Deep Fraud Detection Model: Firewall Traffic Classification and Rule Generation Using Deep Learning

Pankaj Pandey
Department of Computer Science
Student at Chandigarh University
Mohali, India,
pankajpandey4376@gmail.com

Komal Sharma
Department of Computer Science
Student at Chandigarh University
Mohali, India,
komalsharma6821@gmail.com

Vishav Pratap Singh
Department of Computer Science
Faculty at Chandigarh University
Mohali, India,
vishav.e13056@cumail.in

Abstract- A firewall is a networking security module that controls the flow of packets between internal networks and the outside networks, which follows the firewall rules and based on that, filters the network traffic. To secure the network firewall follows the pre-defined firewall rules and matches with the incoming traffic to establish a secure network and getting harmed by malicious attacks. This paper proposes a solution to the We have demonstrated that recurrent neural networks (RNNs), a subset of deep neural networks, can accurately categorise network traffic into many classes. Recurrent Neural Networks (RNNs) are used in the proposed model to produce optimal output. In this solution we generated a dedicated (RNN) solution that tell the particular firewall is attacked or, not and in this work we successfully achieve an accuracy of 99.9%.

Index Terms – Network Security; Machine Learning; Traffic classification; Artificial Intelligence; Network firewall.

I. INTRODUCTION

An essential component of traffic management, network security, and quality of service (QoS) optimization is deep learning-based network traffic classification. CNNs, or convolutional neural networks, and RNNs, or recurrent neural networks, are two deep learning algorithms that show promise in accurately classifying network traffic patterns. In this introduction, I'll go over the concept and components of a deep learning-based network traffic classification system in detail. The process of classifying and identifying network packets according to their attributes, such as the destination, source, protocol, or payload, is known as network traffic categorization. This is important for several things, such as network monitoring, security analysis, and QoS optimization. Deep learning algorithms provide a reliable method for handling the growing amount and complexity of network traffic data while automating the categorization process.

Gathering and pre-processing the data is the initial stage in developing a deep learning system for classifying network traffic. Usually, network devices or routers record network packets and flows, creating a dataset including information on protocol type, source and destination IP addresses, port numbers, packet length, and payload data. To classify network traffic, feature extraction is essential. From the raw data, deep learning models can automatically identify and extract pertinent characteristics. For instance, RNNs can capture temporal relationships in the sequence of network packets, but CNNs can spot patterns in the packet payload data for classifying network traffic, Long Short-Term Memory (LSTM) networks, CNNs, RNNs, and hybrid models are examples of deep learning models that have proven to be beneficial. RNNs and LSTMs help model sequential data, such as network flows, whereas CNNs are appropriate for spatial analysis of packet payloads.

To train a deep learning model on how to correctly categorize network traffic, labeled data that is, data with predetermined classifications must be used. Typically, this procedure entails the following steps: Data Splitting: To assess model performance, Training, validation, and test sets make up the dataset. Loss Function: A loss function is selected in order to compute the error between the projected and actual classifications. Optimisation: Stochastic gradient descent and other optimisation techniques are used to change the model's parameters and lower the loss. First, the validation set and subsequently the test set are used to evaluate the trained model's performance. Evaluations often make use of measures such as the F1-score, accuracy, precision, recall, and receiver operating characteristic (ROC) curve.

Adjusting hyperparameters like learning rate, batch number, and model architecture may have a big effect on how well the model performs. The model may be used for real-time network traffic categorization once it performs well enough. To categorize traffic on the fly, may include integrating the model with security or network monitoring tools. Since network traffic patterns might alter over time, it is important to continuously monitor and update the model to account for these changes.

Network Traffic Classification

Network traffic categorization is the process of identifying certain applications or activities by matching them with network traffic. For network administration and security, this duty is crucial. Network traffic categorization makes it possible to identify various network application types in network administration, facilitating the proper distribution of network resources. Currently, the two main foci of some early methods of classifying network traffic are port-based and deep packet inspection-based. Network communication identified by specified port numbers in port-based

approaches. However, because port deception and dynamic ports are so common in today's network circumstances, the port-based strategy is starting to lose ground.

The practice of classifying network packets or flows into distinct groups or categories according to a variety of qualities and characteristics is known as network traffic categorization. It is essential to network security, administration, and quality of service (QoS) optimization. I'll go into further depth on the classification of network traffic, its significance, techniques, and applications below:

The significance of classifying network traffic according to security measures is one essential component of network security is the ability to recognize questionable or malicious activity. Security risks like malware, viruses, and DDoS assaults may be identified and countered with the use of accurate traffic classification. In line with Network Management For efficient allocation of resources, traffic molding, and bandwidth control, it is crucial to comprehend the many types of traffic that flow across a network. It aids in guaranteeing QoS and streamlining network performance. According to troubleshooting Traffic classification may be used to identify the root cause of network problems and assist network managers in finding solutions more rapidly. Observance and Documentation Network traffic must be monitored and reported on by several legal obligations and compliance standards. To comply with these regulations, accurate traffic is essential.

Method of network traffic classification

Port-Based Classification: Using port numbers found in network packets, this technique groups traffic. For example, port 80 (HTTP) and 443 (HTTPS) are commonly used for online traffic. However, since non-standard ports used by many current apps, this approach is becoming less dependable. Signature-Based Classification: Techniques based on predetermined patterns or signatures are used to identify certain protocols or applications. This method used by intrusion prevention systems (IPS) and intrusion detection systems (IDS). Deep Packet Inspection (DPI) examines a packet's payload as well as its whole content. Applications and services that utilize non-standard ports can still be identified using this approach. It is frequently utilized for application control, firewall rule regulation, and content screening. Deep Learning: Machine learning and deep learning techniques have the potential to classify network traffic based on previously learned patterns automatically. It is possible to classify data using features like statistical characteristics, payload content, or packet headers. Clustering techniques, decision trees, and neural networks are often used. Behavioral Analysis: Rather than emphasizing certain characteristics, this method focuses on the behavior of network traffic. Malicious conduct may be indicated by anomalies or departures from typical behavior. Systems for detecting intrusions frequently employ this (IDS).

Deep Learning

The aim of artificial intelligence and machine learning is to train deep neural networks to carry out tasks by gaining knowledge from data. These networks, also called artificial neural networks, are named after the several layers of linked nodes (neurons) that process data in the human brain, modeling the structure and operation of the brain. The capacity of deep learning to manage intricate tasks like image recognition, natural language comprehension, and gaming has led to its enormous rise in popularity in recent years. Artificial Neural Networks (ANNs) are computer models that are based on the architecture and operation of real neurons. They are made up of layers of networked nodes, or neurons. Every link has an amount of weight that establishes how strong it is. The neurons process information and then produce an output sent to higher levels. DNNs, or deep neural networks: In deep learning, deep neural networks with several hidden layers sandwiched between their input and output layer is crucial. The network can recognize and convey intricate patterns and correlations in the data thanks to these hidden layers.

Numerous benefits that deep learning provide have elevated it to the forefront of machine learning and artificial intelligence research and applications. Its capacity to automatically recognize and express complex patterns from unprocessed data, hence reducing the need for labor-intensive human feature engineering, is one of its main advantages. Deep learning excels at hierarchical feature abstraction thanks to deep neural networks' many hidden layers, which make it possible to identify both basic and complex data structures.

II. LITERATURE REVIEW

A crucial topic of study in the fields of network administration, security, as well as the quality of service, is network traffic categorization. It entails classifying and identifying network flows or packets into distinct classes or categories according to a variety of features and qualities. Here are few related work done by the researcher R. Liu et al[1] K-means and SVM were used to classify internet traffic according to flow measurements. The authors employed two machine learning techniques. Support Vector Machine (SVM) is a supervised machine learning technique, whereas K-means is an unsupervised machine learning method. To choose the most relevant characteristics, the Data Gain characteristic is selected. Nguyen et al[2] implement ML-based IP traffic classification in active networks. The scope of these classifiers in meeting these criteria was examined by authors, along with several significant requirements for choosing machine learning (ML) traffic classifiers in operating IP networks. Xiangshan Yu et al. [3] Provide a framework for classifying network traffic that uses supervised learning approaches to identify and categorise unknown forms of network traffic. In order to develop a classification model using four machine learning algorithms—C4.5, Support Vector Machine, Bayes Net, and Naive Bayes—ten-fold cross-validation was used in this framework. Y. Xiang et al. [4] offered an NTC model based on statistical flow metrics and IP packet payload. The unsupervised machine learning approach is used to uncover

unknown applications and classify flows into several application-based classifications. The scientists developed a unique cluster aggregation technique by merging related traffic clusters based on the payload composition of each cluster. X. Chen et al.[5] A ground-breaking method for locating zero-day applications is robust statistical traffic categorization (RTC), which integrates supervised and unsupervised machine learning approaches. The first module goal is to identify fresh occurrences of zero-day attacks from amount of unlabeled traffic samples. The next module builds an RTC classifier using pre-labeled training examples and zero-day traffic samples as input. H. Singh et al.[6] examined in-depth the Expectation-Maximization (EM) algorithm and K-means, two unsupervised machine learning techniques, to classify internet traffic according to how near it is to other classes. The boring features are eliminated using the feature selection filter based on correlation to get the candidate feature set's most suitable qualities for categorizing internet traffic. C. Dobre et al.[7] is used as an unsupervised machine learning technique to classify the flows from internet traffic into many clusters. After that, supervised machine learning is used to classify the new traffic. The authors took advantage of statistical features of the network traffic flows, including packet durations, sizes, and inter-packet arrival times. M. A. Pongelupe et al. [8] supplied a framework for spotting network breaches using deep learning techniques as well as a technique for classifying encrypted network data. The suggested approach makes use of three deep learning techniques: convolutional neural networks (CNN), long short-term memory (LSTM), and stacked autoencoder (SAE). CNN is used to understand the fundamentals of network communication. Time-related features are learned through the use of LSTM. T. Shapira et al.[9] suggested that Classification of encrypted communications using deep learning: This method automatically extracts and classifies features from encrypted communication using deep learning models. Models such as convolutional neural networks (CNNs) or recurrent neural networks (RNNs) can be fed the transmission characteristics of encrypted communication to identify and categorize the traffic. S. Choi et al.[10] offered a method for utilising a network flow relationship model to categorise traffic. The suggested model consists of two components: "the similarity model" and "the connectivity model." The suggested technique aggregates related flows and automatically determines the coherence index of the network flows. J. Cheng et al.[11] The similarity measure between the samples was used to partition the network traffic into k-subsets. Using spectral clustering (SC), the raw network data was separated into k-subsets having similar traffic characteristics. The next phase involves using a deep neural network approach to extract relevant information from training data related to intrusion detection. H. Gu et al.[12] Deep learning techniques were applied to give a framework for identifying network breaches and a way to categorize encrypted network data. Long short-term memory (CNN) and stacked auto-encoders (SAE) are both employed. CNN learns the properties of raw network traffic using machine learning.

III. LIMITATION OF NTC

1. Complex and Changing Protocols: A lot of applications use complex and constantly changing communication protocols, such as social networking, online gaming, and video streaming. It is difficult to adjust categorization techniques to these constantly shifting patterns.

2. Imbalanced Datasets: Labelled datasets are usually needed for training when classifying network traffic. These datasets frequently exhibit imbalance, with some classes being disproportionately underrepresented. Models with bias and decreased classification accuracy may result from this.[13]

3. Resource-intensive: For the purpose of traffic classification, machine learning and deep learning models may be very inventive and computationally demanding, requiring substantial quantities of memory and processing capacity. Deploying these models in real-time applications can provide challenges, particularly on devices with limited resources.

4. Privacy Issues: Because network traffic inspection for categorization purposes may entail packet content analysis, privacy issues may arise. Ensuring privacy compliance is crucial, particularly when transmitting sensitive or personal data.[14]

IV. PROPOSED SOLUTION

The project traffic classification for firewall rule generation, Provides an exhaustive deep learning (DL) based framework. which is a high-level programming interface used for making decisions about the firewall present in the network for the enhancement of security and better communication between the server and the devices. The flowchart is being prepared for research from the initial stage to the result. **Fig.1** demonstrates the four-state module which are Data classification, model learning, data preparation, and data collection. The study paper discusses these modules in the section below. [15]

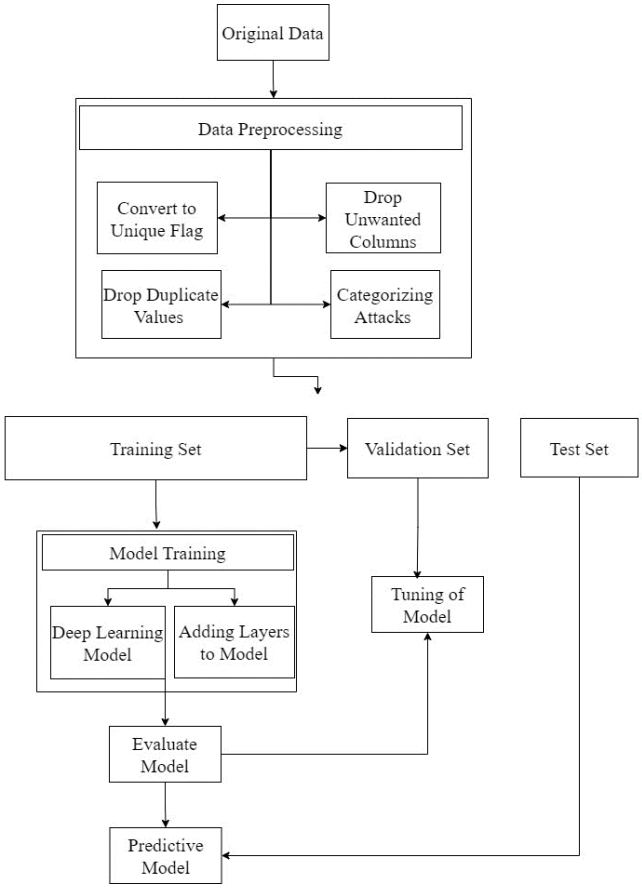

Figure 1: Projected model

A. Data Collection

In the Data collection phase of this research, the primary focus was on gathering comprehensive and diverse network traffic data to facilitate the subsequent stages of the study. The dataset chosen for this purpose was CIDDS-002, a well-known and esteemed dataset in the cyber security space. CIDDS-002, curated and maintained for research purposes, provided a rich repository of real-world network traffic scenarios. By leveraging this dataset, we ensured the inclusion of various network activities, encompassing both normal and malicious behaviors, essential for the robustness of our analysis. This meticulous selection aimed to capture the intricacies of modern network communication, enabling our study to be grounded in real, representative data. The process of data collection laid the foundation for the subsequent steps in our methodology, guaranteeing the validity and applicability of our results in the context of traffic categorization for the creation of firewall rules.[16]

CIDDS-002, a pivotal dataset in evaluation anomaly-based network intrusion detection systems, was meticulously crafted by emulating a small business environment through OpenStack technology. This emulation encompassed diverse clients, including E-Mail and Web servers, replicating real-world scenarios. To ensure authenticity, Python scripts were employed to simulate typical user behaviors on these clients. The dataset is exclusively composed of unidirectional Net Flow data, supplemented with additional attributes (11 to 14) introduced during the labeling process, enhancing its depth and accuracy. Because of its careful design, CIDDS-002 is an invaluable tool for researchers studying anomaly-based security techniques and network intrusion detection systems. It provides a wealth of information for in-depth investigation and study.17]

B. Data Preparation

In traffic classification for the firewall rule generation, data preparation is foundational. This phase involves refining raw data for analysis and modeling. It includes cleaning, structuring, and standardizing datasets, rectifying inconsistencies, and handling missing values. Rigorous pre-processing ensures data quality, a prerequisite for meaningful analysis and accurate modelling. The effectiveness of the entire traffic classification model hinges on the precision of this vital data preparation stage.[18]

- Data Transformation

In dataset CIDDS-002 the records are provided in the form of a for this research, two files, i.e., CIDDS-Week-1 and CIDDS-Week-2, are used, where rows denote individual data samples and columns represent various features, separated by commas. To facilitate seamless integration into our MATLAB development platform, Keras, a crucial transformation step is initiated. This transformation process involves converting the raw .csv data into a double matrix format. By executing this conversion, the dataset becomes compatible with the MATLAB system, enabling efficient and accurate calculations, as well as facilitating subsequent Deep Learning processing. This essential transformation ensures the dataset is prepared for in-depth analysis and model training, laying the foundation for robust traffic classification and firewall rule generation without compromising data integrity or accuracy.[19]

- Data Labelling

In the CIDDS-002 dataset, a diverse array of features is presented, encompassing various data types including integers, floats, and categorical variables. To facilitate comprehensive analysis and effective utilization of this dataset, a pivotal step involves the conversion of these diverse data types into a unified numerical format. This transformation is essential for standardizing the data, enabling seamless integration into deep learning models. Employing advanced deep learning techniques, the class labels within the dataset have been carefully examined and categorized into distinct classes: 'normal,' 'attacker,' and 'victim'. The label class is shown in the fig. [20] Through the fusion of sophisticated deep learning techniques and precise labeling strategies, the CIDDS-002 dataset becomes an asset in the realm of cyber security, empowering researchers, and practitioners to navigate the intricate landscape of network traffic analysis with confidence and precision.

TABLE I : TYPES OF ATTACKS AND PERCENTAGE

	Absolute Frequencies	**Percentage**
Normal	10112095	0.955141

Attacker	314293	0.029687
Victim	160625	0.015172

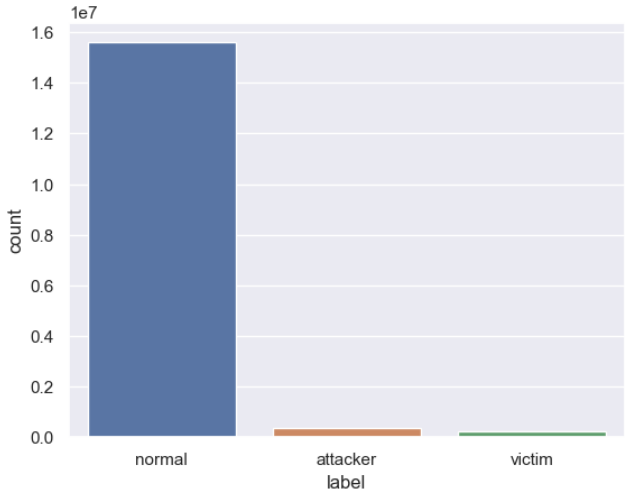

Figure 2: Types of Attack

- Feature Extraction

During the Data Collection phase of the approach, the efficacy of the traffic categorization system is significantly shaped by feature extraction. For this research, the dataset CIDDS-002 is being used to serve as a rich source of network traffic data. Feature extraction involves identifying and selecting relevant characteristics from the CIDDS-002 dataset, they are essential to the training and improvement of the research paper's deep learning models' performance. Features like packet size, protocol type, source and destination IP addresses, and port numbers were meticulously collected through thorough analysis.[21] These features serve as the fundamental building blocks, capturing the intrinsic patterns within the network traffic. By utilizing advanced techniques and algorithms of deep learning, The deep learning models are able to identify complex patterns and correlations within the data thanks to these extracted features, which offer insightful information. This meticulous process of feature extraction ensures that the subsequent stages of the research, including model learning and data classification, are built upon a robust foundation, enhancing the accuracy and efficiency of firewall rule generation for traffic classification.[22]

- Data Splitting

In the Data Splitting stage, the CIDDS-002 dataset is carefully separated into discrete subgroups to guarantee an objective depiction of the entire dataset. This phase is essential for the traffic classification model's resilience and dependability. This research was able to reliably evaluate the model's performance by splitting the dataset into training, testing, and validating the datasets at random. With 70% and 30% of the data being utilised for training and testing sets, respectively, a substantial amount of the data is being utilised, which enables our deep learning algorithms to identify complex patterns and correlations in the traffic data. 20% data of each set are taken for validation. Employing this strategic data-splitting approach enhances the generalizability of our results, making them applicable to real-world scenarios, and ensuring the effectiveness of the firewall rule generation system we propose.[23]

C. Model Learning

In the Model Learning step, the CIDDS-002 dataset was utilized as the foundational data source, comprising a diverse range of network traffic samplesThis stage included implementing two well-known deep learning architectures: Recurrent Neural Network (RNN) and Long Short-Term Memory (LSTM) using cutting-edge methodologies. To facilitate effective training, the dataset was meticulously categorized into three distinct class labels: normal, attacker, and victim. By employing these sophisticated models and employing a three-label classification system, the research aimed to accurately classify network activities, enabling the development of precise firewall rules tailored to different types of network behavior.[24]

- LSTM (Long Short-Term Memory)

One major development in the field of traffic categorization for firewall rule generation is the use of networks with long short-term memory (LSTM). neural networks with recurrence (RNNs) of the LSTM type are excellent at gathering and processing sequential input, which makes them very useful for studying the dynamic patterns present in network traffic.[25] In addition to addressing the difficulties brought about by changing network behaviors, this integration aims to maximize firewall systems' effectiveness in recognizing and handling a variety of traffic kinds. The ensuing discussion elucidates the architecture, training methodologies, and potential benefits of incorporating LSTM into the traffic classification framework, shedding light on its role in bolstering the effectiveness of firewall rule-generation processes. [26]

D. Data Classification

To execute and implement the output, we have used multiclass classification such as the Sequential Model. We have solved the problem using the Sequential Model (SM) for classifying the dataset CIDDS-002. For the classification of the dataset, a class label is used which contains normal, attacker, and victim as their values. [27]

Formally, the sequential model is specified as a 5-tuple.

SM = {{Xi}, C, O, {fi}, {i}}

Whereas,

- The domain is decomposed as X=UNi=1Xi..
- The collection of class labels is denoted by C.
- To make things easier, we indicate the sequence in which the classifiers are assessed and trained as O={o1,o2,....., oN}. f1 = fo1, f2 = fo2,...
- The collection of classifiers that the model uses is denoted by {f1}N1: fi : (Xi, 2|C|) →[0,1]|C|.
- {€i}The constant thresholds in N1 are a set.

V. RESULTS AND DISCUSSION

The dataset CIDDS-002 is being utilized for the research to optimize the output produced and assessed by the deep learning model for the Traffic categorization for firewall rule creation. “Normal”, “Attacker” and “Victim” are the three class labels used for predicting the attacks that performed by the attacker 0or legitimate user. The task is carried out in a high-end PC with modern deep learning techniques such as LSTM and RNN in which a sequential model is adopted for creating the layers in the deep learning which is shown in Table 2. Visual Studio code is used as an IDE along the Anaconda Navigator is used for managing the libraries. [28] To train and test the dataset, it has gone through a series of pre-processing techniques and significantly reduced the memory usage of the data frame.

TABLE 2: SEQUENTIAL MODEL OF LAYERS

Model: "sequential"		
Layer	Output Shape	Params
LSTM (LSTM)	(None, 13, 40)	10300
Dropout (Dropout)	(None, 13, 40)	0
LSTM_1 (LSTM)	(None, 13, 40)	20300
Dropout_1 (Dropout)	(None, 13, 40)	0
LSTM_2 (LSTM)	(None, 13, 40)	20300
Dropout_2 (Dropout)	(None, 13, 40)	0
LSTM_3 (LSTM)	(None, 40)	20300
Dropout_1 (Dropout)	(None, 40)	0
Dense (Dense)	(None,1)	51
Total params: 71,061 **Trainable params: 71,061** **Non-trainable params: 0**		

To analyze the traffic in the firewall dataset CIDDS-002, the major ports which are used for the transferring of packets through source and destination ports are ports: 443, 80, and 53. In this port which is majorly used open ports are usually used for establishing the connection between the users and the servers.[29] The used ports for this research are shown in the **fig 3 and fig 4.**

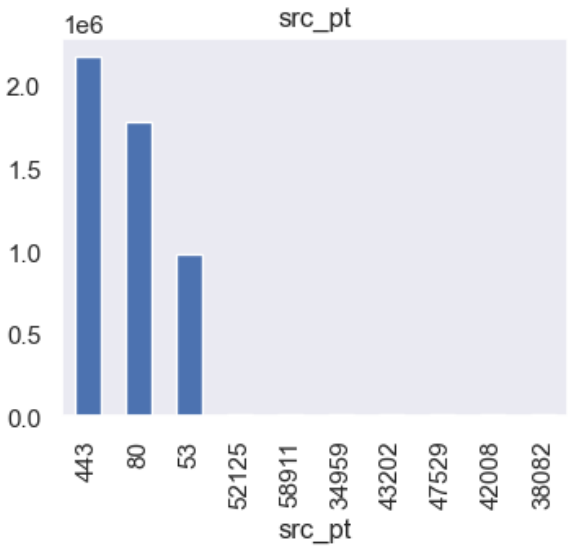

Figure 3: Major Source Ports

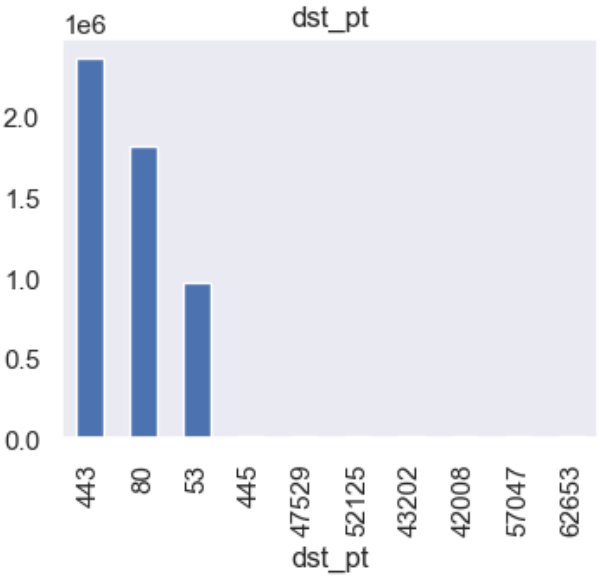

Figure 4: Major destination ports

In addition, **fig 5** shows the histogram of the protocols used in the CIDDS-002 dataset.[31] For viewing the histogram seaborn library is used, and the protocols TCP, UDP, ICMP, and IGMP are the four categories into which the utilized dataset is separated.

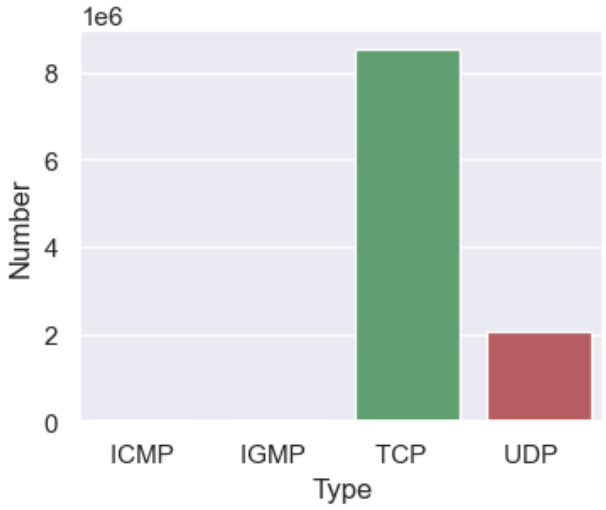

Figure 5: Types of protocols

In training the model using Recurrent Neural Network (RNN) the dataset after pre-processing, is randomized. Through each run of the epoch from 1 to 7 the loss gradually decreases with the increase in approach. The training and validation loss can be plotted with the epoch in the **fig 6.**

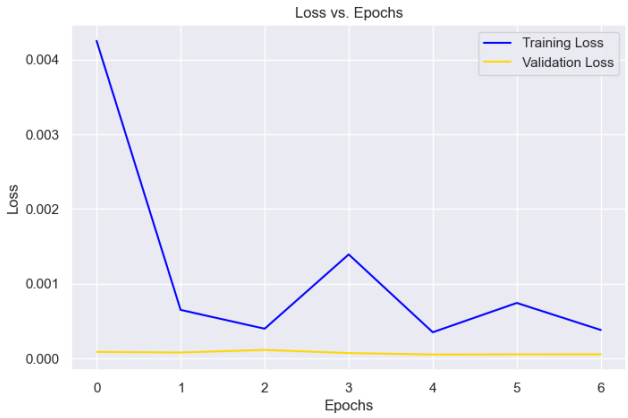

Figure 6: Loss vs Epochs

As from the above table, we analysed our model 'Traffic classification for firewall rule Generation' with the dataset CIDDS-002.Our model is evaluated using the improvement percentage (IM) and contrasted with the other machine learning model. and got an improvement range from ≈ (0.2 to 2.98).[13] The improvement percent (IM) can be derived from the formula from our model to the existing model's accuracy:

$$IM\,\% = \left[\left(\frac{Our\ model\ accuracy}{Other\ model\ accuracy} \times 100\right) - 100\right]\%$$

Finally, from this Research we benchmark our model Traffic classification for firewall rule generation with another model of machine learning from our deep learning-based classification system.[30] The comparisons are listed in **table 3.**

TABLE 3: COMPARING OUR MODEL WITH PREVIOUS MODELS

Research	Year	Techniques	Accuracy	IM %
M.A. Pongelupe	2019	Modified Naïve Bayes technique with relaxation for the hypothesis of attribute independence.	98.88%	1.03%
T. Nguyen	2008	Expectation Maximization, DecisionTree, Naïve Bayes	99%	0.909 %
T. Shapira	2019	Convolutional neural network	99.7%	0.200 %
A. Almomani	2022	Neural networks, support vector machines, and random forests	99	0.909 %
T. Ma	2016	Spectral clustering, deep neural network	97%	2.989 %
Our Model	2023	LSTM, Recurrent Neural Network	99.90%	

VI. CONCLUSION

Ultimately, this study explores the crucial process of traffic classification using deep learning approaches for firewall rule creation. We have shown how well these models operate at properly classifying network traffic into distinct groups by utilising the capabilities of recurrent neural networks (RNNs) and deep neural networks. To achieve the best output, the designed model uses a recurrent neural network (RNN), which takes in 14 characteristics for processing and uses three class labels to categorise the deep learning model. The model is being trained using 70% of the data. Twenty percent of the training data is used for model validation, and thirty percent of the data is used for testing. To obtain the model's accuracy, the model is properly trained and obtained a maximum output of 99.90% using the Recurrent Neural Network (RNN). The proposed approach not only outperforms traditional rule generation methods but also showcases its adaptability to evolving network landscapes. The ongoing pursuit of enhancing firewall rule generation is crucial for maintaining the integrity and resilience of digital networks in the face of ever-evolving cyber threats.

VII. FUTURE SCOPE

1. Provide techniques for generating firewall rules that will allow security policies to be seamlessly coordinated across many cloud environments. This entails formulating regulations that may be adjusted to accommodate various cloud infrastructures, guaranteeing a uniform security stance irrespective of the cloud provider.

2. Quantum computing may affect cryptography methods and create firewall rules that can withstand attacks from this new technology. In the post-quantum computing future, this forward-looking strategy will contribute to ensuring that firewall security remains effective.

3. Sync the creation of firewall rules with the Zero Trust security model's tenets. This entails applying least privilege access rules, requiring authentication and authorization for each network transaction, and regularly assessing the security posture of people and devices.

4. Adopt firewall rules that are user-centric and consider the unique requirements and responsibilities of each user on the

network. To provide more granular control based on user traits, this may include integrating user identity and access management into the firewall rule creation process.

VIII. REFERENCES

[1] Z. Fan and R. Liu, "Investigation of machine learning based network traffic classification," Proc. Int. Symp. Wirel. Commun. Syst., vol. 2017-Augus, pp. 1–6, 2017

[2] T. Nguyen and G. Armitage, "A survey of techniques for Internet traffic classification using machine learning", IEEE Communications Surveys & Tutorials, Vol. 10, No. 4, fourth quarter 2008, pp 56-76

[3] Muhammad Shafiq, Xiangshan Yu, Lu Yao, N abin Kumar Karn, Foudil Abdessamia, "Network Traffic Classification Techniques and Comparative Analysis Using Machine Learning Algorithms", 2nd IEEE International Conference on Computer and Communications,2016, pp2451-2455.

[4] J. Zhang, Y. Xiang, W. Zhou, and Y. Wang, "Unsupervised traffic classification using flow statistical properties and IP packet payload," J. Compute. Syst. Sci., vol. 79, no. 5, pp. 573– 585, 2013

[5] S. Member, Y. Xiang, J. Zhang, X. Chen, "Robust Network Traffic Classify.," IEEE/ACM Trans. Netw. (TON), 23(4), pp.1257-1270, pp. 1–14, 2014

[6] H. Singh, "Performance analysis of unsupervised machine learning techniques for network traffic classification," Int. Conf. Adv. Compute. Commune. Technol. ACCT, vol. 2015-April, pp. 401–404, 2015.

[7] A. Vlăduţu, D. Comăneci, and C. Dobre, "Internet traffic classification based on flows' statistical properties with machine learning," Int. J. Netw. Manag., vol. 27, no. 3, p. e1929, May 2017

[8] K. L. Dias, M. A. Pongelupe, W. M. Caminhas, and L. de Errico, "An innovative approach for real-time network traffic classification," Compute. Networks, vol. 158, pp. 143–157, 2019.

[9] T. Shapira, Y. Shavitt, in IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). FlowPic: encrypted Internet traffic classification is as easy as image recognition. (Pairs, France, 2019), pp.680–687

[10] Y. H. Goo, S. H. Lee, S. Choi, and M. S. Kim, "A traffic grouping method using the correlation model of network flow," 19th Asia-Pacific Netw. Oper. Manag. Symp. Manag. a World Things, APNOMS 2017, no. Group 0, pp. 386–390, 2017.

[11] T. Ma, F. Wang, J. Cheng, Y. Yu, "A hybrid spectral clustering and deep neural network ensemble algorithm for intrusion detection in sensor networks," Sensors (Switzerland), vol. 16, no. 10, 2016.

[12] Y. Zeng, H. Gu, W. Wei, "Deep-Full-Range: A Deep Learning Based Network Encrypted Traffic Classification and Intrusion Detection Framework," IEEE Access, vol. 7, no. ML, pp. 45182–45190, 2019.

[13] A. Javaid, Q. Niyaz, W. Sun, M. Alam, "A Deep Learning Approach for Network Intrusion Detection System," in Proc. Of 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS), NY, USA, 24 May 2016; pp. 21-26.

[14] Laurie Hughes, A.M. Baabdullah, Denis Dennehy, Bhimaraya Metri, "Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy", International journal of information Management – volume 66, October 2022,1-2542.

[15] M. Samadzadeh, N. Farajipour Ghohroud, "Evaluating Security Anomalies by Classifying Traffic Using Deep Learning", 2023 9th International Conference on Web Research (ICWR), pp.135-141, 2023.

[16] E. Grabs, Ernests Petersons, A.s Ipatovs, Dmitrijs Chulkovs, "Supervised Machine Learning based Classification of Video Traffic Types", 2020 24th International Conference Electronics, pp.1-4, 2020.

[17] Y. D. Goli and R. Ambika, "Network Traffic Classification Techniques-A Review," 2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS), Belgaum, India, 2018, pp. 219-222, doi: 10.1109/CTEMS.2018.8769309.

[18] Yair Even-Zohar and Dan Roth, "A Sequential Model for Multi-Class Classification", Department of computer Science University of Illinois at Urbana-Champaign {evenzoha, danr}@uiuc.edu.

[19] A. Azab, M. Khasawneh, S. Alrabee, "Network Traffic classification: Techniques, datasets, and challenges "Digital Communications and Networks-Available online 18 September 2022.

[20] Kandaraj Pimarate, Salima Hamma, " Network Traffic Classification Using Machine Learning for software Define Networks", First Online:20 April 2020-book series(LNISA,volume 12081).

[21] D. -S. Kim and J. -M. Lee, "Machine Learning Algorithm in Network Traffic Classification," 2021 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, Republic of, 2021, pp. 1010-1013, doi: 10.1109/ICTC52510.2021.9620746.

[22] J. Krupski, W. Granizewski, M. Iwanowaski, "Data Transformation Schemes for CNN- Based Network Traffic Analysis: A Survey", Institute of Control and Industrial Electronics, Warsaw University of Technology- Published: 23 August 2021.

[23] J. Luis Guerra, C. Catania, “Datasets are not enough: Challenges in Labelling network traffic”, Computers & Security-Volume 120, September 2022,102810.

[24] H. Shi, DaN Zhang, “Efficient and robust feature extraction and selection for traffic classification”, Computer Networks-Volume 119,4 June 2017, Pages 1-16.

[25] Gianni D’Angelo, F. Palmieri, “Network traffic classification using deep convolutional recurrent autoencoder neural networks for spatial-temporal features extraction”, Journal of Network and Computer Applications-Volume 173, 1 January 2021,102890.

[26] G. Bovenzi, D. Ciuonzo, Antonio Pescape, “A Bog Data-Enabled Hierarchical Framework for Traffic Classification”, Volume:7 Issue:4.

[27] O. Salman, Imad H. Elhajj, “A review on machine learning-based approaches for internet traffic classification”, published:22 June 2020| 75,673-710 (2020)

[28] K. Naresh Kumar Thapa, N. Duraipandian, “Malicious Traffic Classification Using Long Short-Term Memory (LSTM) Model”, Published: 13 March 2021 | 119,2707-2724 (2021)

[29] A. Khan, M. M. Fouda, D. -T. Do, A. Almaleh and A. U. Rahman, "Short-Term Traffic Prediction Using Deep Learning Long Short-Term Memory: Taxonomy, Applications, Challenges, and Future Trends," in IEEE Access, vol. 11, pp. 94371-94391, 2023, doi: 10.1109/ACCESS.2023.3309601.

[30] Qasem Abu- A1-Haija, Abdelraouf Ishtaiwi, “Machine learning Based Model to Identity Firewall Decisions to Improve Cyber-Défense”, Department of Data Science & Artificial Intelligence, University of Petra, Amman 1196-Vol.11(2021) No. 4 | ISSN: 2088-5334.

[31] S. Allagi and R. Rachh, “Analysis of Network log data using Machine Learning,” in Proc. Of IEEE 5th International Conference for Convergence in Technology, India, pp. 1-3, 2019.