WORLD COMET RESEARCH GROUP

International Journal of Applied Data Science & Modern Computing
Vol. 7, No. 1, 2024
Doi: 10.67228/30713498/IJADSMC-2024PI5T9V
PP. 01-15

Original Article

Deep Learning-Based Network Traffic Classification for Next-Generation Networks

Dr. Chen Wei[1], Dr. Hiroshi Tanaka[2]

[1]*Professor Peking University, China.*

[2]*Professor, University of Tokyo, Japan.*

Received: 03-06-2024 Revised: 03-26-2024 Accepted: 04-02-2024 Published: 04-04-2024

ABSTRACT

Network traffic classification has become essential for managing, securing, and optimizing next-generation networks (NGNs) that support IoT, cloud computing, SDN, NFV, and 5G technologies. Traditional classification methods based on port numbers and deep packet inspection are increasingly ineffective due to encrypted traffic, dynamic port allocation, and evolving application behaviors. This study presents a deep learning-based approach for intelligent network traffic classification. It reviews the evolution of traffic classification techniques and proposes a hybrid CNN-LSTM model that combines packet-level feature extraction with temporal sequence learning. The framework effectively captures spatial and temporal characteristics of network traffic, enabling accurate classification of both encrypted and non-encrypted flows. Experimental evaluation using benchmark datasets demonstrates that the proposed model outperforms conventional machine learning methods, achieving classification accuracy above 97%. Performance is validated using metrics such as accuracy, precision, recall, F1-score, and classification efficiency. The results highlight the potential of deep learning to support real-time traffic analysis, network security, QoS management, and resource optimization in modern communication networks. The proposed framework provides an intelligent and scalable solution for traffic classification in future autonomous and secure networking environments.

KEYWORDS

Deep Learning, Network Traffic Classification, Cnn, Lstm, Next-Generation Networks, 5g Networks, Cybersecurity, Traffic Analytics, Machine Learning, Network Intelligence.

WCRG
Global Research
ISSN: 3071-3498
PP: 01-15.

1. INTRODUCTION

1.1. Background and Motivation

Digital communication technologies have changed, and greatly, the nature of modern network environments, and significantly increased the amount of data generated and network traffic. More than billions of connected devices such as smart applications, enterprise infrastructure, mobile networks, and IoT devices are constantly sharing data with each other via cloud platforms. This extensive development has led to a complex and diverse traffic pattern, which makes it crucial to monitor, manage, and optimize traffic efficiently to ensure reliable network performance. The next generation communication technologies, including 5G, 6G, cloud computing and edge computing are developing rapidly and the need for intelligent traffic classification mechanisms is growing. Correct traffic classification helps to allocate resources, enforce traffic security, manage quality of service (QoS), and detect anomalies. While port-based identification and protocol analysis worked well in previous network environments, they are less effective today because of the dynamic application behavior and the growth and evolution of communication protocols. In addition, traffic is increasingly difficult to identify due to the increasing adoption of encrypted communication technologies like HTTPS, VPNs, and secure cloud services, where packet payloads are not directly available. The challenges inspire development of sophisticated deep learning-based traffic classification systems that can automatically learn complex traffic patterns and accurately determine network applications in today's communication environments.

1.2. Deep Learning in Network Traffic Analysis

In the realm of network traffic analysis, deep learning has proven to be a game-changer, providing enhanced tools and insights for comprehending, categorizing, and managing complex network interactions. Internet of Things (IoT) devices, mobile applications, social media platforms, multimedia services and cloud services are generating huge amount of heterogeneous traffic on modern networks, which makes traffic patterns ever more complex and dynamic. Traditional machine learning techniques may have difficulties to handle ever increasing complexity and dynamism of traffic patterns. Deep Learning models extract meaningful feature representations directly from raw network traffic data and do not rely on manually engineered features and domain knowledge to a greater extent than conventional approaches. This automatic feature extraction function not only lowers the dependency on manual processes but also boosts the classification precision and the accuracy of adapting to network changes. A major benefit of deep learning is that it is capable of detecting hierarchical patterns and relationships in network traffic that are not apparent on the surface. The deep neural networks used in deep learning can be used to capture low-level and high-level traffic features. The ability to recognize spatial patterns and structures at the level of packets is one area in which Convolutional Neural Networks (CNNs) excel. They can identify particular characteristics like packet size distributions, protocol behaviors, and communication signatures to differentiate various network applications. However, a Recurrent Neural Network (RNN) and a Long Short-Term Memory (LSTM) network are trained and designed to handle sequential data and temporal dependencies. These architectures are good for learning trends,

ISSN: 3071-3498
PP: 01-15.

behaviours and long-term relationships between communication sequences of packets and flows. Deep learning has also shown tremendous success in encrypted traffic classification, which is a vital problem in today's network management. As packet payloads cannot be accessed in encrypted communications, traditional Deep Packet Inspection techniques fail to be effective. Deep learning models address this limitation by modeling the metadata, flow statistics, packet timing information, and communication patterns without sacrificing user privacy. Additionally, these models can be used to provide real-time traffic analytics, which extracts valuable insights from vast amounts of network data and yields precise classifications in real-time. These features are crucial for cybersecurity monitoring, intrusion detection, quality of service optimization, anomaly detection, and intelligent network orchestration. With this in mind, deep learning has emerged as a crucial enabling technology for the next generation of communication networks, offering scalable, accurate and adaptive solutions to today's traffic analysis problems.

1.3. Challenges in Next-Generation Networks

The implementation of next-generation communications networks is fraught with many issues that have made network management and traffic analysis much more complex. The increasing number of cloud-based applications, Internet of Things (IoT) devices, mobile applications, video streaming platforms and smart connected systems are creating an exponential surge in network traffic volume and velocity, which is one of the most critical challenges. Today's networks handle enormous data volumes, must be high performance and reliable, and must process a large volume of data in real-time. A growing concern is the use of encrypted communications via protocols like HTTPS, SSL/TLS, and Virtual Private Networks (VPNs), which improve user privacy, but diminish the effectiveness of conventional traffic inspection and classification techniques. Moreover, dynamic application behavior poses challenges as most applications today are likely to shift their communication patterns and utilize dynamic ports as well as adaptive networking techniques, making their traffic easier to trick. The high dimensionality of traffic adds to the complexity of the classification, since there are plenty of attributes in network traffic, such as packet size, timing, protocol information, flow statistics, and communication patterns. The processing and analysis of such a large number of features demands advanced computation methods which can extract meaningful information efficiently. Another big challenge is the real-time classification requirements, which is especially important in scenarios where quick decision making is crucial for cybersecurity monitoring, intrusion detection, quality-of-service management, and network optimization. Traffic analysis delays can have a negative effect on network performance and security. Additionally, 5G and upcoming 6G networks impose unprecedented demands for scalability in terms of extreme data rates, high density of machine-type communications and billions of connected devices communicating simultaneously. In such scenarios, traditional traffic management systems can often find it difficult to scale effectively. Threats and cyberattacks are also becoming more and more sophisticated, placing more strain on network administrators. Intelligent detection mechanisms need to be able to detect subtle patterns of malicious communications such as advanced persistent threats, distributed denial-of-service attacks, malware communications, and encrypted malicious traffic. All

ISSN: 3071-3498
PP: 01-15.

these issues indicate that traditional traffic classification techniques are sub-optimal and emphasize the importance of deep learning techniques in traffic classification. Deep learning models can effectively solve these problems and accurately classify traffic for modern and future communication networks, automatically learning complex spatial and temporal traffic characteristics while achieving accuracy, scale, and timeliness. These are key features to guarantee the efficient functioning of networks, improved security and smart resource management in the future of digital infrastructures.

2. LITERATURE SURVEY

2.1. Traditional Traffic Classification Approaches

Until now, the main approaches used for network traffic classification were based on port identification and Deep Packet Inspection (DPI) techniques that focused on identifying the type of network applications generating traffic. Port based classification was widely adopted because many applications operated on fixed port numbers and therefore it is easy and efficient to identify the traffic. Port-based approaches were less effective, however, due to rapid growth of dynamic port allocation, peer to peer applications, tunneling mechanisms, and encrypted communication. These limitations are mitigated by the introduction of DPI techniques where detailed examination of the payloads of the packets for the purposes of protocol identification could be achieved. While DPI was effective for high classification accuracy, it was less effective in encrypted environments and had raised privacy issues because of users' data being inspected. Then, several machine learning techniques including Support Vector Machines (SVM), Decision Trees (DT), Random Forests (RF), and K-Nearest Neighbors (KNN) were used for classification of traffic based on the statistical flow features like packet size, flow duration and inter-arrival time. These approaches were able to achieve high accuracy and adaptability with a considerable amount of feature engineering and domain knowledge.

2.2. Deep Learning-Based Classification Models

With the rapid development of deep learning technologies, network traffic classification has been revolutionized by automatically extracting features and learning end-to-end. In contrast to traditional machine learning techniques, which rely on carefully crafted features, deep learning models are able to extract meaningful representations directly from the raw traffic data. CNNs have been effective in learning the spatial characteristics from a sequence of packets and traffic patterns, while RNNs and Long Short-Term Memory (LSTM) networks can learn the temporal dependencies and sequence within the network flow. These architectures have shown better classification accuracy in different benchmark datasets with accuracy of more than 95%. In addition, hybrid models with CNN and LSTM components have become popular, since they can also take advantage of both the spatial and temporal information and thus produce better predictions. In addition, deep learning techniques offer a level of flexibility in adapting to changing network environments, making them appropriate for next-generation communications systems with a variety of applications and high traffic.

ISSN: 3071-3498
PP: 01-15.

2.3. Encrypted Traffic Classification

The availability of encryption technologies like SSL/TLS, HTTPS, Virtual Private Networks (VPNs) and secure cloud communication protocols poses major challenges to traditional traffic monitoring and classification systems. Conventional Deep Packet Inspection techniques cannot accurately determine the application/service the packets are carrying because of the encryption. To solve this, researchers have come up with deep learning-based encrypted traffic classification methods based on flow-level metadata and statistical features without relying on the contents of the packets. Parameters like packet lengths, timing patterns, flow durations, and packet direction sequences give useful information in identifying encrypted applets. CNNs, RNNs, and Transformer-based models have proven to be highly successful in identifying the types of traffic being encrypted and keep the privacy of users intact. Such methods allow for the precise monitoring of network activity without compromising the privacy of sensitive data, therefore they are especially useful in cloud computing systems, cybersecurity solutions, enterprise networks, and next-generation communication systems where data privacy and security is a vital need.

2.4. Research Gaps and Future Directions

Although the deep learning-based network traffic classification solutions have proven to be highly successful, there are some research challenges that still need to be addressed. Another challenge is the computational complexity of deep neural networks, which may pose difficulties in achieving real-time performance in resource-limited settings like edge devices and IoT networks. Further complicating matters is the lack of interpretability of deep learning models, which makes it hard for administrators to interpret the decisions made by the network and difficult to trust automated systems. The imbalance of datasets and restricted access to data with labels also have an impact on model performance and generalization. Also, models learned from particular data sets might be hard to adapt to new environments in the network, new applications, and the changing traffic flows. Going forward, lightweight and energy-efficient architectures, incorporation of explainable AI methods, federated learning for distributed learning with privacy concerns, and self-learning mechanisms are needed that can continuously update classification models. The developments will improve the scalability, robustness and real-time applicability of traffic classification systems in the next generation of networks such as 5G, 6G, cloud computing and software-defined networking.

3. METHODOLOGY

3.1. Proposed Deep Learning Framework

The proposed Deep Learning-Based Network Traffic Classification Framework utilizes the hybrid Convolutional Neural Network (CNN) and Long Short Term Memory (LSTM) to classify and accurately detect various network traffic flows in the next generation communication environments. The framework aims to address the drawbacks of existing traffic classification techniques by automatically extracting meaningful features from raw network traffic data without relying on large amounts of manual feature engineering. First, the network traffic is gathered from packet capture

ISSN: 3071-3498
PP: 01-15.

files and flow records created in the network infrastructure. Data collected is preprocessed to make it consistent and enhance the model performance, such as data cleaning, normalization, feature extraction, and flow generation. Structured input sequences contain statistical features like packet size, flow duration, packet inter-arrival time, byte count, protocol info and packet direction. The CNN module consists of multiple convolutional and pooling layers used for identifying spatial patterns and local correlations in traffic flows, which is the main feature extractor. These layers automatically learn discriminative representations which capture protocol specific and application specific features. The extracted feature maps are then fed into the LSTM network, which aims to capture the temporal and sequential patterns in network traffic. The LSTM layer is particularly good at learning long-term dependencies, which are not easily learned by traditional machine learning models with fixed architectures, because network flows have varying time-varying behaviors. CNN and LSTM are combined in the framework, which takes full advantage of both spatial and temporal information, leading to high classification accuracy and robust performance. The learned representations are then mapped using fully connected dense layers into class probabilities using a Softmax activation function to yield a final traffic classification output. The framework allows classification of several traffic categories, such as web browsing, video streaming, file transfers, voice communication, cloud services, as well as encrypted applications. Also, regularization methods like dropout and batch normalization are used to avoid over-fitting and improve the model's ability to generalize. The hybrid architecture can be deployed in the modern 5G/6G environments, cloud computing, Internet of Things (IoT), and software-defined networking (SDN) with high classification accuracy, efficient feature learning, and adaptability to dynamic network conditions.

3.2. Data Preprocessing and Feature Engineering

Data Preprocessing and Feature Engineering are crucial steps in the proposed framework for network traffic classification, as the quality of the data provided for the deep learning models will impact their performance. Network traffic is captured from real networks with diverse types of Internet applications and communication protocols, as well as publicly available benchmark data sets. Raw traffic data may have inconsistencies, duplications, missing elements, and noisy data which can hinder the accuracy of the model. To make sure data is of good quality and learning is reliable, a comprehensive preprocessing pipeline is used. Firstly, data cleaning involves eliminating duplicate data, corrupted packets, and irrelevant information. Data with missing values are detected and either deleted or substituted by using suitable statistical techniques to preserve the integrity of the data set. Then feature normalisation, like Min-Max Scaling or z-score normalisation are used to make feature values fall within the same numerical range to make sure that the features with different scales do not dominate the learning process. Flow aggregation is then performed to merge individual packets into meaningful flows, depending on common characteristics like the duration of the communication, protocol type, destination address and source address. Label Encoding is then used after the Flow Generation to represent the classes of traffic in a numerical format for deep learning models. Feature engineering is about extracting informative traffic attributes that are well suited to represent network behavior. These important traffic characteristics are packet size reflecting communication patterns

ISSN: 3071-3498
PP: 01-15.

and application behavior, flow duration representing the lifetime of a network session and packet inter-arrival time reflecting temporal communication dynamics. The other features include protocol type, which can be used to distinguish between different types of communication protocols, such as TCP, UDP, and ICMP. Source and destination statistics such as bytes, packets, transmission rates and connect frequencies can be useful to know to understand traffic patterns and network usage characteristics. These features are engineered and grouped into structured sequences and multi-dimensional vectors which are used as inputs for the hybrid CNN-LSTM model. The framework's preprocessing is not only effective but also detailed, while its feature engineering is robust, thereby making data representation more powerful, boosting model convergence, simplifying training, and boosting classification accuracy. This systematic approach allows the deep learning model to successfully learn complex traffic patterns and separate different network applications, including encrypted traffic and new applications that are prevalent in today's communication networks.

3.3. Hybrid CNN-LSTM Model Development

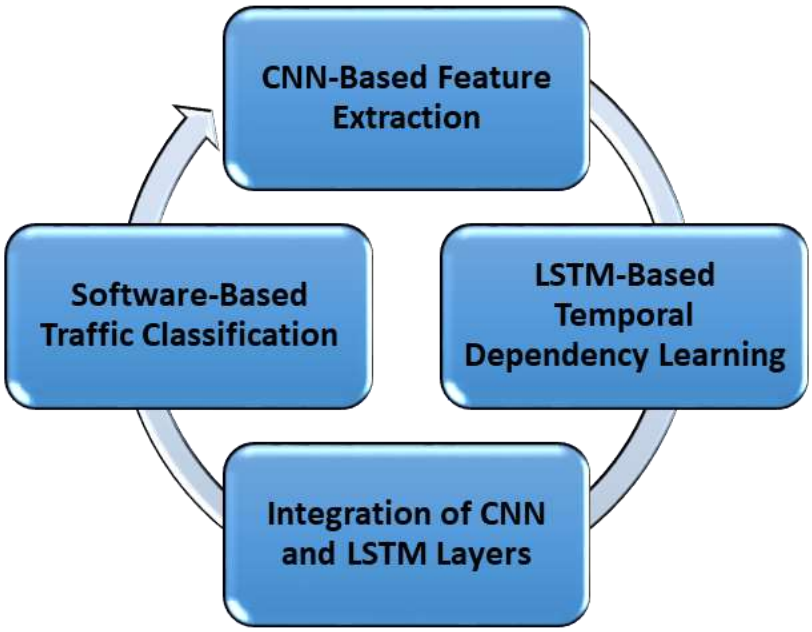

Fig 1 - Hybrid CNN-LSTM Model Development

3.3.1. CNN-Based Feature Extraction

The first step of the proposed hybrid architecture is the Convolutional Neural Network (CNN) which handles the automatic extraction of meaningful spatial information from network traffic data. CNNs use several convolutional filters to the input traffic feature matrices to allow the model to detect local traffic patterns and uncover the relationship between packet-level features. These filters are able to collect essential features like packet size variance, protocol-specific behavior and flow distribution. The CNN is able to reduce the dimensionality of the data while retaining the most important information through successive convolution and pooling operations. The automatic feature extraction process is designed to reduce the need for intensive handcrafted feature

ISSN: 3071-3498
PP: 01-15.

engineering and enhance the model's learning capability of the complex traffic representations efficiently.

3.3.2. LSTM-Based Temporal Dependency Learning

The extracted features by CNN layers are then passed to Long Short-Term Memory (LSTM) network for temporal analysis. Behavioral properties that can only be captured by the sequential and time-dependent behaviors of network traffic cannot be fully described using spatial analysis. The LSTM part is particularly aimed at modeling such temporal dependencies, keeping memory states to carry forward information due to the previous observation. The ability to identify long-term patterns and correlations among traffic sequences, such as communications sessions, user behavior trends, and application-specific traffic qualities. The LSTM's capability to accurately and reliably recognize the temporal relation between packets and flows further improves the framework's ability to classify various types of traffic.

3.3.3. Integration of CNN and LSTM Layers

By combining CNN with LSTM, the resulting hybrid model is a powerful system that can capture both spatial and temporal features of network traffic. The CNN is used to detect the local patterns and structural relationships in traffic data, and the LSTM is used to learn sequential dependencies over time. This complementary learning approach allows the model to produce richer and more informative feature representations than can stand-alone deep learning models. Combining both types of architecture increases classification accuracy and benefits from the advantages of both, making it very useful for detecting complex traffic patterns in today's network conditions, even encrypted and changing traffic flows.

3.3.4. Software-Based Traffic Classification

The last part of the proposed structure is dense layers fully connected with no gaps and a Softmax classification layer. The highly complex feature representations generated by the CNN-LSTM network are passed to the dense layers for further refinement of the learned information and for preparing it for classification.

The outputs of the model are then fed into the Softmax layer to convert them into probability distributions over various traffic categories. The traffic flow is allocated to the traffic class whose probability is the highest, and accurate multiclass traffic classification is achieved. This enables the framework to categorize any network application, such as Web browsing, video streaming, file transfer, cloud services, or encrypted communications. The Softmax classification mechanism performs classification efficiently and plays an important role on the final accuracy and robustness of the proposed traffic classification system.

ISSN: 3071-3498
PP: 01-15.

3.4. Performance Evaluation Metrics

Fig 2 - Performance Evaluation Metrics

3.4.1. Accuracy

One of the most frequently used metrics to assess the overall performance of a network traffic classification model is accuracy. It is the ratio of right classified traffic instances to the number of traffic samples in the dataset. The higher the accuracy, the more accurate the model is able to classify the network traffic. This measures overall classification performance, and is useful when there is a good balance of traffic classes in the dataset. But, being just accurate can be misleading if some traffic types are much underrepresented.

3.4.2. Precision

Precision measures how well the model can accurately classify an instance of traffic without producing too many false classifications in the other classes. It reflects the rate at which it gets the traffic flows it anticipates correct. If a model has a high precision, it will make fewer false positives predictions and hence the model is reliable to identify specific network applications or services. In network security and traffic management systems, accuracy is particularly crucial as misclassifications can impact resource allocation and monitoring decisions.

3.4.3. Recall

Recall is the ability of the classification model to correctly classify all the relevant traffic instances in one class. It is used to test the ability of the model to identify the true traffic flows of interest and to reduce the number of false classifications. The higher the recall value, the more the model is able to capture relevant traffic patterns contained in the data. In cybersecurity applications,

ISSN: 3071-3498
PP: 01-15.

anomaly detection systems, and intrusion monitoring environments, this metric becomes crucial as it can have serious operational and security implications if critical traffic types are not detected.

3.4.4. F1-Score

The F1-Score is a measure that balances precision and recall to give a better idea of the performance of the model. It is particularly useful if the data is skewed, meaning that some traffic categories have much more data than others. High F1-Score means that the model is able to correctly identify and fully detect traffic classes. The F1-Score is a better measure of classification effectiveness than the accuracy-only score because it takes into account the trade-off between precision and recall. Thus, it is commonly used in the field of research on deep learning based network traffic classification as a key performance indicator.

3.4.5. Importance of Multiple Evaluation Metrics

The multi-evaluation metrics help to gain a deeper insight into the performance of the proposed CNN-LSTM model. The accuracy of the model indicates how correct the model is, the precision of the prediction is assessed by the recall, and the F1-Score is used to balance the two. These metrics can then be used to comprehensively evaluate the effectiveness of the classification system for various traffic types. The robust and reliable classification with high accuracy is guaranteed by the developed classification model, which is evaluated based on different metrics and parameters.

4. RESULT AND DISCUSSION

4.1. Experimental Setup

The proposed hybrid CNN-LSTM framework for network traffic classification in next generation communication networks was evaluated through the experimental setup. A benchmark network traffic dataset comprising of various categories of applications was used for training and testing the model. The data set comprised traffic from web browsing, video streaming, Voice over Internet Protocol (VoIP), cloud service, online gaming applications, file transfer services, and encrypted communications. The traffic categories chosen were because they are the most typical applications found in today's network environments and because they have different traffic properties which make them difficult to classify using conventional traffic classification methods. The traffic data was thoroughly preprocessed before training the models, cleansing, normalizing the data, consolidating flows, and extracting features. The data set was split into three sections: training, validation and testing, for model development and for an unbiased assessment of model performance. The training set was employed for the learning of the traffic patterns and optimization of the network parameters, while the validation set was utilized for the tuning of these hyperparameters and preventing the overfitting of the model. The testing set of data were used only for the final performance evaluation. An implementation of the CNN-LSTM architecture was performed with a deep learning framework and trained on high-performance computing resources with the usage of Graphical Processing Units (GPUs) to speed up model training. The hyperparameters such as learning rate, batch size, number of convolutional filters, number of LSTM units, dropout rate and training epochs, were strategically tuned through experimentation for the

ISSN: 3071-3498
PP: 01-15.

best classification results. To efficiently update the weights of the model, the Adam optimization algorithm was used, while the categorical cross entropy was used for multi-class classification as the loss function. To improve generalisation and mitigate overfitting, regularisation methods like dropout and batch norm were added to the model. During the training process, the model's performance was regularly assessed using validation metrics such as accuracy, precision, recall, and F1-score. The experimental setup included an environment that mimics the realistic network conditions, including both encrypted and non-encrypted traffic flows, to evaluate the framework's performance in the classification of various traffic flows. The experimental setup was designed to thoroughly and accurately evaluate the proposed CNN-LSTM model and offer valuable insights into its potential applications for intelligent traffic management, network monitoring, cybersecurity, and quality of service optimization in contemporary 5G/6G, cloud computing, and Internet of Things (IoT) systems.

4.2. Performance Comparison

Table 1: Performance Comparison

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
SVM	88.4	87.6	86.9	87.2
Random Forest	91.7	91.1	90.8	90.9
CNN	95.2	94.8	94.5	94.6
LSTM	96.1	95.8	95.5	95.6
Proposed CNN-LSTM	97.8	97.5	97.2	97.3

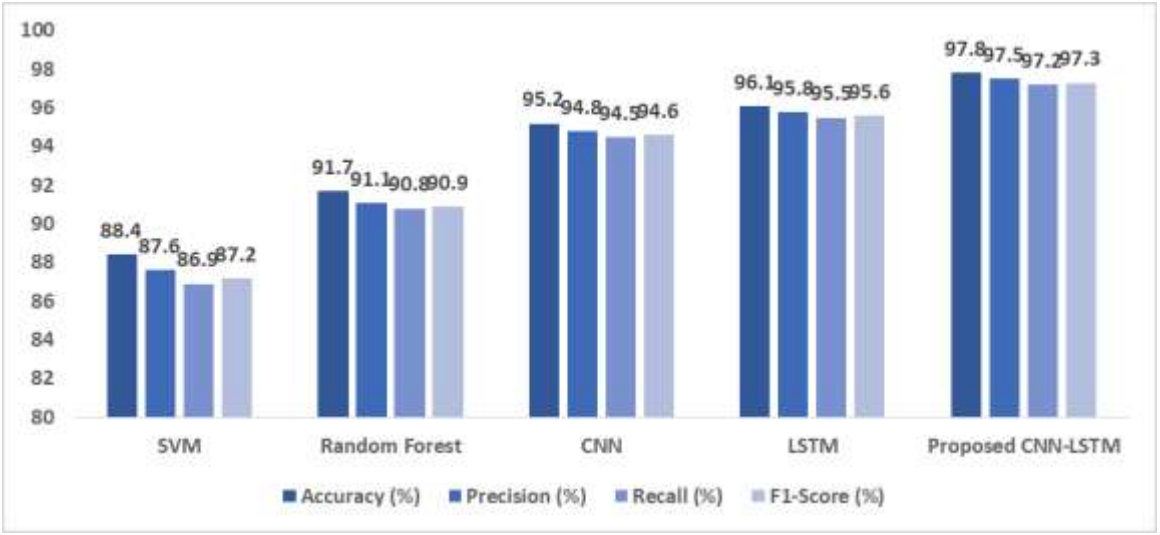

Fig 3 - Performance Comparison

4.2.1. Support Vector Machine (SVM)

The Support Vector Machine (SVM) model resulted in an accuracy of 88.4%, a precision value of 87.6%, a recall value of 86.9% and an F1-score value of 87.2%. The results show that SVM can be used effectively to classify network traffic, as it has successfully found the optimal decision

ISSN: 3071-3498
PP: 01-15.

boundaries for different traffic categories. The algorithm has good generalization properties and is reasonable in moderate size set of data. However, it has a shortcoming in that its performance requires manual feature engineering and it cannot automatically capture complex spatial and temporal traffic patterns. The accuracy of SVM in classifying network traffic decreases as traffic becomes more dynamic and encrypted.SVM's classification accuracy drops when the network traffic is more dynamic and encrypted than with more sophisticated deep learning techniques.

4.2.2. Random Forest

The Random Forest classifier gave better accuracy (91.7%), Precision (91.1%), Recall (90.8%) and F1 score (90.9%). Random Forest consists of several decision trees and the overall classification is obtained by aggregating the outputs of all these decision trees, which reduces the overfitting effect and makes the classification more stable. The model is able to cope well with high dimensional traffic features and can discover non-linear relationship in the network traffic. Notwithstanding this benefits, Random Forest requires handcrafted features and might lack the ability to capture sequential dependencies, which exist in network traffic flows. Thus, it continues to perform worse than deep learning-based models which automatically learn the hierarchical feature representation.

4.2.3. Convolutional Neural Network (CNN)

The classification accuracy of CNN model was 95.2 % with the precision and recall value of 94.8 % and 94.5 % respectively, for F1 score 94.6 %. The results show that the convolutional networks are effective in automatically learning spatial features from network traffic data. CNNs are able to detect local patterns and hidden structures at the packet level that are hard to capture with traditional machine learning algorithms. The performance improvement from SVM and random forest over the deep learning based feature extraction is significant, which shows the advantage of deep learning based feature extraction. CNNs, however, are limited to learning spatial information and may not be able to learn the temporal dependency within sequential traffic flows.

4.2.4. Long short-term memory (LSTM)

Moreover, the LSTM model has enhanced the classification performance with 96.1% accuracy, 95.8% precision, 95.5% recall, and 95.6% F1-score. LSTM networks are particularly designed to handle sequential data and long term temporal dependence. This is used in network traffic classification to learn over time the patterns and behaviour of the communications. This results in LSTM outperforming single CNN-based models when it comes to recognizing complex classes of traffic. However, although LSTM can capture temporal relationships well, the ability to extract spatial features may be less efficient as compared to convolutional networks, and thus, its overall classification ability may be restricted.

4.2.5. Proposed CNN-LSTM Framework

The proposed CNN-LSTM approach demonstrated the best results with the accuracy of 97.8%, precision 97.5%, recall 97.2% and F1 score 97.3% among the other tested approaches. The superior results indicate the efficacy of the CNN with LSTM architectures combined together in the

ISSN: 3071-3498
PP: 01-15.

same architecture. The CNN part is used to extract the spatial traffic features and the LSTM part is used to capture the temporal dependency and sequential flow characteristics. The hybrid model combines both learning mechanisms, providing more comprehensive feature representations and enhancing classification performance in various traffic categories. The framework also has excellent generalization performance and robustness in the case of encrypted and complex network traffic patterns.

4.2.6. Overall Comparative Analysis

It is evident that the performance of classification improves with the evolution of simple machine learning algorithms to powerful deep learning architectures, as demonstrated by the comparative results. SVM and Random Forest have acceptable results, but suffer from manual feature engineering and limited representation learning. CNN and LSTM models greatly improve performance with the use of automatic feature extraction and temporal learning. Experimental results show that the proposed CNN-LSTM framework outperforms all baseline methods in terms of each evaluation metrics, which validates the fact that the proposed CNN-LSTM framework is the most effective solution for modern network traffic classification. These results corroborate the appropriateness of the proposed paradigm in the context of intelligent traffic management, monitoring of cyber security and future network applications.

4.3. Discussion

The results of the experiments clearly indicate the usefulness of the proposed hybrid CNN-LSTM framework in solving the problems facing the current network traffic classification problem. The proposed model gives significantly better performance in all evaluation metrics, accuracy, precision, recall, and F1-score, when compared to the traditional machine learning approaches like Support Vector Machines and Random Forests. This improvement is due to the complementary strengths of CNN and LSTM. CNN layers are used to efficiently extract spatial features and packet-level patterns from network traffic data, allowing the model to detect significant structure features related to diverse applications and protocols. At the same time, the LSTM layers are able to learn the temporal dependencies and sequential relationships between traffic flows, which enables the framework to learn complex traffic communication behaviors over time. By combining these two deep learning architectures, they are able to achieve a much more complete understanding of network traffic than is possible with other models. The overall classification accuracy of the proposed framework is 97.8% and can successfully classify various types of traffic, such as web browsing, video streaming, VoIP communications, cloud services, gaming traffic, and encrypted applications. The high classification performance suggests that discriminative traffic representations are successfully learned even in cases of payload information not being present because it is encrypted. This is especially crucial in today's networks where encrypted traffic forms a large part of all communications. Moreover, the model has demonstrated good generalization ability due to the high accuracy in various traffic flow and application scenarios. The value of 97.5% for precision indicates that the framework has a very low rate of false positive classifications, whereas the value of 97.2% for recall shows that it is able to correctly identify the majority of the relevant traffic instances with few

ISSN: 3071-3498
PP: 01-15.

false negatives. Such qualities are crucial for real-world network monitoring and security scenarios, where misclassification may result in suboptimal resource usage or failure to identify threats. In general, the results validate that the suggested CNN-LSTM network is reliable, scalable, and highly accurate for intelligent traffic classification. Because it can manage complex and encrypted traffic patterns, it is a promising solution for next generation network infrastructures, SDN, cybersecurity solutions, cloud computing environments, and new 5G and 6G communication environments.

5. CONCLUSION

In this paper, the authors gave a thorough analysis of network traffic classification using deep learning methods in next generation communication networks, highlighting the significance of intelligent traffic analysis in contemporary digital infrastructure. The volume, diversity, and complexity of network traffic have grown considerably as network environments are rapidly changing with the widespread adoption of cloud computing, Internet of Things (IoT) devices, 5G and emerging 6G technologies. Existing traffic classification methods such as port-based, or Deep Packet Inspection (DPI) are no longer effective, as dynamic ports, encrypted traffic and advanced network applications are becoming increasingly common. The restrictions underscore the need for sophisticated classification methods that can accurately classify traffic patterns, be scalable, efficient, and adaptable. In this regard, deep learning becomes a promising solution, as it can learn complex feature representations from raw network traffic in an automatic fashion, without requiring significant manual efforts to design features. The authors analyzed the available traffic classification methods and analyzed the pros and cons of the conventional machine learning methods and deep learning methods. Particular emphasis was placed on Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks and hybrid architectures which integrate spatial and temporal learning. In light of these findings, a hybrid CNN-LSTM model was proposed to take the best of both models. The proposed framework comprised of four stages: data preprocessing, feature normalization, feature extraction, temporal sequence modeling, and multiclass classification. The CNN component was able to effectively capture the local packet-level and flow-level characteristics, and the LSTM component modeled temporal dependencies and sequential traffic behavior. This combination not only allowed the framework to learn richer traffic representations, but also boosted classification accuracy for various network applications. The experimental results showed the effectiveness of the proposed framework, with high accuracy of classification of 97.8%, and high values of precision, recall, and F1 scores. The superior performance of the CNN-LSTM model compared with traditional machine learning techniques and standalone deep learning models validates the effectiveness of combining spatial and temporal feature learning mechanisms. Moreover, the framework was able to correctly identify encrypted and non-encrypted traffic flows, thus showing its applicability in current secure communication environments. The high accuracy and robustness of the model indicate its potential for deployment in real-world network monitoring, cybersecurity, quality-of-service management, anomaly detection, and intelligent resource allocation systems. The results of this research indicate that deep learning is going to be key to future network intelligence and automation. In the future, communication networks will be more autonomous and

ISSN: 3071-3498
PP: 01-15.

data-centric, and intelligent traffic classification will be one of the basic parts to efficient network management and security operations. Transformer-based architectures, federated learning approaches, explainable artificial intelligence techniques, edge computing solutions, and adaptive online learning mechanisms can be integrated into the proposed framework in future research to further improve it. These developments will render communication systems more scalable, transparent, private and deployable in real time and in turn help in building more intelligent and resilient communication systems of the future.

REFERENCES

[1] T. T. T. Nguyen and G. Armitage, "A survey of techniques for internet traffic classification using machine learning," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 4, pp. 56–76, 2008.

[2] A. W. Moore and D. Zuev, "Internet traffic classification using Bayesian analysis techniques," in *Proceedings of ACM SIGMETRICS*, Saint Malo, France, 2005, pp. 50–60.

[3] T. Karagiannis, K. Papagiannaki, and M. Faloutsos, "BLINC: Multilevel traffic classification in the dark," in *Proceedings of ACM SIGCOMM*, Philadelphia, PA, USA, 2005, pp. 229–240.

[4] J. Erman, M. Arlitt, and A. Mahanti, "Traffic classification using clustering algorithms," in *Proceedings of ACM SIGCOMM Workshop on Mining Network Data*, Pisa, Italy, 2006, pp. 281–286.

[5] N. Williams, S. Zander, and G. Armitage, "A preliminary performance comparison of five machine learning algorithms for practical IP traffic flow classification," *ACM SIGCOMM Computer Communication Review*, vol. 36, no. 5, pp. 5–16, 2006.

[6] W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, "Malware traffic classification using convolutional neural network for representation learning," in *Proceedings of the International Conference on Information Networking (ICOIN)*, Kota Kinabalu, Malaysia, 2017, pp. 712–717.

[7] Y. Wang, Y. Xiang, J. Zhang, W. Zhou, and Y. Xiang, "Internet traffic classification using constrained clustering," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 11, pp. 2932–2943, 2014.

[8] A. Lotfollahi, M. J. Siavoshani, R. S. H. Zade, and M. Saberian, "Deep packet: A novel approach for encrypted traffic classification using deep learning," *Soft Computing*, vol. 24, no. 3, pp. 1999–2012, 2020.

[9] R. Aceto, D. Ciuonzo, A. Montieri, and A. Pescapé, "Mobile encrypted traffic classification using deep learning: Experimental evaluation, lessons learned, and challenges," *IEEE Transactions on Network and Service Management*, vol. 16, no. 2, pp. 445–458, 2019.

[10] M. Lopez-Martin, B. Carro, A. Sanchez-Esguevillas, and J. Lloret, "Network traffic classifier with convolutional and recurrent neural networks for internet of things," *IEEE Access*, vol. 5, pp. 18042–18050, 2017.

[11] X. Wang, S. Chen, and S. Jajodia, "Tracking anonymous peer-to-peer VoIP calls on the internet," in *Proceedings of ACM CCS*, Alexandria, VA, USA, 2005, pp. 81–91.

[12] P. Wang, X. Chen, F. Ye, and Z. Sun, "A survey of techniques for mobile service encrypted traffic classification using deep learning," *IEEE Access*, vol. 7, pp. 54024–54033, 2019.

[13] G. Aceto, D. Ciuonzo, A. Montieri, and A. Pescapé, "MIMETIC: Mobile encrypted traffic classification using multimodal deep learning," *Computer Networks*, vol. 165, Art. no. 106944, 2019.

[14] M. Shafiq, X. Yu, A. K. Bashir, H. N. Chaudhry, and D. Wang, "A machine learning approach for feature selection traffic classification using security analysis," *Journal of Supercomputing*, vol. 74, no. 10, pp. 4867–4892, 2018.

[15] R. Boutaba, M. A. Salahuddin, N. Limam, S. Ayoubi, N. Shahriar, F. Estrada-Solano, and O. M. Caicedo, "A comprehensive survey on machine learning for networking: Evolution, applications and research opportunities," *Journal of Internet Services and Applications*, vol. 9, no. 1, pp. 1–99, 2018.

[16] Gajula, S. (2023). A review of anomaly identification in finance frauds using machine learning system. *International Journal of Current Engineering and Technology, 13*(6), 568–575. https://ijcet.evegenis.org/index.php/ijcet/article/view/820.