IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp736-745

A DEEP LEARNING FRAMEWORK WITH ATTENTION AND BIG-STEP CONVOLUTION FOR NETWORK TRAFFIC ANOMALY DETECTION

[1]*B.Mahesh Babu*, *MCA Student, Department of MCA*

[2]*Dr.M.Veeresha, Ph.D, Professor, Department of MCA*

[12]*Dr KV Subba Reddy Institute of Technology, Dupadu, Kurnool*

ABSTRACT

Finding unusual traffic is essential for both network security and service quality. A big-step convolutional neural network traffic detection model based on the attention mechanism is developed since the single dimension of the detection model and feature similarity make it very difficult to identify anomalous traffic. First, the raw traffic is preprocessed and mapped into a two-dimensional greyscale picture after the network traffic characteristics are examined. After that, histogram equalisation is used to create multi-channel greyscale pictures, and an attention mechanism is added to give traffic characteristics varying weights in order to improve local features. Lastly, traffic characteristics of various depths are extracted by combining pooling-free convolutional neural networks, which improves convolutional neural network flaws including overfitting and local feature omission. A balanced public data set and an actual data set were used for the simulation experiment. The suggested model is contrasted with ANN, CNN, RF, Bayes, and two more recent models, using the widely used method SVM as a baseline. In experiments, 99.5% accuracy is achieved using several classifications. The best anomaly detection is found in the suggested model. Additionally, the suggested approach beats other models in F1, recall, and accuracy. It is shown that the model is strong and resilient to many complicated situations in addition to being effective at detection.

I. INTRODUCTION

Every aspect of life uses internet technology, which has greatly aided in the growth of the economy and society. However, there are still a lot of issues with the mainstream network security and defence technologies that are currently in use, and the extensive application requirements further complicate the security configuration of the entire network, making it extremely vulnerable to attacks. The TCP/IP network architecture's openness also makes it easier for computer viruses to propagate via disguise, interfering with regular network operations and contributing to social and economic downturns. Maintaining network security greatly depends on how to use efficient techniques for data analysis in order to forecast the current network development, identify anomalies, and take the necessary corrective action [1].

Network traffic categorisation is a useful tool for detecting abnormal traffic. Its fundamental concept is that there are three primary methods: machine learning-based [4], deep packet detection-based [3], and port-based [2]. There are two types of machine learning: deep learning and standard machine learning. The first two approaches performed steadily and produced excellent classification results in the early days, when the Internet was limited and the kinds of traffic were simple [5, 6, 7]. However, the categorisation impact is diminished as a result of the growing variety of traffic kinds and the complexity of traffic components brought

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp736-745

about by the ongoing development of new Internet applications. To overcome the shortcomings of the aforementioned approaches, machine learning enhancement techniques are suggested. The goal of machine learning is to reliably and accurately categorise network traffic by extracting its statistical properties. It has several potential applications as well.

The collection of data sets, the creation of normalised data, data pre-processing, feature extraction, model training, and classification make up the whole network traffic classification process. Different techniques are used in traditional machine learning classification to choose the best subset of features that closely resemble the complete feature results for classification. This method depends on feature selection, which might have a direct impact on the classification outcomes and is unable to keep up with the changes in contemporary network traffic. Furthermore, the intricate interactions between distinct characteristics cannot be captured by conventional machine learning algorithms. Deep learning thus emerges as the best technique for network traffic classification, achieving excellent results in demanding and dynamic traffic categorisation settings.

Network traffic categorisation has been the subject of several deep learning experiments in recent years [8, 9, 10]. Although deep learning is still in its infancy for network anomaly detection research, these findings demonstrate the performance-enhancing viability of deep learning algorithms for handling traffic categorisation problems. By automatically collecting structured and complicated characteristics and sending them straight into a training classifier, deep learning, as opposed to machine learning, not only makes it possible to classify network traffic, but it also reflects intricate nonlinear connections between features. In conclusion, the model for detecting abnormal traffic in network security defence has become more effective and useful. But there are still a lot of issues: First, for traffic data with comparable attribute qualities, the categorisation results are subpar. Second, the accuracy of classifying network traffic is somewhat diminished by the rigid structure of the anomalous network detection model, which is unable to extract features in many dimensions and fields of view. Third, the sequence may become less significant if information is lost during repeated pooling using convolution neural networks.

The following contributions are made in this research to address the aforementioned issues and challenges: • We provide an Attention and Big Step Convolution Neural Network (ABS-CNN) model that is based on the attention mechanism [11]. In order to address issues like comparable features producing subpar classification results, the attention mechanism is asked to give data sequences attention weights in order to identify subtle characteristics. In order to address issues like comparable features producing subpar classification results, the attention mechanism is asked to give data sequences attention weights in order to identify subtle characteristics. Experiments demonstrate that the model with improved features is more resilient and has a greater classification accuracy.

• To address the issue of single model dimensionality, we use histogram equalisation in this article. Greyscale pictures are initially created from the traffic data, and the images are then histogram equalised. In conjunction with enhanced multi-channel convolution, multi-field fine-grained features may be automatically extracted and fused. The trials demonstrate that traffic with histogram equalisation is rather well-defined, leading to improved resilience and detection performance of the model.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp736-745

• The traffic characteristics are retrieved by combining big-step convolution in order to counteract the decreased correlation of traffic sequences caused by pooling. Stepwise convolution is another name for big-step convolution. Stepwise convolution lessens the damage of accuracy loss from information loss while maintaining the sequence-related characteristics that the convolution layer has extracted.

There are five sections to this study. The research background and primary contributions of this study are briefly described in Section I. The present state of the study will be outlined and summarised in Section II. The procedure of introducing the model and implementing the algorithm is completed in Section III. Section IV will conduct in-depth experiments and analyse the findings. Section V will conclude by analysing and summarising the model put forward in this work and suggesting some potential avenues for further investigation.

II. LITERATURE SURVEY

An overview of machine learning-based methods for classifying internet traffic

Early on, the Internet community became interested in traffic categorisation. Various methods have been put out to categorise Internet traffic in order to control security and Quality of Service (QoS). However, since they are difficult to administer, conventional categorisation methods that involve altering the Transmission Control Protocol/Internet Protocol (TCP/IP) scheme have not been embraced. Furthermore, deep packet inspection and port-based techniques are not always able to handle novel traffic features (such as dynamic port allocation, tunnelling, and encryption). Machine learning (ML) systems, on the other hand, efficiently categorise traffic down to the particular user activity and device type. To protect user privacy, another line of inquiry attempts to defy categorisation and anonymise Internet data. Current traffic surveys ignore anonymisation in favour of categorisation. Here, we examine methods for classifying and obfuscating Internet data, with a focus on machine learning-based solutions. This study also provides a thorough analysis of the various approaches to data representation and the varied goals of classifying Internet traffic. Lastly, we outline the main conclusions, restrictions, and suggestions for more study.

An Extended Investigation of P2P Traffic Categorisation

The measuring of network traffic for peer-to-peer (P2P) Internet applications is the main topic of this article. P2P apps are said to account for a significant amount of today's Internet traffic. Nonetheless, a variety of obfuscation strategies are used by contemporary P2P programs, such as chunked file transfers, HTTP masquerading, port hopping, dynamic port numbers, and encrypted payloads. P2P traffic identification requires reliable and efficient techniques as P2P applications develop further. Three approaches to P2P application classification are compared in this paper: transport-layer analysis, application-layer signatures, and port-based classification. Empirical network traces gathered from the University of Calgary's Internet connection during the previous two years are used in the research. The findings demonstrate the inefficiency of port-based analysis, which cannot detect between 30% and 70% of current Internet traffic. Although application signatures are correct, they could not be feasible due to technological or legal constraints. The transport-layer approach seems promising as it offers a reliable way to evaluate P2P traffic in aggregate. According to the latter approach, P2P accounted for 30–70% of campus Internet traffic over the previous 12 months.

Using application signatures for precise and scalable in-network P2P traffic identification

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp736-745

Numerous network activities, such as application-specific traffic engineering, capacity planning, provisioning, service differentiation, etc., depend on the ability to precisely identify the network traffic linked to various P2P applications. However, for many P2P applications, conventional traffic to higher-level application mapping methods like default server TCP or UDP network-port based disambiguation are very imprecise. In this research, we provide an effective method for using application level signatures to detect P2P application traffic. By looking through some of the accessible literature and packet-level traces, we first determine the application level signatures. Then, using the signatures that have been found, we create online filters that can effectively and precisely monitor P2P activity, even over fast network connections. We use five well-known P2P protocols to test our application-level identification method's performance. According to our measurements, our method often produces false positive and false negative ratios of less than 5%. Additionally, we demonstrate that our method is very scalable as it only needs to analyse the first few packets (less than ten packets) in order to detect a P2P connection. Our method can much outperform the P2P traffic volume estimations offered by pure network port-based methods. For example, compared to the conventional port-based method, we were able to detect three times as much traffic for the well-known Kazaa P2P protocol.

Classification of internet traffic using an increasing vector of flow

By examining the connections between flows rather than each one separately, we suggest a novel traffic classification technique that uses fewer packets to classify flows. By looking for pertinent flows within a certain time range, we present seven different kinds of connections for a flow and a further Expanding Vector (EV) based on the flow identities. The suggested Expanding Vector (TCEV)-based Traffic Classification approach may be used with a linear complexity of the flow number since it does not need a rigorous flow property assessment. The tests conducted on actual traffic data confirm that our approach (1) achieves comparable performance to the representative methods while reducing the number of packets processed significantly; (2) is resilient to packet loss and the lack of flow direction; and (3) can achieve higher accuracy in identifying TCP mouse flows.

Deep Packet Inspection for Quick and Memory-Efficient Traffic Classification in CMP Architecture

For many network applications, including network monitoring, traffic categorisation is crucial. It becomes useless to use the traditional method of identifying flows, such as looking at the port numbers in the packet headers. In this situation, traffic categorisation is more significantly impacted by deep packet inspection technology, which examines both the packet payloads and the packet headers. In the meanwhile, regular expressions are being used to describe patterns instead of strings due to their versatility, simplicity, and expressive capability. However, the regular expressions mathcing approach results in bad overall performance because to its large memory utilisation and processing cost. We examine the network traffic's application-level protocol distribution in this study and draw conclusions about its characteristics. Additionally, in contrast to earlier one-layer architectures, we use regular expressions in multi-core architecture to create a fast and memory-efficient two-layer system for traffic categorisation. We use a compression approach called CSCA to match regular expressions in order to minimise DFA's memory consumption, which may be reduced by 95%. In order to improve the matching

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp736-745

performance, we additionally implement a few optimisations. Our tests are conducted using real-world traffic and all L7-filter protocol patterns, and the results demonstrate that the system operates at Gbps on servers with four cores.

III. SYSREM ANALYSIS AND DESIGN

EXISTING SYSTEM

A cost-sensitive SVM (CMSVM) was introduced by Shi et al. [16] to address the issue of network traffic imbalance. The model employs adaptive weights to handle the imbalance issue for various applications using a multi-class SVM with an active learning method. A real-time network classification model using SPPSVM was suggested by Cao et al. [17]. The model employs an enhanced particle swarm optimisation approach to determine the ideal parameters after reducing the dimensionality of the original data using the principal component analysis (PCA) feature selection method. When compared to the conventional SVM model, the classification accuracy is better. In order to identify anomalous traffic while removing superfluous characteristics from the traffic data, Farid et al. [18] integrated naive bayes and decision trees. The detection rate is increased by the suggested algorithm. Manual feature creation and selection are often required by machine learning-based categorisation techniques, which are unable to keep up with the current state of network development.

An autoencoder-based deep neural network was suggested by Gianni et al. [19]. The model employs stacked fully connected neural networks to classify network traffic and embeds several autoencoders into convolutional and recurrent neural networks to extract the fundamental properties of interest.

A tree-structured recurrent neural network was introduced by Ren et al. [20]; it divides big classification issues into smaller classification problems using a tree topology. The nonlinear link between the input and output data may be automatically learnt by the model, improving the classification impact. A novel technique for classifying encrypted communications was put out by Tal et al. [21]. In order to classify traffic, the technique first transforms traffic data into comprehensible visuals, which are then combined with convolutional neural networks. To address the issue of recurrent neural networks' susceptibility to gradient explosion or disappearance, Li et al. [22] suggested a bidirectional independent recurrent neural network with parallel operations and tunable gradients. In order to highlight the key aspects of network traffic, the model combines global attention with forward and backward inputs to extract the bi-directional structural elements of the traffic.

A multi-level feature fusion approach was put up by Lin et al. [23] to address the issue of data imbalance. For improved efficiency, the model integrates statistical, byte, and data temporal aspects. A traffic categorisation model called TSCRNN based on temporal and spatial characteristics was introduced by Lin et al. [24]. To accomplish effective traffic classification, the model first preprocesses the original data before learning the traffic's spatial and temporal properties using CNN and bi-directional RNN, respectively. A deep learning integrated model was presented by Saadat et al. [25]. To classify network traffic, the model initially automatically extracts traffic characteristics using a one-dimensional convolutional neural network. This is followed by the use of ALO for effective feature selection and SOM-based clustering.

Disadvantages

- To increase the efficacy and efficiency of abnormal traffic detection generation, an efficient ML model detection policy or hybrid deep learning are not applied in the current system.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp736-745

- The Attention and Big Step Convolutional Neural Network (ABS-CNN) model, which is more accurate and efficient, has never been applied in an actual system..

Proposed System

• Based on the attention mechanism, we provide an Attention and Big Step Convolutional Neural Network (ABS-CNN) model in this research [11]. In order to address issues like comparable features producing subpar classification results, the attention mechanism is asked to give data sequences attention weights in order to identify subtle characteristics. In order to address issues like comparable features producing subpar classification results, the attention mechanism is asked to give data sequences attention weights in order to identify subtle characteristics. Experiments demonstrate that the model with improved features is more resilient and has a greater classification accuracy.

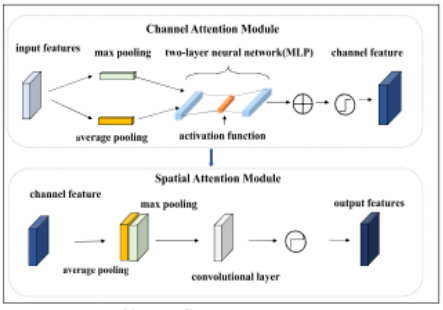
• To address the issue of single model dimensionality, we use histogram equalisation in this article. After processing the traffic data into greyscale pictures, the images undergo histogram equalisation. In conjunction with enhanced multi-channel convolution, multi-field fine-grained features may be automatically extracted and fused. The trials demonstrate that traffic with histogram equalisation is rather well-defined, leading to improved resilience and detection performance of the model.

• The traffic characteristics are retrieved by combining big-step convolution in order to counteract the decreased correlation of traffic sequences caused by pooling. Stepwise convolution is another name for big-step convolution. Stepwise convolution lessens the damage of accuracy loss from information loss while maintaining the sequence-related characteristics that the convolution layer has extracted.

Advantages

- The ABS-CNN model consists of an input layer, three convolutional layers, a fully connected layer, and an output layer. To improve convolution's capacity to extract traffic information, a convolutional attention mechanism is included.
- To confirm the effect of each component on the model, the ablation research in the suggested system is carried out by eliminating each component from the proposed ABS-CNN one at a time and comparing it with the ABS-CNN of the whole pair. To investigate how large-step convolution, histogram equalisation, and attention mechanisms affect model performance.

SYSTEM ARCHITECTURE



IV. IMPLEMENTATION

Modules Description

Service Provider

The Service Provider must use a working user name and password to log in to this module. Following a successful login, he may do several tasks including browsing data sets and training and testing. View all remote users, download predicted data sets, view traffic type ratio results, view trained and tested accuracy in a bar chart, view trained and tested accuracy results, and view traffic type prediction and ratio.

View and Authorize Users

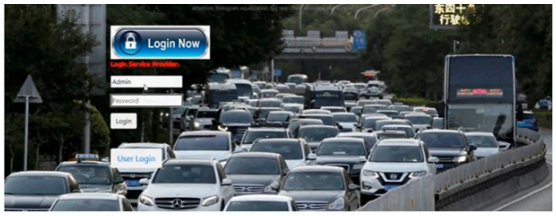
International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp736-745

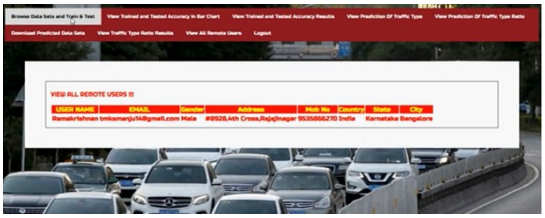
The administrator may see a list of all registered users in this module. Here, the administrator may see the user's information, like name, email, and address, and they can also grant the user permissions.

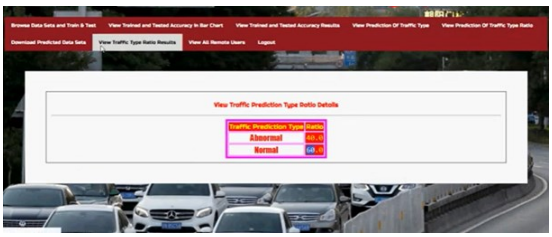
Remote User

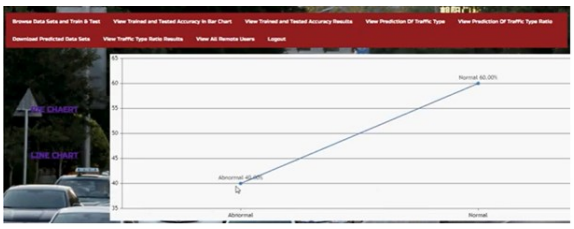
A total of n users are present in this module. Before beginning any actions, the user needs register. Following registration, the user's information will be entered into the database. Following a successful registration, he must use his password and authorised user name to log in. Following a successful login, the user may do tasks including registering and logging in, predicting the kind of traffic, and seeing their profile.

V. SCREEN SHOTS

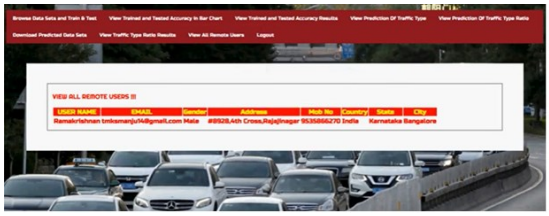


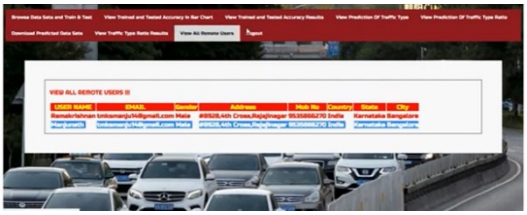






International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp736-745





VI. CONCLUSION

This work suggests a detection model based on attention and big-step convolution to overcome the challenges posed by comparable characteristics and a single model structure on anomalous traffic identification. Both publicly accessible datasets and datasets from actual environment crawls were used for the experiments. Performance analysis shows how effective the model is.

• When compared to conventional models, ABS-CNN has the best accuracy, precision, recall, and F1-Score. It has been shown that ABS-CNN produces predictions with excellent accuracy and a good detection effect. Additionally, the classification accuracy of multiple traffic is 100% based on the confusion matrix of different kinds of traffic, demonstrating the excellent sensitivity of ABS-CNN in detecting aberrant traffic.

• ABS-CNN operates effectively and requires less time for testing and training than other CNN model variations. And with the greatest classification results, ABS-CNN exhibits unmatched benefits in accuracy, precision, recall, and F1-Score.

• The ablation analysis's findings demonstrate that ABS-CNN improves feature differentiation and alleviates the challenges posed by feature similarity by introducing an attention mechanism to allocate attention weights for distinct features. In data preparation, ABSCNN adds histogram equalisation, which strengthens the model's single channel structure and increases its detection capabilities. Simultaneously, the sequence-related characteristics are retained when the pooling layer is removed, lowering the training parameters, increasing operational efficiency, and achieving effective anomalous traffic detection.

• ABS-CNN delivers outstanding detection results when tested on traffic crawled by actual environments. Encrypted traffic is what the actual environment records. ABS-CNN demonstrates the fine-grained ability to encrypt harmful traffic in addition to efficiently classifying encrypted traffic application kinds. This indicates that the ABS-CNN has some resilience and can adjust to situations with varying levels of complexity. In addition to offering a potential remedy for the challenges of comparable characteristics and single model dimension on abnormal traffic recognition, the suggested method expands the use of attention mechanisms and histogram equalisation in abnormal traffic detection. Future avenues for study include the following:

• In order to collect samples for data pre-processing, existing network techniques still need splitting, which leads to a small number of samples being lost. The five-tuple sequence also produced duplicate and invalid samples that were not labelled. In the future, do further study to identify better pre-processing tools and sequences.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp736-745

• To investigate anomalous traffic identification in spatial and temporal mining, examine the temporal and geographical correlations of various packets.

REFERENCES

[1] O. Salman, I. H. Elhajj, A. Kayssi, and A. Chehab, ‘‘A review on machine learning–based approaches for internet traffic classification,’’ *Ann. Telecommun.*, vol. 75, nos. 11–12, pp. 673–710, Dec. 2020.

[2] A. Madhukar and C. Williamson, ‘‘A longitudinal study of P2P traffic classification,’’ in *Proc. 14th IEEE Int. Symp. Modeling, Anal., Simulation*, Monterey, CA, USA, Sep. 2006, pp. 179–188, doi: 10.1109/MASCOTS. 2006.6.

[3] S. Sen, O. Spatscheck, and D.Wang, ‘‘Accurate, scalable in-network identification of P2P P2P traffic using application signatures,’’ in *Proc. 13th Int. Conf. World Wide Web*, New York, MY, USA, May 2004, pp. 512–521.

[4] L. Ding, J. Liu, T. Qin, and H. Li, ‘‘Internet traffic classification based on expanding vector of flow,’’ *Comput. Netw.*, vol. 129, pp. 178–192, Dec. 2017.

[5] T. Liu, Y. Sun, and L. Guo, ‘‘Fast and memory-efficient traffic classification with deep packet inspection in CMP architecture,’’ in *Proc. IEEE 5th Int. Conf. Netw., Archit., Storage*, Macau, China, Jul. 2010, pp. 208–217, doi: 10.1109/NAS.2010.43.

[6] N. Cascarano, L. Ciminiera, and F. Risso, ‘‘Optimizing deep packet inspection for high-speed traffic analysis,’’ *J. Netw. Syst. Manage.*, vol. 19, no. 1, p. 7–31, Mar. 2011.

[7] G. Aceto, A. Dainotti, W. de Donato, and A. Pescape, ‘‘PortLoad: Taking the best of two worlds in traffic classification,’’ in *Proc. IEEE Conf. Comput.Commun. Workshops (INFOCOM)*, San Diego, CA, USA, Mar. 2010,pp. 1–5, doi: 10.1109/INFCOMW.2010.5466645.

[8] L. Vu, C. T. Bui, and Q. U. Nguyen, ‘‘A deep learning based method for handling imbalanced problem in network traffic classification,’’ in *Proc. 8th Int. Symp. Inf. Commun. Technol.*, Dec. 2017, pp. 333–339.

[9] P. Wang, F. Ye, X. Chen, and Y. Qian, ‘‘Datanet: Deep learning based encrypted network traffic classification in SDN home gateway,’’ *IEEE Access*, vol. 6, pp. 55380–55391, 2018.

[10] J. H. Shu, J. Jiang, and J. X. Sun, ‘‘Network traffic classification based on deep learning,’’ *J. Phys., Conf. Ser.*, vol. 1087, Sep. 2018, Art. no. 062021.

[11] D. Bahdanau, K. H. Cho, and Y. Bengio, ‘‘Neural machine translation by jointly learning to align and translate,’’ 2014, *arXiv:1409.0473*.

[12] C.Wang, T. Xu, and X. Qin, ‘‘Network traffic classification with improved random forest,’’ in *Proc. 11th Int. Conf. Comput. Intell. Secur. (CIS)*,Shenzhen, China, Dec. 2015, pp. 78–81, doi: 10.1109/CIS.2015.27.

[13] Z. Yuan and C. Wang, ‘‘An improved network traffic classification algorithm based on Hadoop decision tree,’’ in *Proc. IEEE Int. Conf. Online Anal. Comput. Sci. (ICOACS)*, Chongqing, China, May 2016, pp. 53–56, doi: 10.1109/ICOACS.2016.7563047.

[14] A. V. Phan, M. L. Nguyen, and L. T. Bui, ‘‘Feature weighting and SVM parameters optimization based on genetic algorithms for classification problems,’’ *Appl. Intell.*, vol. 46, no. 2, pp. 455–469, Mar. 2017.

[15] B. Schmidt, A. Al-Fuqaha, A. Gupta, and D. Kountanis, ‘‘Optimizing an artificial immune system algorithm in support of flow-based internet traffic classification,’’ *Appl. Soft Comput.*, vol. 54, pp. 1–22, May 2017.

[16] S. Dong, ‘‘Multi class SVM algorithm with active learning for network traffic classification,’’ *Expert Syst. Appl.*, vol. 176, Aug. 2021, Art. no. 114885.

[17] J. Cao, Z. Fang, G. Qu, H. Sun, and D. Zhang, ‘‘An accurate traffic classification model based on support vector machines,’’ *Int. J. Netw.*

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp736-745

Manage., vol. 27, no. 1, Jan. 2017, Art. no. e1962.

[18] D. Md. Farid, N. Harbi, and M. Zahidur Rahman, ‘‘Combining Naive Bayes and decision tree for adaptive intrusion detection,’’ 2010, *arXiv:1005.4496*.

[19] G. D’Angelo and F. Palmieri, ‘‘Network traffic classification using deep convolutional recurrent autoencoder neural networks for spatial– temporal features extraction,’’ *J. Netw. Comput. Appl.*, vol. 173, Jan. 2021, Art. no. 102890.

[20] X. Ren, H. Gu, and W. Wei, ‘‘Tree-RNN: Tree structural recurrent neural network for network traffic classification,’’ *Expert Syst. Appl.*, vol. 167, Apr. 2021, Art. no. 114363.