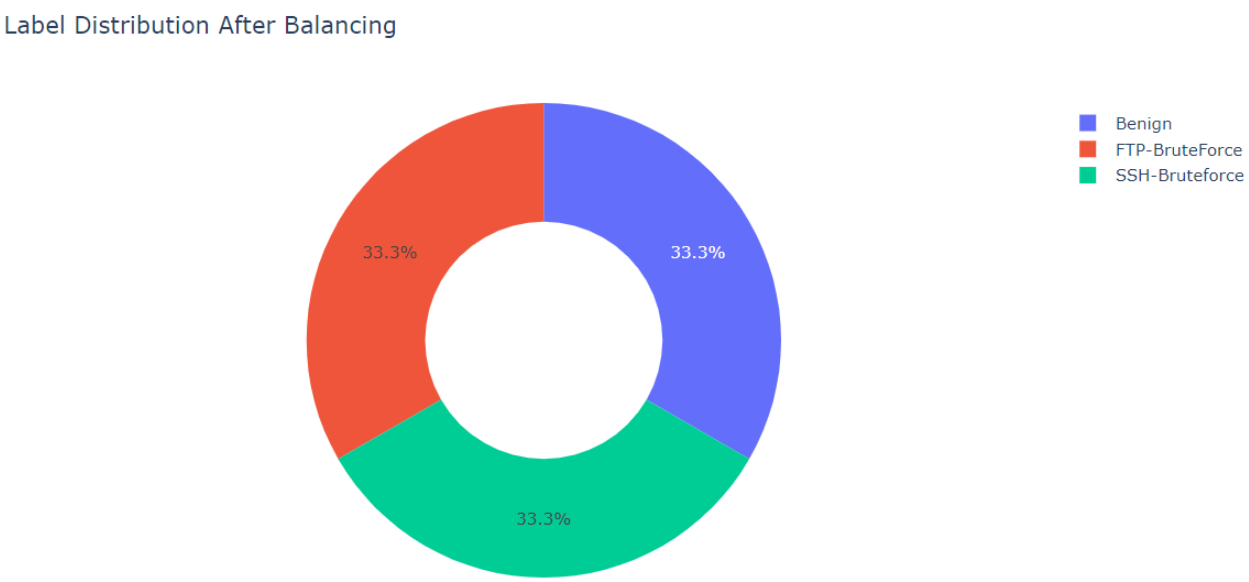

Figure 14 Balanced Categories in Label Feature of CSE-CIC-IDS2018 (Dataset 2)

3.6 Model Training:

After executing the feature engineering and the pre-processing of both datasets, both datasets are divided into the training and the test data at 80% and 20% respectively. In this research work, four different deep learning algorithms are administered for both datasets. These algorithms are Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Convolutional Long Short-Term Memory (Conv-LSTM), and Autoencoders. The training of these algorithms is executed using training data and the validation of the algorithms are executed using test data so that the best-performing algorithm can be identified on a variety of Intrusion data.

3.7 Model Evaluation:

The objective of this research is to identify the most effective deep learning algorithm on both datasets for classifying incoming packets of information in the connection network as either benign information or suspicious activities that attempt to compromise the platform's security. Because of the target variables' multi-class classification challenging nature and the fact that there are greater than two kinds, it is supervised learning. As a result, the classification measures efficiency, precision score, recall score, and F1 score is used to assess each classifier. Every classifier that was developed on the training examples and then deployed to the test set generates these four metrics. The option with the greatest ratings across all measures and one that was effectively executed is the right pick.

4 Design Specification

Three distinct models are used in this research study to construct an efficient system for detecting intrusions utilizing deep learning methodologies. These algorithms are Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), Convolutional Long Short-Term Memory (Conv-LSTM), and Auto-Encoders. Additional subdivisions cover each individual's architecture and fundamental operation.

4.1 Convolutional Neural Network (CNN):

A Convolutional Neural Network is a Deeper Classification algorithm that could feed in an intake picture, give various components and entities in the visual significance (trainable values and biases), and just be capable of recognizing between them. Comparatively speaking, a Convolution requires substantially less pre-processing than most other different classifiers. Convolutional networks have the ability to grasp such filtering and properties, whereas in basic techniques filters are hand-engineered. A Convolutional network structure was influenced by how the Vision Circuit is arranged and is similar to the connection network of neurons located in the human brain. Only in this constrained area of the peripheral vision, termed as the Excel In the field, do neurons react to stimuli. The architecture of this algorithm is shown in figure 15.

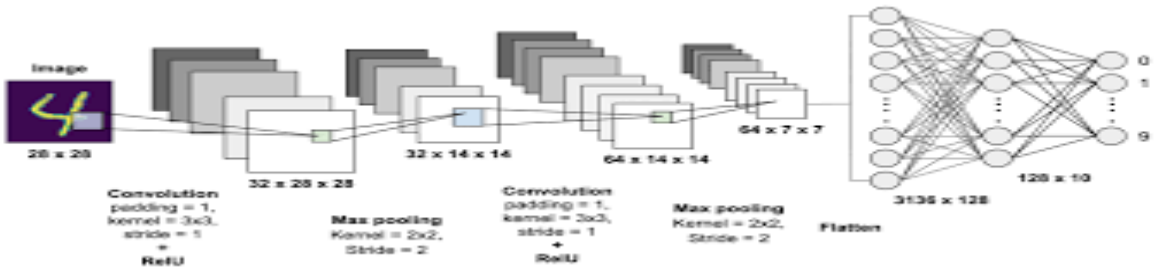

Figure15 Convolutional Neural Network Algorithm

4.2 Long Short-Term Memory (LSTM):

LSTM stands for Long Short-Term Memory Algorithms. It is difficult to build Recurrent Neural Networks (RNNs) with LSTMs. When given a formula as input, LSTM keeps only

the conditions that affect the outcome and discards the rest. When the algorithm generates this data, it is sent in the following format through the LSTM memory cells: If a value is present, it is stored in one of these slots; otherwise, it is ignored. LSTMs solve problems better than RNNs because they know what to remember and what to forget. If the algorithm determines that it is worthwhile, the gate allows data to be stored in memory. When data or words are deemed irrelevant to a result, they are ignored. As a result, the LSTM can recall relevant information. While LSTMs are more powerful and require more processing resources than RNNs, they are slower. The architecture of this algorithm is shown in figure 16.

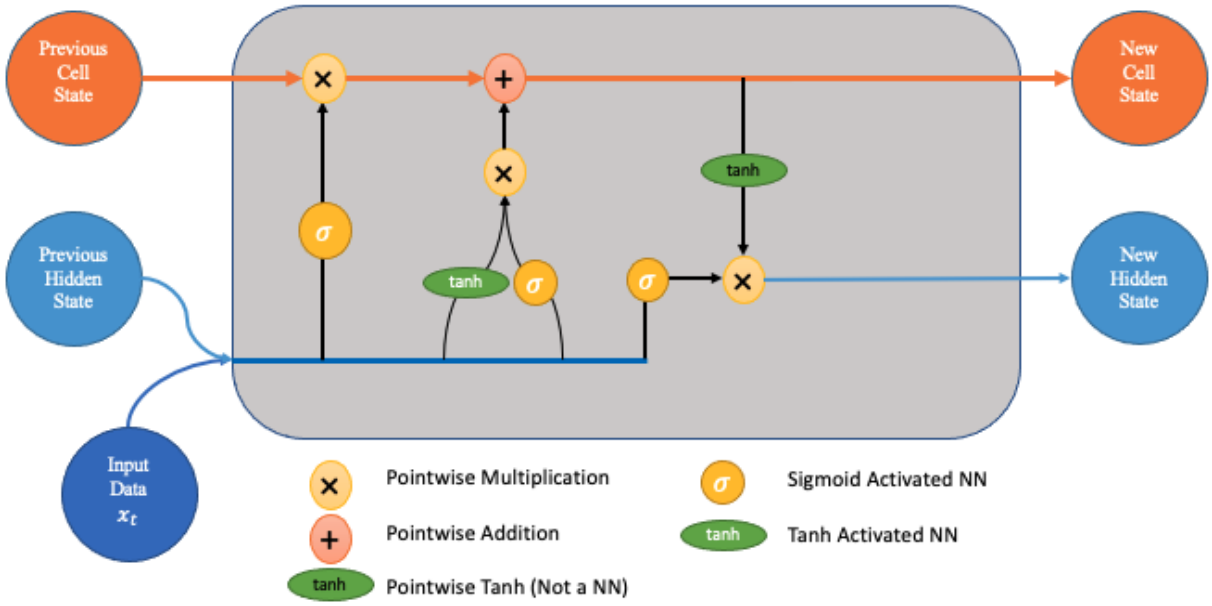

Figure 16 Long Short-Term Memory Network Algorithm

4.3 Convolutional Long Short-Term Memory (Conv-LSTM):

Convolutional-Long-Short-Term Memory Network (Conv-LSTM) is an LSTM architecture designed specifically to solve sequence prediction problems using spatial input arrays such as videos and images. Typically, this architecture includes two network models. H. CNN and Long Short-Term Memory Networks (LSTM). Through a combination of LSTMs that can support sequence prediction, we use CNNs to build specific layers to extract features from the input data. It is intended to generate textual descriptions for image sequences and to establish visual time series prediction problems. As a result, the network architecture can be said to be a real-time solution for various prediction activities, assisting in drilling deeper into problem prediction via visual representation and text mining. The architecture of this algorithm is shown in figure 17.

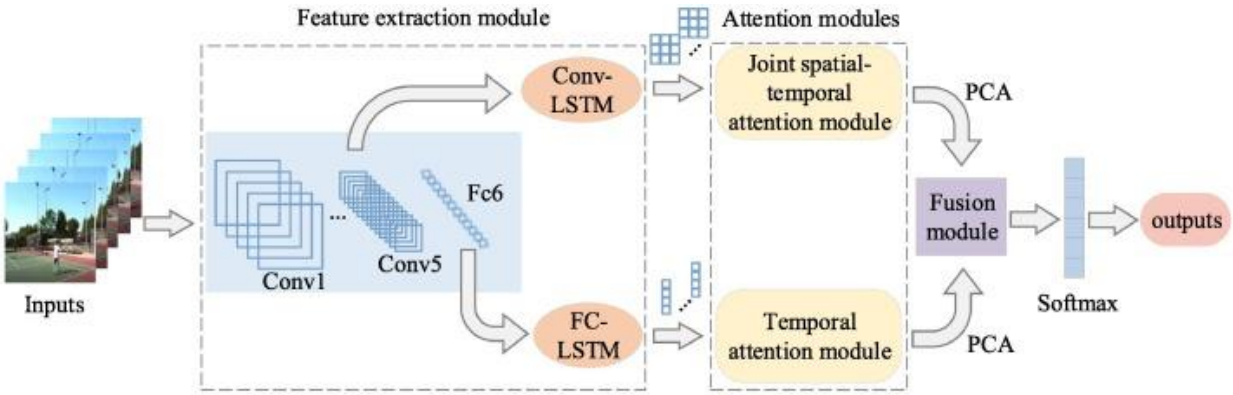

Figure 17 Convolutional Long Short-Term Memory Network Algorithm

4.4 Auto-Encoders:

The inputs and results of neural network models that use autoencoders are generally identical. They reduce the input's dimensionality before using this description to recreate the outcome. The program, also known as the low dimensional, is an efficient "description" or "compaction" of the information. Encoding, coding, and decoding are the three parts of an autoencoder. The information is compressed by the encoder, which also creates a pattern. The decoder subsequently recreates the information exclusively using the format. To create the pattern, the information first goes via the encoder, which comprises a totally ANN. The result is subsequently produced solely from the pattern by the decoder, which has an identical ANN design. Getting a result that matches the source is the aim. Keep in mind that the design of the encoder and decoder are identical. The architecture of this algorithm is shown in figure 18.

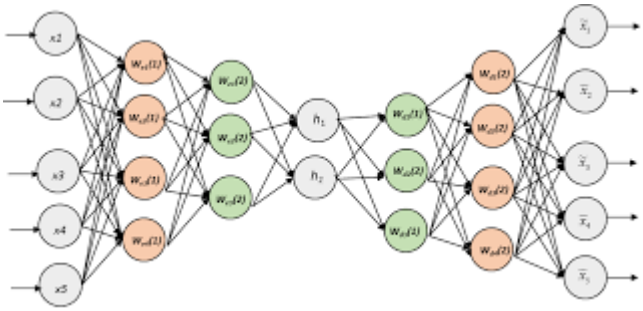

Figure 18 Autoencoders Algorithm

5 Implementation

Intrusions are difficult to identify by brute search and traditional approaches but nowadays machine learning and deep learning approaches have overcome such problems as well providing automated detection to the systems. In this work deep learning is considered to be implemented on the accessed data. Convolutional Neural Networks (CNN), Long- Short Term Memory (LSTM), Convolutional Long Short-Term Memory (Conv-LSTM), and Autoencoders are four deep learning incorporated into this research task. First data is collected, analysed, and transformed followed by the splitting of both data into training and test data. Each model is built using these algorithms and trained on both training data. After complete training of the model, testing and evaluation of the model is executed using both test data. For evaluation purposes, classification metrics such as accuracy, precision, recall, and F1-score. This evaluation enables the identification of the best-performing model. In

order to develop these models' standard libraries are. After developing each algorithm, hyperparameters are tuned using the hit and trial method because deep learning is an iterative process while default parameters are used while first training the algorithms. Evaluation based on different metrics allows the identification of the superficial model after the comparative analysis of the models. This superficial model promises more promising results when applied in real-world scenes. In order to achieve this standard library used are NumPy, Matplotlib, Pandas, Seaborn, Sklearn, plotly, sampling, TensorFlow, and Keras, etc. Programming of the algorithms is implemented using Python. The data used in this research work contains numerical data therefore Anaconda along with Jupyter Notebook is aligned as the framework for the task.

- Operating System (OS): Windows 10
- Random Access Memory (RAM): 16 GB
- Hard Drive: 1 TB
- Programming Language: Python
- Framework: Anaconda
- Platform: Jupyter Notebook
- Standard Libraries: NumPy, Pandas, Matplotlib, Seaborn, Plotly, Sklearn, Imblearn

6 Results and Evaluation

In order to choose the best-performing algorithm which is able to recognize the restrictive interconnection and classify them into multiple categories, dos, probes, and normal, it is crucial to assess the conducted classifiers on various key metrics. This will assist with determining the network packets that encompass the restrictive interconnections, records, or connections. Every algorithm is developed on both training data in order to accomplish this task, which is then assessed using key parameters, including accuracy, precision, recall, and validation loss. The best algorithm is decided upon as the modelling because it achieves the maximum standard of these parameters on the testing data. Here is a discussion of each algorithm's performance on several metrics.

6.1 Experiment 1 / Evaluation Based on the Accuracy

Since the task is a classification task, more clearly a multi-class classification task, therefore, an accuracy metric is implemented first to calculate the obtained accuracy by each algorithm on the first data. Accuracy is generally used to assess how accurate is the prediction made by the classifier while predicting the data into different classes. The same algorithms are implemented on both data to identify the superlative model in various different cases because in real-world applications data sources and systems can be varied.

CNN is the initial classifier to be used, and it is learned from training examples before being tested on the testing dataset. This classifier achieves an accuracy of 99.82%. The LSTM algorithm, which is the second classifier run, employs a similar method, and achieves an accuracy of 99.79% on testing data. The Conv-LSTM approach, the subsequent classifier in the sequence to be run, likewise adhered to the identical testing and training procedures. The accuracy achieved by this mechanism is 97.09%, while the accuracy of the last algorithm used, Auto-Encoders, on testing data was 99.86%. The Autoencoder algorithm achieves the highest level of accuracy among all on the first dataset. The Comparative analysis of executed Algorithms based on accuracy on the first dataset is shown in figure 19.

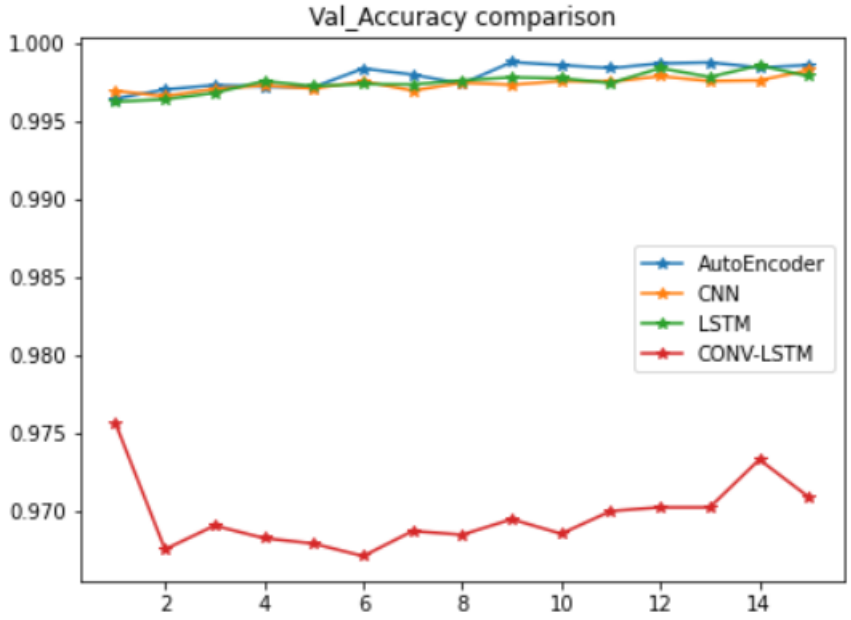

Figure 19 Comparison of Algorithms Based on Accuracy on KDD CUP 99 IDS (Dataset 1)

In the next phase, the second dataset is used for training and testing purposes of the algorithms and the same algorithms are executed on the second dataset. The accuracy achieved by the CNN algorithm, and LSTM algorithm is 59.75% and 57.87 respectively on the test data while the accuracy accomplished by the Conv-LSTM and Auto-encoders is 66.62% and 99% respectively. The foremost accuracy for second dataset is accomplished by Autoencoder. The Comparative analysis of executed Algorithms based on accuracy on the second dataset is shown in figure 20.

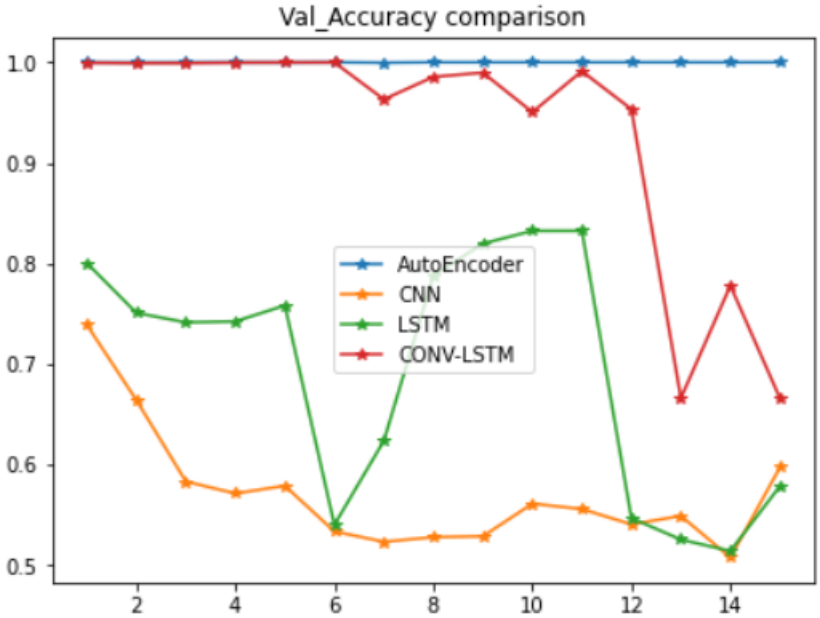

Figure 20 Comparison of Algorithms Based on Accuracy on CSE-CIC-IDS2018 (Dataset 2)

6.2 Experiment 2 / Evaluation Based on the Precision and Recall (PR Score)

Generally, while implementing deep learning algorithms accuracy exhibits the frequency of the algorithm predicting the right classes overall. At the same time, Precision indicates the goodness of the model at predicting the specific class and Recall indicates the frequency of prediction of the specific class by the model. On the first dataset, the precision value obtained by the CNN algorithm on test data is 0.9983 while the precision value of LSTM is 0.9979. The precision value scored by the Conv-LSTM and Autoencoders is 0.9709 and 0.9986 respectively. The Recall value obtained by CNN, LSTM, Conv-LSTM, and Autoencoders on the first data are 0.9982, 0.9979, 0.9709, and 0.9986 respectively. The comparative analysis of the algorithm based on Precision and Recall on the First dataset is visualized below in figure 21.

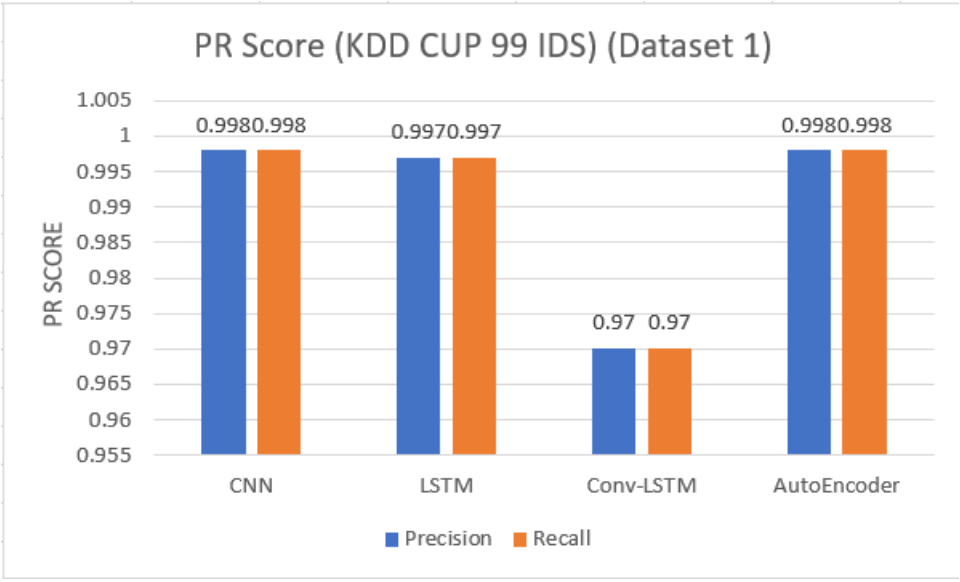

Figure 21 Comparison of Algorithms Based on PR Score on KDD CUP 99 IDS (Dataset 1)

The same algorithms are implemented on the second dataset in the same way as on the first dataset. The precision value obtained by the CNN and LSTM algorithms is 0.99 and 0.98 respectively while the value of precision scored by Conv-LSTM and Autoencoders are 0.66 and 0.99 respectively while The Recall value obtained by CNN, LSTM, Conv-LSTM, and Autoencoders on the second data are 0.26, 0.24, 0.66 and 0.99 respectively. The comparative analysis of the algorithm based on Precision and Recall on the second dataset is visualized below in figure 22.

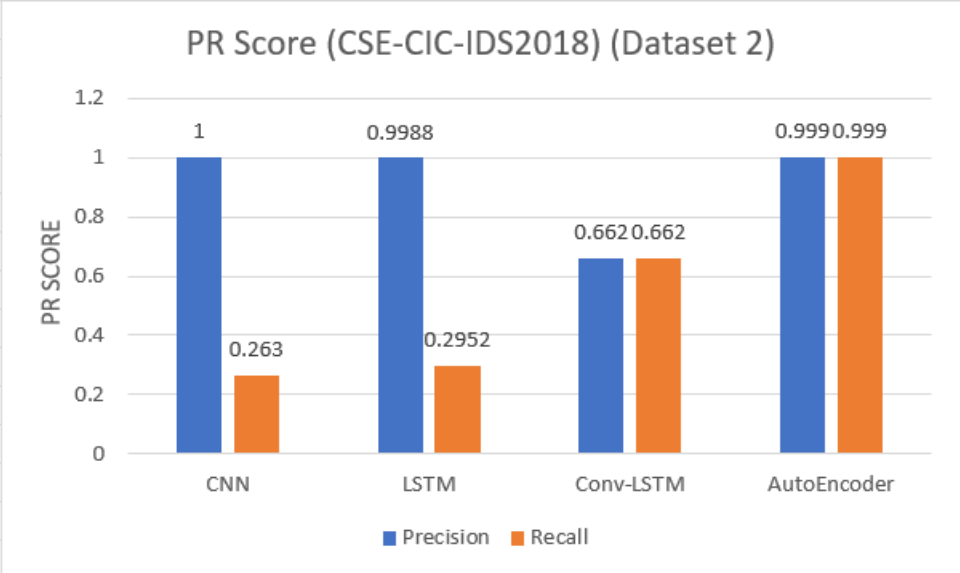

Figure 22 Comparison of Algorithms Based on PR Score on CSE-CIC-IDS2018 (Dataset 2)

.

6.3 Experiment 3 / Evaluation Based on the Validation Loss:

Validation loss is the difference between the predicted and actual value. This loss indicates the training of the algorithm and is a good way to identify whether the model is training in the correct way or not. If the loss increases suddenly and continues to increase which increases that indicates overfitting which is fatal in real-world applications. The first data validation loss on the last epoch of the CNN and LSTM algorithm is 0.0084 and 0.0101while the validation loss of the Conv-LSTM and Autoencoders is 0.0768 and 0.0081 respectively. The comparative analysis of the algorithm based on validation loss on the second dataset is visualized below in figure 23.

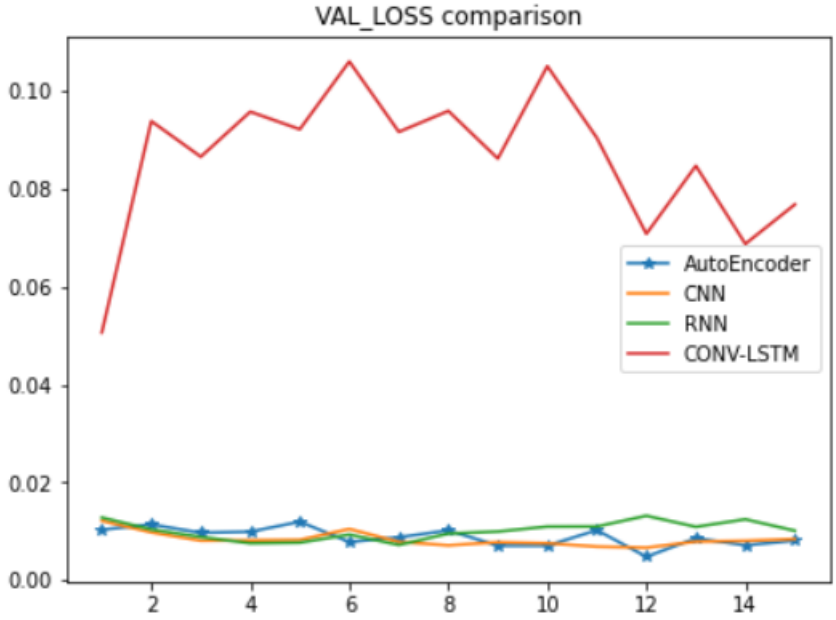

Figure 23 Comparison of Algorithms Based on Validation Loss on KDD CUP 99 IDS (Dataset 1)

On the second dataset, the validation loss accompanied by the CNN, LSTM, Conv-LSTM, and Autoencoders is 0.6935, 0.7340, 0.8423, and 0.00005 respectively. The validation loss of

the Autoencoder is negligible on this dataset. The comparative analysis of the algorithm based on validation loss on the second dataset is visualized below in figure 24.

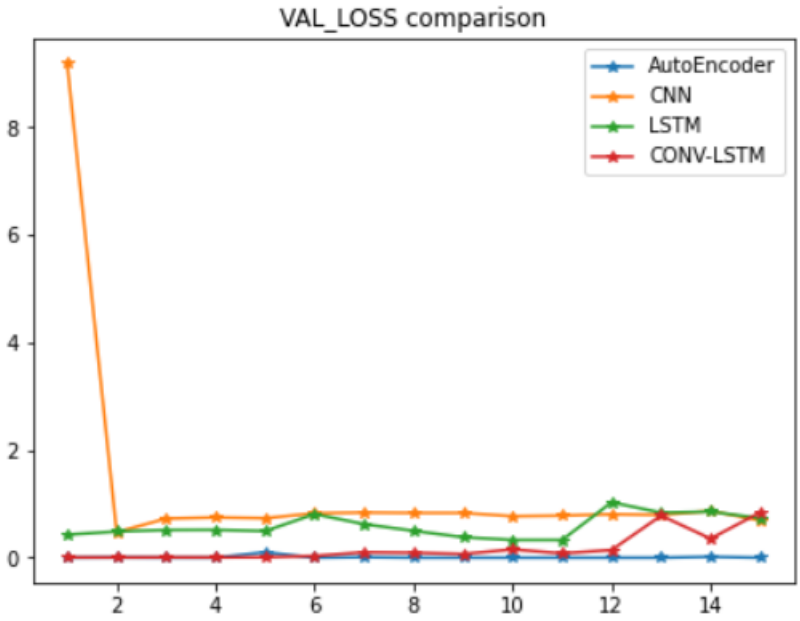

Figure 24 Comparison of Algorithms Based on Validation Loss on CSE-CIC-IDS2018 (Dataset 2)

7 Discussion

The purpose of this task is to figure out the most efficient algorithm on the KDD CUP 99 IDS dataset and CSE-CIC-IDS2018 dataset to sense various invasions done through the connections and data packets. In this task, four experiments are executed on both datasets, and it is found that the Autoencoder algorithm outplaced the other performed algorithms which are CNN, LSTM, and Conv-LSTM on both datasets. It is observed that on the KDD CUP 99 IDS datasets CNN and LSTM algorithm has also shown good results whereas the Conv-LSTM algorithm results are comparable with all other too. This is because the KDD cup dataset is densely populated and applied algorithms are advanced in nature. On the CSE-CIC-IDS2018 dataset, the autoencoder algorithm surpasses all other executed classifiers and this is because the autoencoders are also performed as PCA because Whenever the underlying area has a lower dimension than those of the feed, autoencoders can be utilized to decrease the level of complexity. Intuitively, these lesser latent constructs should hold the most significant attributes as they can reconstruct the inputs. The result of the Autoencoder is adequate and significant. During the training of algorithms, the default hyperparameters are taken and after when the training is complete, every algorithm is estimated on the test precision, test recall, test f1-score, and test accuracy for a better differentiation amongst the performed algorithms. The autoencoder algorithm has displayed good outcomes as on the KDD CUP 99 IDS dataset the accuracy, precision, and recall scores obtained by this algorithm are 99.86%, 0.9986, and 0.9985 respectively while on the second dataset is CSE-CIC-IDS2018 dataset the values are 99.98%, 0.99 and 0.99 respectively which are really satisfying. This model can be further used for good predictions as this prototype attained great results. For the ease of spotting invasions, this prototype can be used for the determination of different invasions.

8 Conclusion and Future Work

Innovation is constantly developing in the civilized era with new and innovative ideas. This change is particularly evident in the growing widespread use of the internet, which demands an especially special perspective. The potential threat that results from the best possible utilization of the electronic state creates unthinkable activity, not just by outside intruders but also by internal usage as a pretentious act or extortion. While analysing the attacks, a system that detects intrusions typically monitors the hosted virtual machine for potential incursion risks. Many computer systems and activity Identifiers that seem to be strongly related to underlying data records are dismissed by host-based solutions. This work will adhere to a machine learning methodology to assess the detection results for deeply scalable knowledge. In order to anticipate and categorize the network packets into matching classes that include maliciously invasive material and linkages, three different machine learning methods are used in this study. As machine learning is used for text categorization increasingly often because the methods are efficient and simple to build, the scope of this area of investigation is growing. In this research study, deep learning advanced algorithms such as CNN, LSTM, Conv-LSTM, and Autoencoders. Each model is created from the scratch and developed in order to find a surpassing model therefore after training the algorithms each is tested on the test data and hence evaluated using different classification metrics. Since it is not always sure that the data source will be the same so here two different datasets are taken which are KDD Cup 99 IDS and CSE-CIC-IDS2018. Each algorithm is trained on both and then evaluated on both datasets which result in the outcome that the Autoencoder Model performed extremely well on both datasets, therefore, being clear for the determination of various data packets into their respective classes in both datasets. This approach is capable of dividing invasive behaviours into their respective classes. In this job, it is shown that the collection is a fair size for the goal, which influences the classification result and results in a decent performance on this information. Future studies will employ the big class categorization approach to recognize intrusions because of the newly created sophisticated intruding behaviours and the breadth of invasion classifications.

References

Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, *32*(1), e4150. https://doi.org/10.1002/ETT.4150

Ahmim, A., Maglaras, L., Ferrag, M. A., Derdour, M., & Janicke, H. (2019). A novel hierarchical intrusion detection system based on decision tree and rules-based models. *Proceedings - 15th Annual International Conference on Distributed Computing in Sensor Systems, DCOSS 2019*, 228–233. https://doi.org/10.1109/DCOSS.2019.00059

Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowledge-Based Systems*, *189*, 105124. https://doi.org/10.1016/J.KNOSYS.2019.105124

Almiani, M., AbuGhazleh, A., Al-Rahayfeh, A., Atiewi, S., & Razaque, A. (2020). Deep recurrent neural network for IoT intrusion detection system. *Simulation Modelling*

Practice and Theory, *101*, 102031. https://doi.org/10.1016/J.SIMPAT.2019.102031

Alsoufi, M. A., Razak, S., Siraj, M. M., Nafea, I., Ghaleb, F. A., Saeed, F., & Nasser, M. (2021). Anomaly-Based Intrusion Detection Systems in IoT Using Deep Learning: A Systematic Literature Review. *Applied Sciences 2021, Vol. 11, Page 8383*, *11*(18), 8383. https://doi.org/10.3390/APP11188383

Halimaa, A. A., & Sundarakantham, K. (2019). Machine learning based intrusion detection system. *Proceedings of the International Conference on Trends in Electronics and Informatics, ICOEI 2019*, 916–920. https://doi.org/10.1109/ICOEI.2019.8862784

Jin, D., Lu, Y., Qin, J., Cheng, Z., & Mao, Z. (2020). SwiftIDS: Real-time intrusion detection system based on LightGBM and parallel intrusion detection mechanism. *Computers & Security*, *97*, 101984. https://doi.org/10.1016/J.COSE.2020.101984

Kasongo, S. M., & Sun, Y. (2020). A deep learning method with wrapper based feature extraction for wireless intrusion detection system. *Computers & Security*, *92*, 101752. https://doi.org/10.1016/J.COSE.2020.101752

Khan, M. A. (2021). HCRNNIDS: Hybrid Convolutional Recurrent Neural Network-Based Network Intrusion Detection System. *Processes 2021, Vol. 9, Page 834*, *9*(5), 834. https://doi.org/10.3390/PR9050834

Khan, M. A., & Kim, J. (2020). Toward Developing Efficient Conv-AE-Based Intrusion Detection System Using Heterogeneous Dataset. *Electronics 2020, Vol. 9, Page 1771*, *9*(11), 1771. https://doi.org/10.3390/ELECTRONICS9111771

Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J., & Alazab, A. (2019). A Novel Ensemble of Hybrid Intrusion Detection System for Detecting Internet of Things Attacks. *Electronics 2019, Vol. 8, Page 1210*, *8*(11), 1210. https://doi.org/10.3390/ELECTRONICS8111210

Li, X. K., Chen, W., Zhang, Q., & Wu, L. (2020). Building Auto-Encoder Intrusion Detection System based on random forest feature selection. *Computers & Security*, *95*, 101851. https://doi.org/10.1016/J.COSE.2020.101851

Liu, M., Xue, Z., Xu, X., Zhong, C., & Chen, J. (2018). Host-Based Intrusion Detection System with System Calls. *ACM Computing Surveys (CSUR)*, *51*(5). https://doi.org/10.1145/3214304

Resende, P. A. A., & Drummond, A. C. (2018). Adaptive anomaly-based intrusion detection system using genetic algorithm and profiling. *Security and Privacy*, *1*(4), e36. https://doi.org/10.1002/SPY2.36

Saranya, T., Sridevi, S., Deisy, C., Chung, T. D., & Khan, M. K. A. A. (2020). Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review. *Procedia Computer Science*, *171*, 1251–1260. https://doi.org/10.1016/J.PROCS.2020.04.133

Seo, E., Song, H. M., & Kim, H. K. (2018). GIDS: GAN based Intrusion Detection System for In-Vehicle Network. *2018 16th Annual Conference on Privacy, Security and Trust, PST 2018*. https://doi.org/10.1109/PST.2018.8514157

Smys, S., Basar, A., Mohammad Bin, P., & Wang, H. (2020). Hybrid Intrusion Detection System for Internet of Things (IoT). *Journal of ISMAC*, *02*(04), 190–199. https://doi.org/10.36548/jismac.2020.4.002

Tama, B. A., Comuzzi, M., & Rhee, K. H. (2019). TSE-IDS: A Two-Stage Classifier Ensemble for Intelligent Anomaly-Based Intrusion Detection System. *IEEE Access*, *7*, 94497–94507. https://doi.org/10.1109/ACCESS.2019.2928048

Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep Learning Approach for Intelligent Intrusion Detection System. *IEEE Access*, *7*, 41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334

Zhou, Y., Cheng, G., Jiang, S., & Dai, M. (2020). Building an efficient intrusion detection system based on feature selection and ensemble classifier. *Computer Networks*, *174*, 107247. https://doi.org/10.1016/J.COMNET.2020.107247