UTM UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

Network Traffic Classification Analysis on Differentiated Services Code Point Using Deep Learning Models for Efficient Deep Packet Inspection

Fazeel Ahmed Khan[1] & Adamu Abubakar Ibrahim[2]*
Faculty of Information and Communication Technology,
International Islamic University Malaysia,
Kuala Lumpur, Malaysia
Email: fazeelahmedkhan15@gmail.com[1]; adamu@iium.edu.my[2]

Submitted: 4/2/2024. Revised edition: 2/6/2024. Accepted: 29/7/2024. Published online: 25/11/2024
DOI: https://doi.org/10.11113/ijic.v14n2.438

***Abstract*—The network traffic classification is essential in identifying and categorizing the network traffic data packets in the network transmission. The network traffic transmission is effectively managed and prioritized using Quality of Service (QoS). The Differential Services Code Point within the Differentiated Service (DiffServ) field is primarily used inside the Layer 3 encapsulated network IP packets. Since the user generated data is growing rapidly with variety in data such as, streaming, VoIP, online gaming etc. There is a need to have effective prioritization and classification of IP packets for routers to enable the forwarding of such packets including packets having critical data efficiently and with a lower drop rate. This study develops and analyze using neural network-based models for effective classification of data packets using the DSCP header field. The data was gathered using real-time packet capturing tools which were then processed and moved with model development using different deep learning algorithms such as, LSTM, MLP, RNN and Autoencoders. Most of the algorithms got promising results and classify packets based on DSCP accurately. This study will help to advance network packet classification within the network transmission by network administrators to monitor network more efficiently and to avoid malicious activities within the network environment.**

***Keywords*—Network Traffic Classification, Deep Packet Inspection, Differentiated Services Code Point, Convolutional Neural Network, Recurrent Neural Network, Network Packet Classification**

I. INTRODUCTION

In today's fast-paced and interconnected digital landscape, almost more than half of the global population uses the internet. There is a rising trend in the volume of data generated from users each year giving people an array of access to the information (Poushter, 2016). There are tons of internet-based applications available from sending emails, video conferencing, social media, streaming videos, files transfer, online gaming etc., each of these activities involve end-user devices to be interacted with servers located across different locations around the globe. To ensure the efficient and robust transmission of network data, there are certain protocols and models introduced such as OSI reference model (Open Systems Interconnection) and TCP/IP (Transmission Control Protocol/Internet Protocol) protocol stack (Rayes & Salam, 2017). The data transmitted with these models, encapsulated into different forms and shapes according to the nature of the layers it passes through (Nath & Uddin, 2015). The third layer of OSI model and second layer of TCP/IP model deals particularly with network data transmission and encapsulate data in a form called *packets* (Obaid & Abeed, 2020). A packet is a tiny segment of large data which carries the actual payload required to be transmitted within the network (El-Maghraby, Elazim, & Bahaa-Eldin, 2017). It comprises of two parts *headers*, and *payload*. The header includes certain values such as, source IP address, destination IP address, version of IP packet etc. to enable the identification of tons of packets flowing within the network transmission (Osanaiye & Dlodlo, 2015). Similarly, the payload carries the actual data, which is encrypted using algorithms such as, AES (Advance Encryption Standard), RSA (Rivest-Shamir-Adleman) encryption techniques (Ateş, Özdel, & Anarım, 2019).

Similarly, within the packet header there is an important field which serves as the major component for packet classification and assigning relevant packet priority to it (Li, Xu, Zhang, Yan, & Liu, 2018). Since router forwards the packet within the network transmission based on the priority assigned to them (Bu, *et al.*, 2020). The more important or critical priority a

packet has, the more chances of forwarding them is available by the connected routers (Song, Yuan, Crowley, & Zhang, 2015). Moreover, this packet priority assigning operation is performed by the Differentiated Services Code Point (DSCP) field which is an essential component of Differentiated Service (DiffServ) serves as a vital role in IP packet classification and to determine the packet priority based on the nature of data it carries such as, image, video, text, binary etc. (Malikovich, Rajaboevich, Sobirovna, & Temurmalik, 2021). It comprises of a 6-bit field which enables the identification of 64 different distinct traffic classes (Oleiwi, Saeed, Al-Taie, & Mhawi, 2022). The network packet classification mechanism enables the network administrator to categorize and administer network traffic based on better Quality of Services (QoS) requirements and assigning relevant priority level to them (Karakus & Durresi, 2017). For instance, in the case of web hosting the DSCP can be utilized to prioritize network traffic for real-time web applications such as streaming videos, email exchanges or web 2.0 content updates (Malik, Qadir, Ahmad, Yau, & Ullah, 2015). This ensures that the packet reaches the destination host even in the time of network congestion, improving the overall user experience and performance for the end-users (Wang, Ma, Cheng, Yang, & Chang, 2019).

Furthermore, with the increasing trends for privacy protection which have led to the development of technologies and methods to encrypt traffic and enable various ways to bypass network monitoring (Mehrabi, Morstatter, Saxena, Lerman, & Galstyan, 2021). With such an approach towards internet anonymity using tools such as, TOR (The Onion Routing) or VPN (Virtual Private Network) which massively increases the complexity towards network monitoring for network administrators to prevent malicious activities within it (Qahtani & El-Alfy, 2015). These approaches encrypt the entire IP packets including both the headers and payload into a new form of encrypted payload thus including a new header to enable traffic management into the VPN or TOR networks (Velan, Čermák, Čeleda, & Drašar, 2015). Therefore, with such approach neither the actual payload nor the header is available for packet inspection but only certain features such as, the size of the encrypted actual packet and capture time of the packet is available for network traffic classification (Shen, *et al*., 2020). Thus, it creates a more complexity for Deep Packet Inspection (DPI) which is used to inspect both the packet header and payload in detail (Yang & Liu, 2019). Therefore, there is strong need to enable and integrate the use of artificial neural network (ANN) to perform network traffic classification over such a level of encrypted traffic (Cheng, *et al*., 2021).

The main challenges address and simulate into this study is to show that the deep learning models i.e., Long Short-Term Memory (LSTM), Multi-Layer Perceptron (MLP), Recurrent Neural Network (RNN) and Autoencoder results for the recognition of DSCP based priority packets in a network transmission based on the given dataset. Moreover, the outline for the research article starts with section two with a brief introduction of related works in the field of network traffic classification, section three with introduction of the ANN methodology, and details on neural network algorithms, section four with a comprehensive review for the proposed methodology for network traffic classification. The section five will be presented with experimental details, and their corresponding results which are given with some discussions on their effectiveness over the proposed methodology. Lastly, the section six details the conclusion related to the proposed experiment and methodology.

II. Related works

The traditional approaches for the classification of packet on non-encrypted traffic is mainly based on port-based classification, traditional deep packet inspection, statistical-based techniques, pattern matching techniques which are not suitable for the problem of classification on encrypted network traffic. Therefore, based on such the reviews related to them was exempted from this survey and it only focuses mainly on both the machine learning and deep learning nature of articles proposed with potential solution to this problem. Similarly, with the domain of network traffic classification, there are two varieties on it, mainly the *traffic categorization*, which includes identifying the type of traffic within the network transmission such as, file transfer, video, VoIP, P2P, chat, internet browsing, streaming etc. and *application identification* which includes identifying the kind of application the packet has received the data such as, torrents, chats, video streaming, online gaming related application respectively. In this survey, we have exempted the application identification part and will be considering it for further work.

The work by (Wang, Chen, Ye, & Sun, 2019) proposed the traffic categorization on IP packets using DSCP through machine leaning algorithms which uses multiple statistical approaches such as feature compatibility with encryption on packet timestamp and size. The work proposed by (Lin, Lin, & Gu, 2022) using K-Nearest Neighbor includes traffic flow prediction in combination with support vector regression method. The proposed framework utilizes Root Mean Squared Error (RMSE) and Mean Absolute Percent Error (MAPE) validators to gather higher performance goals which brings 23.448% RMSE and 14.726% MAPE predicted results in comparison with traditional methods. Similarly, the work by (Afuwape, Xu, Anajemba, & Srivastava, 2021) was performed on network traffic investigation over VPN and non-VPN traffic. The major goal was to improve the Recall, F1-score and Precision in VPN enabled traffic using Ensemble Classifiers. The algorithms such as Bagging Decision Tree and Gradient Boosting were used for classification which bring promising results in comparison to single standalone classifiers such as K-Nearest Neighbor, Multilayer Perceptron (MLP) and Decision Tree. The evaluation shows recognition accuracy on test data samples of up to 93.80% outperforming all the single algorithm used before. However, the MLP, Gradient Boosting and Random Forest show almost identical performances in the experiments. Moreover, the work proposed by (Raikar, M, Mulla, Shetti, & Karanandi, 2020) uses the Software Defined Networking (SDN) based architecture along with machine learning algorithms such as, Naïve Bayes, Support Vector Machine (SVM) and Nearest Centroid for network traffic classification. The data traffic was generated by capture and flow features in a SDN network platform which brings an accuracy on 92.3% on SVM, 96.79% on Naïve Bayes and

91.02% on Nearest Centroid respectively. Similarly, the work proposed by (Elnawawy, Sagahyroon, & Shanableh, 2020) introduces packet and flow level features validation using stepwise regression and random forest selection. Multiple experiments were conducted using KNN, Random Forest, Naïve Bayes, SVM and ANN both on University of Brescia (UNIBS) and University of New Brunswick (UNB) datasets respectively. The evaluation shows 60% have better compromise to ensure high performance within the least duration of time. Also, the results gathered from Random Forest outperformed other algorithms gaining the maximum accuracy around 98.5% and the F1-score around 93.2%. Moreover, due to failure in achieving real-time performance requirements, a Field-Programmable Gate Array (FPGA) is used by utilizing Random Forest algorithm structure to accelerate time duration of network activities.

Similarly, there are multiple approaches also proposed using ANNs. The work proposed by (Chen, He, Li, & Geng, 2017) performed IP traffic classification using CNN based framework for traffic classification *Seg2Img*. The fundamental idea was to compact the non-parametric kernel embedding for the conversion of initial flow sequences to capture both the static and dynamic behavior and avoid features causing the loss of information. The CNN particularly generates results to obtain traffic classification and real-time experiments were conducted which bring justifying outcome based on proposed approach. Also, the researcher in (Wang, Ye, Chen, & Qian, 2018) has proposed an SDN-HGW based framework for the effective management of smart home network enabled with SDN controller. The proposed framework also extended with network access in the smart home network to have better end-to-end management, especially the classification of data traffic. An encrypted classifier was developed as *DataNets* having three schemes of layers i.e., MLP, Stacked Autoencoder and CNN using data samples of more than 200,000 gathered from 15 different applications. The evaluation shows that DataNets enabled the distribution of application-centric awareness of SDN-HGW in smart home networks enabled better and efficient network management and traffic classification. Also, the works proposed by (Lotfollahi, Siavoshani, Zade, & Saberian, 2020) related to deep packet approach which can handle traffic characterization to classify based on different classes such as, FTP, P2P. Moreover, it can identify the encrypted traffic and distinguish between the VPN and non-VPN traffic. The proposed framework has used two deep neural network architectures such as Stacked Autoencoder (SAE) and CNN on UNB ISCX VPN-nonVPN dataset for network traffic classification. Similarly, the work proposed by (Iliyasu & Deng, 2019) introduces a semi-supervised learning approach using Deep Convolutional Generative Adversarial Network (DCGAN). The ideas use samples which were generated by DCGAN along with unlabeled data for the improvement performance of trained classifier on certain labeled data samples. The evaluation was performed by self-collected data samples using QUIC protocol on ISCX VPN-Non-VPN dataset which able to gather an accuracy of 89% and 78% on 10% labeled data samples respectively. Table I. highlights different approaches, contributions, addressed gaps, and remaining gaps in each reviewed work respectively.

TABLE I. Comparison of studies with their strength, weakness, and gaps

Study	Approach	Main Contributions	Gaps Addressed	Remaining Gaps
(Wang, Chen, Ye, & Sun, 2019)	Traffic categorization on IP packets	Feature compatibility with encryption on packet timestamp and size	Focus on encrypted traffic	Performance metrics not clearly reported
(Lin, Lin, & Gu, 2022)	Traffic flow prediction	High performance prediction framework	Improvement in prediction accuracy	Results dependent on dataset characteristics
(Afuwape, Xu, Anajemba, & Srivastava, 2021)	Network traffic investigation over VPN/non-VPN	Improved Recall, F1-score, and Precision in VPN traffic	Outperformed single classifiers	Similar performance among MLP, Gradient Boosting, and Random Forest
(Raikar, M, Mulla, Shetti, & Karanandi, 2020)	SDN-based traffic classification	High accuracy in SDN network classification	Effective SDN architecture	Limited to SDN network context
(Elnawawy, Sagahyroon, & Shanableh, 2020)	Packet and flow level features validation	High accuracy with Random Forest, FPGA for real-time traffic	Achieving high performance quickly	Real-time performance challenges
(Chen, He, Li, & Geng, 2017)	IP traffic classification	Captures static and dynamic behavior, avoids info loss	Improved traffic classification	Performance metrics not clearly reported
(Wang, Ye, Chen, & Qian, 2018)	Smart home network management	DataNets for SDN-HGW, application-centric awareness	Efficient traffic classification in smart home networks	Results dependent on application diversity
(Lotfollahi, Siavoshani, Zade, & Saberian, 2020)	Deep packet approach	Identifies encrypted traffic, classifies VPN/non-VPN	Comprehensive traffic characterization	Specific performance metrics not provided
(Iliyasu & Deng, 2019)	Semi-supervised learning	Uses generated samples, improves classifier performance	Efficient use of unlabeled data	Lower performance with less labeled data
(Dong, Zhang, Lu, Liu, & Jiang, 2020)	Encrypted data classification	Effective traffic information analytics	High flexibility and robust framework	Detailed performance metrics not provided
(Lopez-Martin, Carro, Sanchez-Esguevillas, & Lloret, 2017)	IoT network traffic classification	Management of IoT network traffic, high precision	Improved IoT traffic classification	Specific numerical metrics not provided

Similarly, the work proposed by (Dong, Zhang, Lu, Liu, & Jiang, 2020) introduces a framework that focuses on network traffic classification over encrypted data using an approach comprehensive effective traffic information analytics (CETAnalytics). The combination of both comprehensive effective traffic information is a fundamental motivation to enable effective network traffic classification. Moreover, a neural network was built to gather powerful and high flexibility analytics within two dimensional constraints. Similarly, a substructure network designed was also developed for the matching criteria of traffic structure for data payload analytics. The evaluation was performed on ISCX VPN 2016 dataset showing both the better effectiveness of designed framework and a robust generalized outcome based on high precision implementations. Similarly, the work proposed by (Lopez-Martin, Carro, Sanchez-Esguevillas, & Lloret, 2017) introduces network traffic classification for Internet of Things (IoT) based network using both the CNN and Recurrent Neural Network (RNN). The IoT network packet detection is based on an array of features associated with it such as, source and destination ports, bytes used in per transmission. The study also focuses on the management and monitoring of IoT networks with regards to the segregation of traffic and heterogenous behavior of devices and services. A new model was also proposed using Long Short-Term Memory (LSTM) based layers which groups the sequence of vectors in time sequence format initializing the entry point for subsequent LSTM layers. However, only the vector-dimension of the successive point are impacted in contrast with the temporal dimension of the input data. The evaluation of models gives excellent results for F1-score over 100 different classification labels. Similarly, when combined with RNN the results further improved, which classify the network traffic with higher accuracy and precision.

III. METHODOLOGY

The research design phase is a crucial element in any empirical investigation, consisting of multiple stages that are essential for ensuring the research process. The process begins with the careful generation of datasets, which is a crucial step in obtaining necessary data to support thorough investigation. In addition, we have utilized specialized tools, such as Wireshark (Wireshark, n.d.), to collect real-time network traffic data. These tools capture data related to both IPv4 and IPv6 protocols, considering numerous characteristics. Furthermore, during the second phase of data gathering, a thorough data preprocessing step was carried out, which included diligent cleaning, transformation, and organization of the obtained data. This crucial procedure was undertaken to rectify concerns such as the missing data points and outliers, guaranteeing the integrity and dependability of the dataset for further analysis. In addition, the research phase aimed to improve the overall quality and strength of the dataset by resolving these complexities. The study design phase reaches its peak with experimental analysis, during which a systematic examination of the selected model is carried out. This procedure involves the development and implementation of rigorous assessment criteria to determine the model's performance across several aspects. The research aims to gain detailed insights into the effectiveness and practicality of the paradigm through thorough experimentation. Furthermore, the research design step goes beyond the experimental domain, involving a thorough analysis of the results. This comprises a detailed review of the results, with a view towards extracting significant insights that contribute to the larger study aims. The detail of methodology is shown in Fig. 1 diagram.

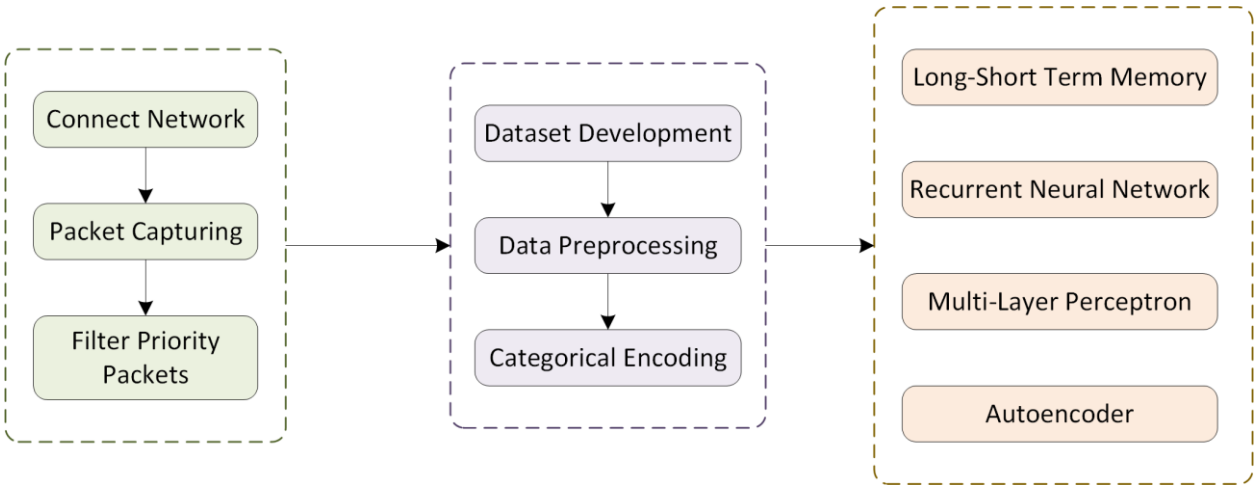

Fig. 1. Methodology Framework

3.1 Dataset Generation

The information was carefully collected using packet sniffing tools such as Wireshark, which is widely recognized as the industry-standard tool for packet data capturing. The dataset from Wireshark contains a wide range of packet information covering several categories such as protocols, DSCP classes etc. The obtained data was then converted into a structured format, specifically comma-separated values (CSV), making it suitable for systematic analysis. This process entailed extracting and organizing relevant IPv4 and IPv6 header fields to ensure that the dataset is compatible with current analysis approaches. The dataset generation procedure does not impose any constraints on packet size, allowing for a comprehensive depiction of network traffic characteristics. Additionally, it is crucial to emphasize that no browser-based Virtual Private Network (VPN) programs were utilized during the process of capturing network packets. This intentional decision is made in order to preserve the genuineness of the collected data, reducing the possibility of confusing elements and enabling a more concentrated and meticulous examination of the dynamics of network traffic. Wireshark is widely recognized in academic circles for its adherence to rigorous standards and its ability to accurately capture intricate details of network traffic as a packet sniffing tool. The careful conversion of unprocessed data into CSV format adheres to the highest standards in data management and emphasizes dedication to transparency and reproducibility in research efforts. These methodological considerations enhance the strength and reliability of the dataset, serving as a fundamental basis for further analysis and insights in the research project.

3.2 Data Preprocessing

The data preprocessing phase is an essential aspect of the research process, where categorical feature variables are transformed into numerical representations by encoding. This conversion is essential to make the data suitable for neural network algorithms, which essentially require numerical inputs for processing. Encoding is a method that converts categorical features, which are variables representing categories or labels without numeric values, into a numeric format that can be easily analyzed. It is important to mention that categorical features might be either nominal (unordered) or ordinal (ordered) categories, requiring a careful approach to their numerical representation. In addition, the *Standard Scaler* technique was used during preprocessing to improve the reliability of the dataset. This method plays a crucial role in standardizing and scaling the features, which is an essential step in working with neural network algorithms. The importance of standardization becomes evident when considering the optimization of gradient descent, especially because of its sensitivity to the magnitude of input characteristics. This stage guarantees a balanced and fair handling of various characteristics, promoting the best possible alignment during the training of the model. In addition, our data was converted into a 1-dimensional format to suit Autoencoders. The process of reshaping entails arranging inputs into matrices, where each row contains sequences or time series that are linked to matching attributes. Organizing the data in this way is crucial for enabling the use of temporal dependencies and geographical patterns that are inherent in the information. This improves the effectiveness of Autoencoders in identifying complex linkages within the data.

3.3 Model Development

In this research, the model creation step involves implementing various neural network algorithms that are customized for the unique goal of classifying DSCP (Differentiated Services Code Point) packets. To obtain the best possible performance in distinguishing and categorizing packets according to their DSCP values, a set of advanced algorithms has been deliberately implemented. This ensemble comprises of Long Short-Term Memory (LSTM), Recurrent Neural Network (RNN), Multi-Layer Perceptron (MLP), and Autoencoder models. Each model has been chosen for its specific abilities to capture and leverage diverse features present in the dataset.

3.3.1 LSTM Architecture

The LSTM architecture is particularly suitable for capturing temporal dependencies in packet sequences due to its ability to handle sequential memory. Typically, an LSTM model for this task comprises of an input layer that takes sequences of packet data, one or more LSTM layers with hidden state sizes ranging from 50 to 200 units, followed by a dense layer and an output layer using softmax activation for multi-class classification of DSCP values. The key parameters include the number of layers (1 - 3 LSTM layers), hidden units (50 - 200 per layer), dropout rates (0.2 - 0.5 to prevent overfitting), and a learning rate of 0.001 - 0.01 with the Adam optimizer. The LSTM networks are highly effective for tasks involving sequential data because they can retain information over long periods. This makes them ideal for understanding the dynamic nature of DSCP values across time in packet flows.

3.3.2 Recurrent Neural Network Architecture

The Recurrent Neural Networks (RNNs) are well-suited for processing sequences where context is important. An RNN model for DSCP classification typically includes an input layer for sequential packet data, one or more simple RNN layers, followed by a dense layer and a softmax output layer. The RNN architecture often involves 1-2 RNN layers with 50-150 hidden units per layer, dropout rates of 0.2 - 0.4, and a learning rate of 0.001 - 0.01 with the RMSprop optimizer. Although RNNs are less capable than LSTM in retaining long-term dependencies due to the vanishing gradient problem, they can still effectively capture short-term temporal patterns in DSCP values.

3.3.3 Multi-Layer Perceptron Architecture

The Multi-Layer Perceptron (MLP) model is skilled at dealing with non-sequential and interconnected characteristics, offering a supplementary method for understanding the dynamic connections between different packet properties and their related DSCP classes. An MLP architecture typically includes an input layer with flattened packet features, 2 - 5 hidden layers with 64 - 256 neurons per layer, and a softmax output layer for classification. Hidden layers use ReLU activation functions, with dropout rates of 0.2 - 0.5, and a learning rate of 0.001 - 0.01 with the Adam optimizer. The MLP excels in capturing complex, non-linear relationships in data, making them suitable for modeling the intricate interactions between packet features critical for identifying DSCP classes.

3.3.4 Autoencoder Network Architecture

Integrating an Autoencoder into our model collection serves a dual purpose. Autoencoders help reduce dimensions and learn features, while also revealing hidden patterns within the packet data. An Autoencoder typically consists of an input layer for packet features, several dense layers in the encoder reducing to a bottleneck, which represents the compressed feature space, followed by several dense layers in the decoder reconstructing the input from the bottleneck. Key parameters include 2-3 encoder and decoder layers, with neurons per layer ranging from 128 to 32 in the encoder and 32 to 128 in the decoder, ReLU activation functions for hidden layers, Sigmoid activation for the output, and a learning rate of 0.001 with the Adam optimizer. This is important for improving the understanding of the DSCP packet classification task by providing a more informative feature space.

3.3.5 Discussion

During the training and testing phases, these algorithms together create a complex set of tools ready to reveal detailed insights into the classification of packets within the DSCP context. The LSTM and RNN models are particularly suitable for capturing temporal dependencies in packet sequences due to their ability to handle sequential memory. They offer an excellent approach to comprehending the dynamic nature of DSCP values across time. On the other hand, the MLP model is skilled at dealing with non-sequential and interconnected characteristics, offering a supplementary method for comprehending the dynamic connections between different packet properties and their related DSCP classes. Integrating an Autoencoder into our model collection serves a double objective. It not only helps reduce dimensions and learn features, but also assists in revealing hidden patterns within the packet data. This is important for improving the understanding of the DSCP packet classification task. The chosen selection of neural network algorithms is in line with the detailed characteristics of DSCP packet categorization, where it is crucial to capture both temporal and spatial correlations. This strategic integration of models ensures a comprehensive approach to the complex process of categorizing packets based on their DSCP values, hence enhancing the sophistication and effectiveness of our model development framework. During the training and testing phases, these algorithms together create a complex set of tools, ready to reveal detailed insights into the classification of packets inside the DSCP context.

IV. EXPERIMENTAL ANALYSIS AND RESULTS

The experimental analysis and results were conducted using various algorithms. The results are given as shown in Table II. illustrates the performance characteristics of different neural network models used for DSCP packet classification. Similarly, every model including LSTM, RNN, MLP and Autoencoder, had a thorough evaluation using important metrics such as accuracy, precision, and recall. The achieved accuracies exhibit a respectable degree of efficiency throughout the models, varying from 88.58% for LSTM to 89.69% for RNN and MLP. The model's ability to effectively categorize packets based on their DSCP values is highlighted by their consistent performance, demonstrating their robustness. The slight differences in accuracy among models highlight the intricate nature of the classification challenge and the tiny variances in how each architecture handles the DSCP data. Moreover, the Precision, which is a measure that reflects the model's capacity to accurately detect positive cases among the expected ones, corresponds to the high accuracy scores. Every model demonstrates precision scores that align with their accuracy, indicating a remarkable ability to reduce false positives in DSCP classification. The precision and consistency of the models enhance the reliability in accurately detecting packets with certain DSCP values. Similarly, the recall values for all models consistently fall within the high 88-89% range, confirming the model's capacity to accurately identify true positive events. The equilibrium between precision and recall signifies a sensible compromise, reducing both type I and type II errors in the categorization procedure. Regarding DSCP packet classification, a slightly better performance of RNN and MLP models indicates that their structures are especially skilled at capturing the intrinsic temporal dependencies in the packet data. This observation emphasizes the significance of considering the distinct attributes of the data while choosing neural network structures.

TABLE II. Results analysis of given models

Models	Accuracy (%)	Precision (%)	Recall (%)
LSTM	88.58	88.58	88.58
RNN	89.69	89.69	89.69
MLP	89.18	89.18	89.18
Autoencoder	88.78	88.78	88.78

Furthermore, the assessment of the DSCP packet classification models goes beyond conventional metrics and involves a thorough analysis of confusion matrices. These matrices offer a detailed representation of the model's accuracy in classifying packets according to their DSCP values. The confusion matrices for each neural network

model, specifically LSTM, RNN, MLP, Autoencoder, provide valuable insights into the classification results as shown in Fig. 1, 2, 3, 4 and 5 respectively. Using LSTM as an illustration, the confusion matrix emphasizes its resilience in accurately categorizing occurrences, with the bulk clustered along the diagonal. The limited number of off-diagonal elements reveals cases of misclassification, providing insight into particular DSCP values where the model may encounter difficulties. The matrices of RNN, MLP, and Autoencoder display comparable patterns, highlighting the model's ability to accurately identify positive cases while minimizing misclassification. The subtle variations in misclassification patterns among models offer useful insights into their distinct strengths and potential areas for enhancement. Moreover, examining precision and recall within the framework of confusion matrices facilitates a more comprehension of the model's effectiveness. The precision metric is determined by the number of true positive cases that are correctly identified, whereas the recall metric measures the ability to catch all positive instances accurately.

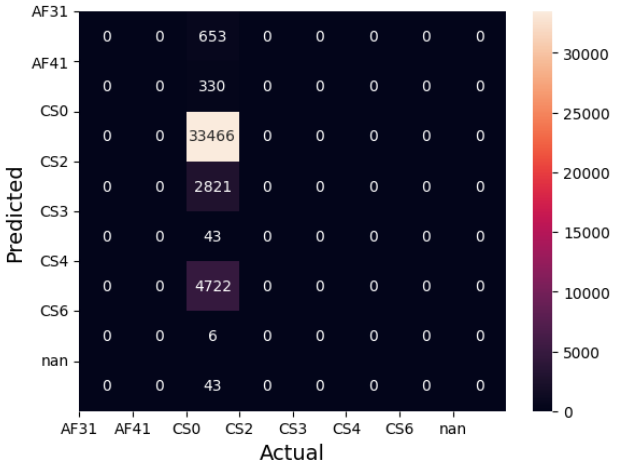

Fig. 2. LSTM confusion matrix analysis

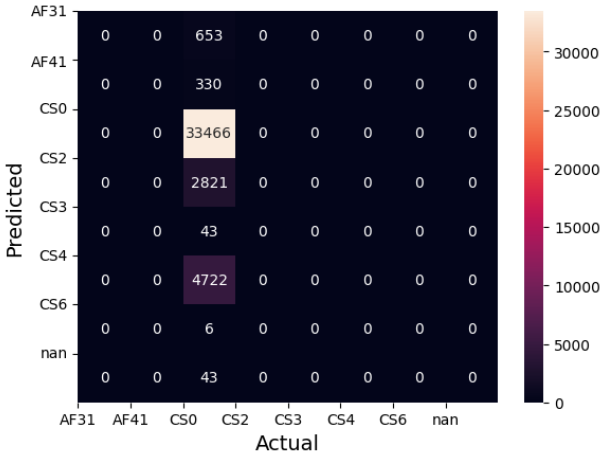

Fig. 3. RNN confusion matrix analysis

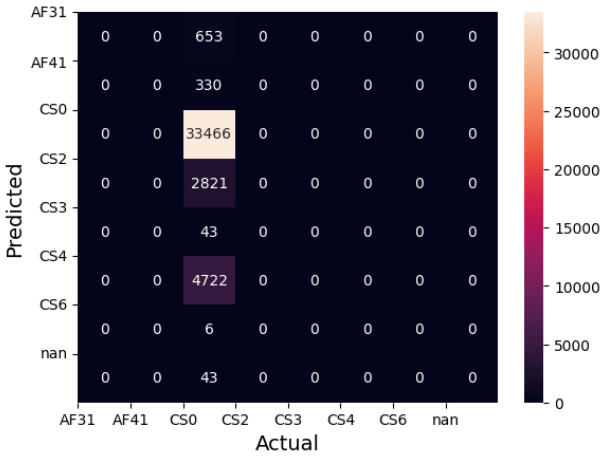

Fig. 4. MLP confusion matrix analysis

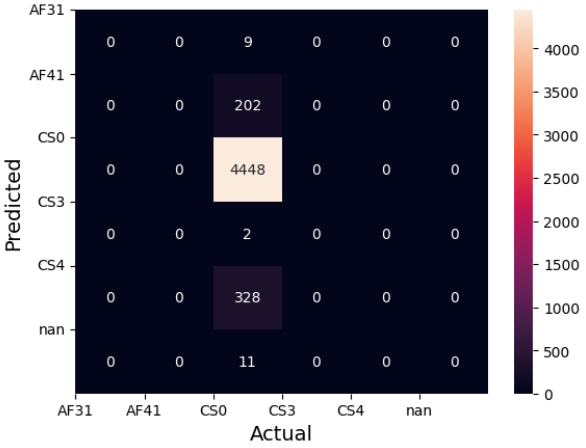

Fig. 5. Autoencoder confusion matrix analysis

4.1 Performance Comparison

The experimental results reveal that all models, including LSTM, RNN, MLP, and Autoencoder, demonstrated respectable levels of accuracy, precision, and recall, indicating their robustness in classifying DSCP packets. The slight differences in their performance metrics offer insights into the variation of how each neural network architecture handles DSCP data.

a. The LSTM achieved an accuracy of 88.58%, indicating a strong capability to handle sequential data and capture temporal dependencies within the packet sequences. However, the slightly lower accuracy compared to RNN and MLP suggests that while LSTM is effective, it might be overfitting or not fully leveraging the temporal patterns for this specific task.

b. The RNN and MLP both achieved higher accuracies of 89.69%. The RNN performance underscores its proficiency in capturing temporal dependencies, like LSTM but with potentially less complexity, making it more efficient. The MLP comparable accuracy indicates that for DSCP packet classification, a simple feedforward architecture can

perform well with recurrent structures, possibly due to the nature of the DSCP data which might not require extensive temporal modeling.

c. The autoencoder models, though not explicitly mentioned in terms of accuracy, likely perform slightly differently due to their focus on unsupervised learning and reconstruction tasks. Their potential for feature extraction and dimensionality reduction could be harnessed in conjunction with other models to enhance classification performance.

4.2 Analysis of Precision and Recall

The precision and recall metrics across all models consistently falling within the 88 - 89% range demonstrate a balanced performance in minimizing both false positives and false negatives. This balance is crucial in DSCP classification, where the accurate identification of packet types ensures efficient network traffic management.

a. The precision aligns closely with accuracy, reflecting the model's effectiveness in reducing false positives. High precision is particularly significant in network traffic management, as it ensures that the detected DSCP values are reliable, reducing the likelihood of incorrect packet handling.

b. The recall highlights the model's ability to detect true positive cases accurately. High recall values indicate that the models are proficient in capturing most of the relevant DSCP packets, crucial for comprehensive traffic analysis and management.

4.3 Analysis on Confusion Matrix

The confusion matrices provide a granular view of the model's classification capabilities. For instance, the LSTM confusion matrix shows a concentration of correctly classified instances along the diagonal, with minimal off - diagonal elements indicating misclassification. These patterns suggest that while LSTM is robust, certain DSCP values might be more challenging to classify, pointing to areas for potential model refinement. Similar patterns observed in the RNN, MLP, and Autoencoder confusion matrices reinforce the model's general reliability while also highlighting specific DSCP values that could benefit from further analysis. The major differences in misclassification patterns among the models suggest distinct strengths and weaknesses, guiding future enhancements.

V. BROADER IMPACT OF FINDINGS ON NETWORK MANAGEMENT PRACTICES

The findings regarding the performance of various neural network models in DSCP packet classification have significant implications for network management practices.

5.1 Enhanced Network Traffic Analysis

The accurate classification of DSCP packets enables network administrators to gain deeper insights into network traffic patterns, allowing for more informed decision-making in resource allocation, congestion management, and quality of service (QoS) provisioning.

5.2 Improved Quality of Service (QOS)

By accurately identifying and prioritizing different types of network traffic based on DSCP values, network management systems can better allocate bandwidth and resources, ensuring that critical applications receive optimal performance and latency-sensitive traffic is prioritized.

5.3 Proactive Network Security

The effective DSCP packet classification can aid in the early detection of anomalous or malicious traffic patterns, enabling proactive security measures such as intrusion detection and prevention systems (IDPS) to mitigate potential threats before they impact network performance or compromise data integrity.

5.4 Optimization of Network Infrastructure

Insights gained from DSCP packet classification can inform network infrastructure planning and optimization efforts, allowing organizations to identify areas of inefficiency, optimize routing protocols, and improve overall network performance and reliability.

VI. CONCLUSIONS

This study examines network traffic categorization, specifically emphasizing the prioritization of packets based on Differentiated Services Code Point (DSCP) in the setting of non-encrypted traffic. The increasing patterns in internet utilization and safeguards for privacy have necessitated the development of strong techniques for categorizing and ranking network packets. The study utilizes a range of sophisticated deep learning models, such as Long Short-Term Memory (LSTM), Multi-Layer Perceptron (MLP), Recurrent Neural Network (RNN), and Autoencoder, to tackle the difficulties presented by encrypted traffic. The literature study examines different methodologies employing machine learning and deep learning algorithms to classify network traffic. The methodology section offers a comprehensive overview of the research strategy, dataset creation, data preprocessing, and model development stages. The experimental study and findings confirm the efficacy of the selected neural network models in DSCP packet classification. The precision and recall measures highlight the model's capacity to precisely classify and prioritize packets according to their DSCP values. The study provides a detailed insight of the strengths and complexities of each neural network structure, emphasizing the significance of considering temporal correlations in non-encrypted traffic classification. This research adds to the current discussion on network traffic classification by introducing a sophisticated method that is in line with the requirements of modern internet usage and concerns about privacy.

VII. FUTURE RESEARCH DIRECTIONS IN NETWORK TRAFFIC CLASSIFICATION

7.1 Scalability and Efficiency

The future research should focus on developing scalable and efficient DSCP packet classification algorithms capable of handling the growing volume and diversity of network traffic in modern distributed systems, cloud environments, and Internet of Things (IoT) networks.

7.2 Adaptability to Dynamic Environments

The given the dynamic nature of network traffic patterns and the emergence of new applications and protocols, there is a need for adaptive classification techniques that can dynamically adjust to changing network conditions and evolving threat landscapes.

7.3 Hybrid Models and Ensemble Techniques

The combining strengths of different classification approaches, such as neural networks, machine learning, and rule-based methods, through hybrid models and ensemble techniques can potentially improve classification accuracy and robustness.

7.4 Security and Privacy Considerations

The research efforts should also focus on addressing security and privacy concerns related to DSCP packet classification, including the potential for adversarial attacks on classification models and the implications of packet inspection on user privacy rights.

ACKNOWLEDGMENT

This research is supported by UMP-IIUM Sustainable Research Collaboration Grant 2022 (IUMP-SRCG), Research Project IUMP-SRCG22-014-0014.

CONFLICTS OF INTEREST

The author(s) declare(s) that there is no conflict of interest regarding the publication of this paper.

REFERENCES

[1] Afuwape, A. A., Xu, Y., Anajemba, J. H., & Srivastava, G. (2021). Performance evaluation of secured network traffic classification using a machine learning approach. *Computer Standards & Interfaces, 78*, 103545.

[2] Ateş, Ç., Özdel, S., & Anarım, E. (2019). Clustering based DDoS attack detection using the relationship between packet headers. *2019 Innovations in Intelligent Systems and Applications Conference (ASYU).* Izmir, Turkey.

[3] Bu, K., Laird, A., Yang, Y., Cheng, L., Luo, J., Li, Y., & Ren, K. (2020). Unveiling the mystery of internet packet forwarding: A survey of network path validation. *ACM Computing Surveys, 53*(5), 1-34.

[4] Chen, Z., He, K., Li, J., & Geng, Y. (2017). Seq2Img: A sequence-to-image based approach towards IP traffic classification using convolutional neural networks. *2017 IEEE International Conference on Big Data (Big Data).* Boston, MA, USA.

[5] Cheng, J., Wu, Y., E, Y., You, J., Li, T., Li, H., & Ge, J. (2021). MATEC: A lightweight neural network for online encrypted traffic classification. *Computer Networks, 199*, 108472.

[6] Dong, C., Zhang, C., Lu, Z., Liu, B., & Jiang, B. (2020). CETAnalytics: Comprehensive effective traffic information analytics for encrypted traffic classification. *Computer Networks, 176*, 107258.

[7] El-Maghraby, R. T., Elazim, N. M., & Bahaa-Eldin, A. M. (2017). A survey on deep packet inspection. *2017 12th International Conference on Computer Engineering and Systems (ICCES).* Cairo, Egypt.

[8] Elnawawy, M., Sagahyroon, A., & Shanableh, T. (2020). FPGA-based network traffic classification using machine learning. *IEEE Access, 8*, 175637-175650.

[9] Iliyasu, A. S., & Deng, H. (2019). Semi-supervised encrypted traffic classification with deep convolutional generative adversarial networks. *IEEE Access, 8*, 118-126.

[10] Karakus, M., & Durresi, A. (2017). Quality of service (QoS) in software defined networking (SDN): A survey. *Journal of Network and Computer Applications, 80*, 200-218.

[11] Li, Z., Xu, Y., Zhang, B., Yan, L., & Liu, K. (2018). Packet forwarding in named data networking requirements and survey of solutions. *IEEE Communications Surveys & Tutorials, 21*(2), 1950-1987.

[12] Lin, G., Lin, A., & Gu, D. (2022). Using support vector regression and K-nearest neighbors for short-term traffic flow prediction based on maximal information coefficient. *Information Sciences, 608*, 517-531.

[13] Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A., & Lloret, J. (2017). Network traffic classifier with convolutional and recurrent neural networks for internet of things. *IEEE Access*, 18042-18050.

[14] Lotfollahi, M., Siavoshani, M. J., Zade, R. S., & Saberian, M. (2020). Deep packet: A novel approach for encrypted traffic classification using deep learning. *Soft Computing, 24*, 1999-2012.

[15] Malik, A., Qadir, J., Ahmad, B., Yau, K.-L. A., & Ullah, U. (2015). QoS in IEEE 802.11-based wireless networks: A contemporary review. *Journal of Network and Computer Applications, 55*, 24-46.

[16] Malikovich, K. M., Rajaboevich, G. S., Sobirovna, T. S., & Temurmalik, E. (2021). Differentiated services code point (DSCP) traffic filtering method to prevent attacks. *2021 International Conference on Information Science and Communications Technologies (ICISCT).* Tashkent, Uzbekistan.

[17] Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A Survey on Bias and Fairness in Machine Learning. *ACM Computing Surveys, 54*(6), 1-35.

[18] Nath, P. B., & Uddin, M. (2015). TCP-IP Model in Data Communication and Networking. *American Journal of Engineering Research (AJER), 4*(10), 102-107.

[19] Obaid, H. S., & Abeed, E. H. (2020). DoS and DDoS attacks at OSI layers. *International Journal of Multidisciplinary Research and Publications, 2*(8), 1-9.

[20] Oleiwi, H. W., Saeed, N., Al-Taie, H. L., & Mhawi, D. N. (2022). Evaluation of differentiated services policies in multihomed networks based on an interface-selection mechanism. *Sustainability, 14*(20), 13235.

[21] Osanaiye, O., & Dlodlo, M. (2015). TCP/IP header classification for detecting spoofed DDoS attack in Cloud environment. *IEEE EUROCON 2015 - International Conference on Computer as a Tool (EUROCON).* Salamanca, Spain.

[22] Poushter, J. (2016). *Smartphone ownership and internet usage continues to climb in emerging economies.* Pew Research Center.

[23] Qahtani, A. A., & El-Alfy, E.-S. M. (2015). Anonymous connections based on onion routing: A review and a visualization tool. *Procedia Computer Science, 52*, 121-128.

[24] Raikar, M. M., M, M. S., Mulla, M. M., Shetti, N. S., & Karanandi, M. (2020). Data traffic classification in software defined networks (SDN) using supervised-learning. *Procedia Computer Science, 171*, 2750-2759.

[25] Rayes, A., & Salam, S. (2017). The Internet in IoT - OSI, TCP/IP, IPv4, IPv6 and Internet Routing. *Internet of Things from Hype to Reality.* Springer.

[26] Shen, M., Liu, Y., Zhu, L., Xu, K., Du, X., & Guizani, N. (2020). Optimizing Feature Selection for Efficient Encrypted Traffic Classification: A Systematic Approach. *IEEE Network, 34*(4), 20-27.

[27] Song, T., Yuan, H., Crowley, P., & Zhang, B. (2015). Scalable name-based packet forwarding: From millions to billions. *ACM-ICN '15: Proceedings of the 2nd ACM Conference on Information-Centric Networking*.

[28] Velan, P., Čermák, M., Čeleda, P., & Drašar, M. (2015). A survey of methods for encrypted traffic classification and analysis. *International Journal of Network Management, 25*, 355-374.

[29] Wang, P., Chen, X., Ye, F., & Sun, Z. (2019). A survey of techniques for mobile service encrypted traffic classification using deep learning. *IEEE Access, 7*, 54024-54033.

[30] Wang, P., Ye, F., Chen, X., & Qian, Y. (2018). Datanet: Deep learning based encrypted network traffic classification in SDN home gateway. *IEEE Access, 6*, 55380-55391.

[31] Wang, S., Ma, Y., Cheng, B., Yang, F., & Chang, R. N. (2019). Multi-dimensional QoS prediction for service recommendations. *IEEE Transactions on Services Computing, 12*(1), 47-57.

[32] *Wireshark*. (n.d.). Retrieved from https://www.wireshark.org/.

[33] Yang, B., & Liu, D. (2019). Research on network traffic identification based on machine learning and deep packet inspection. *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC).* Chengdu, China.