Original Research Article

AN ENHANCED CONVOLUTIONAL NEURAL NETWORK FOR ENCRYPTED INTERNET TRAFFIC CLASSIFICATION

Abstract

The increasing reliance on Internet-based services has rendered secure and efficient network traffic classification a criticaltask. Conventional methods of categorising traffic such as port and payload methods often strugglewith the challenges posed by encrypted traffic. Deep learning techniques have emerged as a predominant method for traffic classification given its success in domains such as image recognition, document analysis and genomics This research proposes an enhanced DenseNet architecture that leverages deep learning to accurately classify encrypted internet traffic categories. The approach introduces a compression layer into the DenseNet architecture to address the co-adaptation problem as a result of information flow and optimise the CNN’s accuracy. The experimental results show that the approach can distinguish various encrypted Internet traffic categories with a high level of accuracy.

Keywords: Convolutional neural network, Internet, Traffic, Classification, DenseNet

INTRODUCTION

Internet traffic classification has become a vital aspect of network management and security. As the volume and complexity of internet traffic continue to expand, efficient and accurate classification methods are essential for distinguishing various applications that utilise the internet, this is useful for operations such as network optimisation, security monitoring, and quality of service management [1]. Conventional approaches to traffic classification, such as port-based and payload-based methods, have become less effective due to the widespread utilisation of encryption and dynamic port allocation [2].

Consequently, machine learning techniques, particularly deep learning models, have gained prominence in recent years for their capacity to analyse complex patterns in network traffic data [3]. These advanced methods can extract salient features from raw packet data or flow statistics, enabling more precise classification of internet traffic, even in the presence of encryption [4]. The development of sophisticated classification algorithms continues to be an active area of research, with ongoing efforts to enhance accuracy, scalability, and adaptability to evolving network protocols and applications.

Deep learning approaches for encrypted traffic classification have demonstrated the most promising results for the Internet traffic classification task. Due to successes recorded in tasks such as image classification, voice recognition and video classification, convolutional neural networks (CNN) have been utilised for the Internet traffic classification task. One of the most prominent variants of CNN is the DenseNet architecture [5] that enables information propagation through all the layers of the network; however, a significant drawback of the architectureis that as information is passed from the input to the output layer of the network, it can result in the detection of the same features by neurons, thereby resulting in reduced network capacity utilisation[6][7]. This study addresses this drawback by introducing a compression layer into the DenseNet architecture to prune the redundant neurons in the fully connected layer of the architecture.

The contributions of the paper are listed below:

- An enhanced DenseNet architecture with a neuron pruning layer for efficient encrypted internet traffic classification
- A classifier that is able to accurately distinguish between encrypted Internet traffic categories.
- Comparison of the performance of the proposed architecture with the conventional DenseNet architecture.

The paper is organised as follows: a review of literature, themethodology and results and discussionsare presented.

2. Literature review

DenseNet architecture was created to ensure maximum information flow between the various layers of the CNN architecture. It uses a feedforward architecture whereby each layer receives input feature maps from the preceding layers and passes its feature maps to all subsequent layers. Features are not combined through summation but through concatenation. Despite these challenges, researchers have used several strategies to address these limitations. Approaches involving supervised and semi-supervised learning approaches have been used [8] while parameter-efficient fine-tuning methods aim to decrease computational resource usage [9]. Efforts are also being made to improve the interpretability of deep learning models for encrypted traffic classification [10].

[11] stacked convolution layers to enhance feature extraction in DenseNet architecture and mitigate redundancies. Squeeze excitation modules were employed to represent interdependencies of salient feature maps. [12] incorporated PSA modules into the DenseNet architecture to improve computational efficiency by dividing convolution kernels in the Dense PSA block into asymmetric convolutions. [13] utilised a squeeze and excitation module to model interdependencies between features of different convolutional layers. [14] introduced a variant of DenseNet inspired by ResNet that substitutes concatenation operations within the dense blocks to reduce model complexity and the number of parameters. [15] employed Dense blocks to modify convolution layers in MobileNet, resulting in higher recognition accuracy. [16] combined DenseNet and LSTM for multivariate tasks. However, this approach has the limitation of high computational time. [17] enhanced the DenseNet architecture using sliding dense blocks to reduce redundancies in the network.

Several researchers have applied the DenseNet architecture to the Internet Traffic Classification task. [18] utilised a rap-DenseNet framework for network traffic classification. The limitation of this approach is its computational intensity. [19] incorporated a normalisation layer into the DenseNet architecture for data stabilisation and to enhance convergence speed. [20] employed a convolutional neural network for the classification of Internet Applications. The technique achieved high accuracy; however, it has the limitation of misclassifying encrypted internet traffic. [21] utilised a fully connected neural network and a 1-dimensional convolutional neural network for classifying internet traffic payload. The approach achieved an accuracy of 96%. However, the method is computationally intensive. [22] employed an ensemble of CNNs to classify network traffic in the Cambridge dataset. An accuracy of 98% was achieved. The approach, however, is susceptible to overfitting. [23] proposed a deep learning-based framework for encrypted network traffic that utilises stacked autoencoders, multi perceptron and convolutional neural networks. The method achieved low accuracy.

The reviewed studies have presented various techniques that have used DenseNet and other CNN variants for Classification; however, a common limitation is the susceptibility to overfitting and the high computational overhead involved in training and deploying the DenseNet model. This study seeks to address this by integrating a compression layer that reduces the number of neurons using neuron pruning.

3. Methodology

The methodology of this study focuses on the development of an enhanced DenseNet architecture for classifying encrypted Internet traffic. This method aims to address the challenges posed by traditional traffic classification techniques when dealing with encrypted data streams. The DenseNet architecture is enhanced by adding a compression layer for neuron pruning.The pruning of neurons is modelled as a tradeoff problem where neurons are pruned while maintaining classification performance. The approach proposed in this study incorporates key improvements such as the removal of redundant neurons in the neural network using the Upper Confidence Bound Multi-Armed Bandits algorithm to boost the classification performance of the neural network. The following subsections detail the dataset preparation, network architecture, training and evaluation metrics used in the study.

Dataset

To assess the deep-learning-based classification method, the Intrusion Detection dataset (ISCX) 2016 from the Canadian Institute of Cybersecurity was used.The ISCX-VPN datasetcomprises Internet traffic transmitted via an encrypted Internet connection. Within the ISCX VPN category, six traffic categories are captured: VoIP, Streaming, Email, Chat, Peer-to-peer (P2P) traffic and File Transfer. The categories of the ISCX dataset are shown in the table 1 below

Table 1: Internet traffic categories and applications

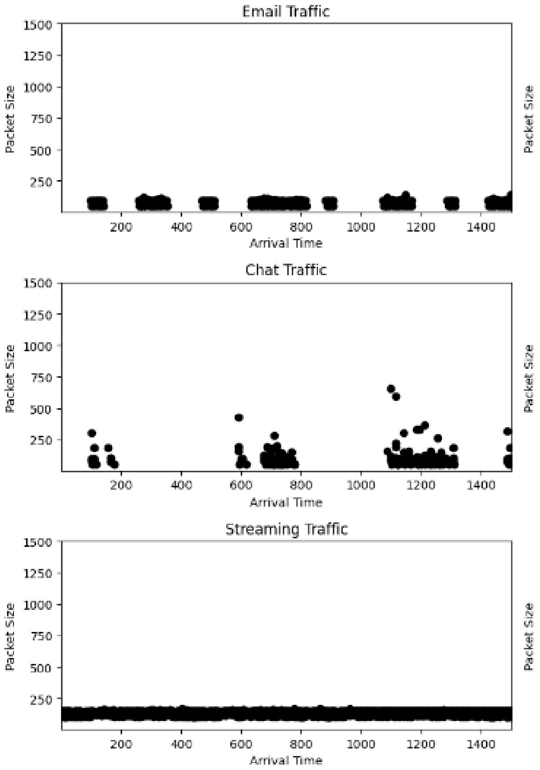
Traffic Category	VPN
Voice over IP (VoIP)	Google Hangouts, VoipBuster and Skype
Streaming	Netflix, YouTube and Vimeo
Email	Thunderbolt, SMTP, POP3 and Gmail
Chat	Facebook, Google Hangouts, Skype, IAM and ICQ
Peer to Peer (P2P)	Bittorrent and uTorrent

The dataset comprises packet capture files corresponding to specific application categories

Pre-processing and Image Construction

The ISCX Packets with similar 5-tuple attributes {source IP, source port, destination IP. Destination port, protocol}. The image construction approach used by [24] was adopted in this work, packets from the ISCX dataset were converted to packet flows with a size of 100 Bytes.These packets were converted to flow-based two-dimensional histograms. The histograms were construced by plotting the packet-arrival time on the X-axis and the packet size for packets in a packet flow on the Y-axis.

Figure 1 illustrates the histograms for the various categories captured from the ISCX dataset.



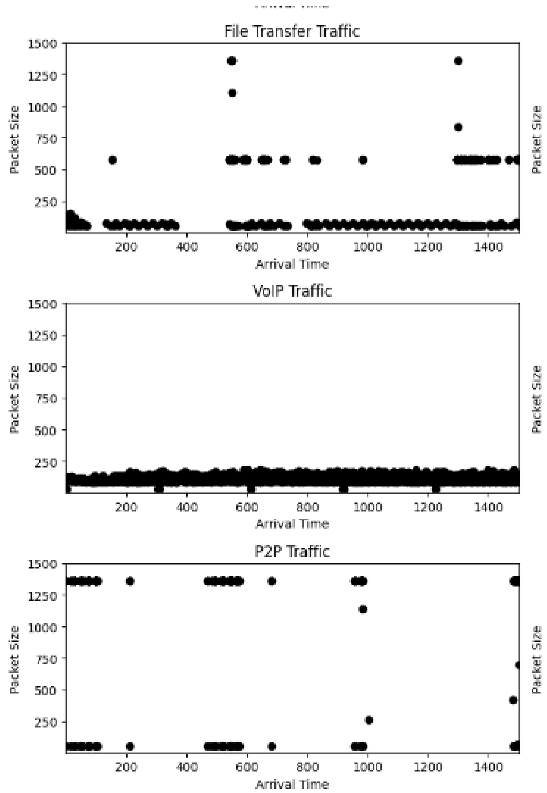


Figure 1: Two-dimensional histograms constructed for Chat, Email, File Transfer, VoIP, P2P and Streaming categories

Network Architecture

The DenseNet architecture comprises the convolution, pooling and fully connected layers with each utilising a non-linear transformation whereH_l = indexes the layer H_l. Transformation operations such as convolution, pooling, batch normalization, rectified linear units are carried out at each respective layer. The pooling layers in the architecture are divided into multiple dense blocks. These operations are condensed into multiple densely connected *Blocks*. Figure 2 below illustrates the architecture of DenseNet with 3 Dense blocks.

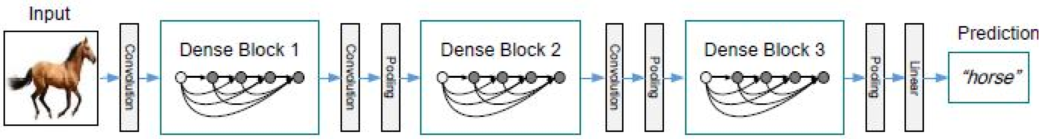


Figure 2: DenseNet Architecture (Source: Huang et al. (2016))

Figure 3 depicts the compression layer added to the DenseNet architecture in the proposed architecture.

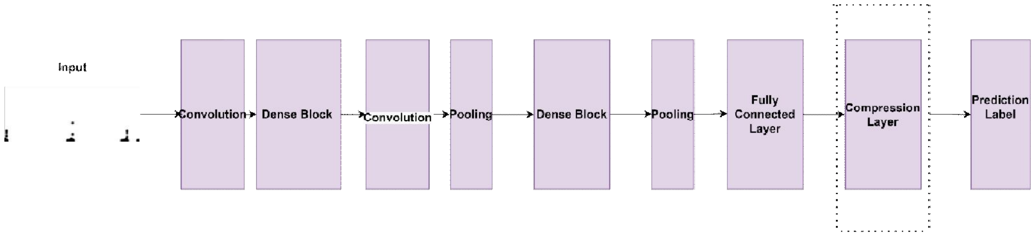


Figure 3: Enhanced DenseNet Architecture with Compression Layer

The three major components of the proposed architecture are discussed below:

Convolutional Layer: The convolutional layer is a fundamental part of CNN. An input tensor is transformed into an output tensor by convolving the input with filters. It is done for input images with a size $W_1 \times H_1 \times C_1$ and accepts four hyper-parameters namely: the number of filters, their spatial extent, the zero padding between the borders of the input and a stride with which filters are applied to each image.

Pooling Layer: The pooling layers reduce the size of representations with fixed downsampling transformation. Each channel in the input is independent of others and are downsampled spatially.

Compression Layer: The conventional DenseNet architecture consists of a compression layer that is used to reduce the number of feature maps. However, this approach relies on arbitrairlysetting the compression factor. In this study, the neurons in the fully connected layers are pruned using the Upper Confidence Multi-Armed Bandits Algorithm which is integrated into the enhamcedDenseNet. This approach provides a more efficient means of reducing the number of feature maps thereby compressing the DenseNet without degrading classification performance.

Experimental Setup

The dataset used in this research was stored in Google Drive.The Google Colaboratory environment was used for training and evaluation of the architecture to enable the use of its free GPU resources. Empirical tests were carried out to contrast and compare the enhanced and conventional DenseNet architecture. The DenseNet classifier were trained using Stochastic gradient descent with an initial learning rate set to 0.1, The RelU activation function andthe cross-entropy loss function were used to minimise loss. The dataset was split into 80% for training and 20% for testing.

Results and Discussion

The conventional and enhanced DenseNet architectures were evaluated. The two architectures were evaluated using performance metrics such as precision, recall, F1 Score, Area under the ROC Curve, and False positive Rate. Table 2 below shows the performance of the Conventional DenseNet architecture in the evaluation metrics. The Peer-to-peer Category recorded near-perfect results in all the metrics. Overall, the classifier provided a balance between precision and recall and controlled the false positive rates effectively. The Chat category displayed the lowest classification performance, a phenomenon that can be explained by the heterogenous nature of Chat traffic in general.

Table 2: Performance of Conventional DenseNet Classifier

	Precision	Recall	F1-Score	FPR	TP	TN	FN	FP
Chat	83	89	86	1.91	170	1781	22	34
Email	94	88	91	0.21	63	1888	9	4
File Transfer	91	83	87	1.61	276	1675	55	27
Peer to Peer (P2P)	99	98	98	0.40	453	1498	6	8
Streaming	84	96	89	3.09	268	1683	11	52
VoIP	96	94	95	2.36	721	1230	47	29

Figure 4 illustrates the confusion matrix of the conventional CNN classifier which shows that the P2P, Streaming and File Transfer recorded the best results. The classifier distinguishes between the various categories. The conventional classifier struggles with distinguishing between the VoIP and Streaming categories.

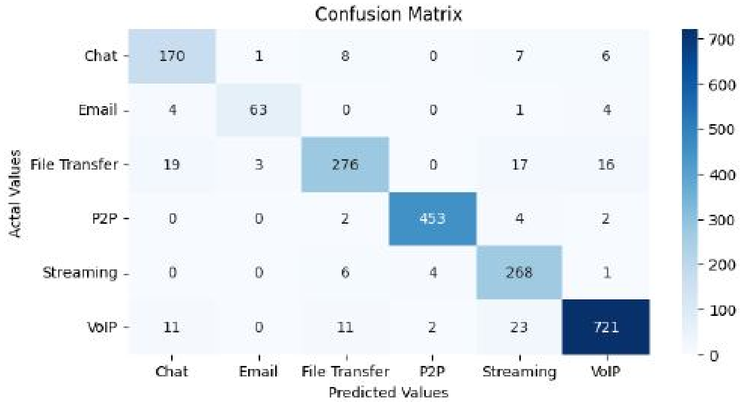


Figure 4: Confusion Matrix for DenseNet Classifier

The P2P recorded the highest AUC from the curve in the figure below, closely followed by Streaming, VoIP, Email and Chat categories.

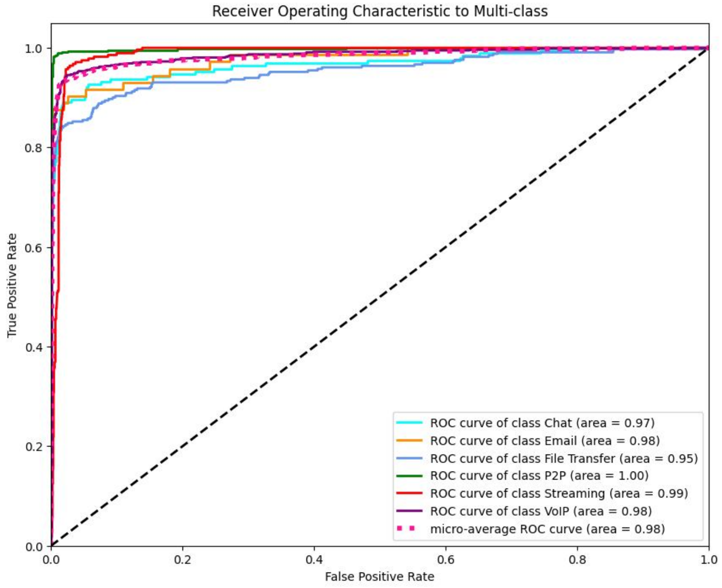


Figure 5: ROC Curve for DenseNet Classifier

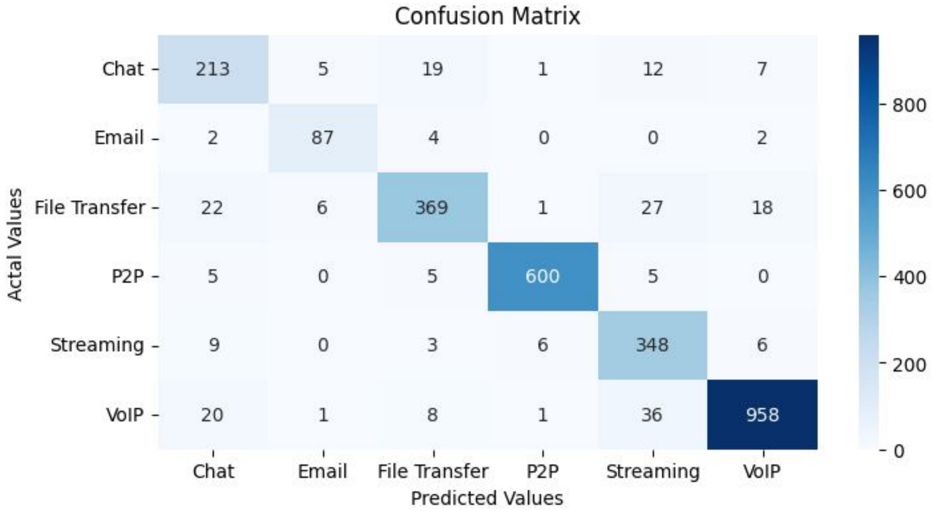
The classification performance of the Enhanced DenseNet architecture was also evaluated. Table shows the performance in metrics such as metrics such as precision, recall, F1 Score, Area under the ROC Curve, False positive Rate.The enhanced DenseNet architecture outperformed the conventional DenseNet architecture in the file transfer and streaming categories.

Table 3: Performance of Enhanced DenseNet Classifier

	Precision	Recall	F1-Score	FPR	TP	TN	FN	FP
Chat	81	85	83	2.5	213	2472	44	44

Email	90	94	90	0.48	87	2691	8	8
File Transfer	92	85	89	1.83	369	2324	74	74
P2P	99	100	100	0.46	600	2188	15	15
Streaming	83	96	89	1.54	348	2354	24	24
VoIP	99	96	97	0.82	33	1749	66	66

Figure which illustrates the confusion matrix shows that the VOIP category was the most correctly classified category followed by P2P, File Transfer, Streaming, Chat and Email. The enhanced classifier was able to distinguish between streaming and VoIP catgories unlike the conventional classifier.



	Chat	Email	File Transfer	P2P	Streaming	VoIP
Chat	213	5	19	1	12	7
Email	2	87	4	0	0	2
File Transfer	22	6	369	1	27	18
P2P	5	0	5	600	5	0
Streaming	9	0	3	6	348	6
VoIP	20	1	8	1	36	958

Figure 6: Confusion Matrix for Enhanced DenseNet Classifier

The ROC curves for all the categories show impressive performance across all the traffic categories. P2P has the highest classification followed by Email, Streaming, Chat and File Transfer. Overall, the classifier maintains high positive rates for all categories while maintaining low false positive rates.

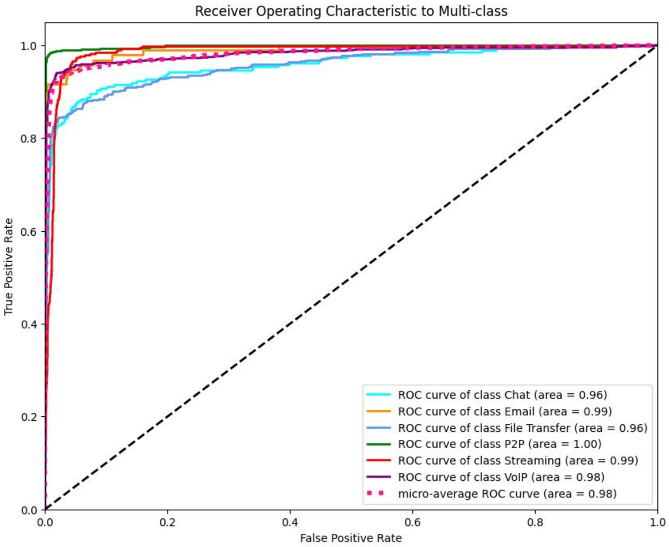


Figure 7: ROC Curve for Enhanced DenseNet Classifier

Conclusion and Future Work

In this paper, we introduce a novel DenseNet architecture for identifying Internet traffic application categories. Experimental results show that the approach used in this study outperforms the conventional DenseNet architecture. The key insight behind the approach utilised is the conversion of traffic flows into images. As shown, the flow-feature statistics-based approach used is able to successfully distinguish between encrypted Internet traffic categories. Future studies can optimize the DenseNet architecture further by compressing input images before feeding them into the classifier. Another approach would be to incorporate modalities such as payload and temporal features into the dataset to further improve the classification performance.

References

1. Ihm, S., & Pai, V. S. (2011). Towards understanding modern web traffic. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference* (pp. 295-312).
2. Wu, H., Zhang, X., & Yang, J. (2021). Deep learning-based encrypted network traffic classification and resource allocation in SDN. *Journal of Web Engineering*, *20*(8), 2319-2334.
3. 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.

4. He, X., Yang, Y., Zhou, W., Wang, W., Liu, P., & Zhang, Y. (2021). Fingerprinting mainstream IoT platforms using traffic analysis. *IEEE Internet of Things Journal*, *9*(3), 2083-2093.
5. Huang, G., Liu, Z., Van Der Maaten, L., & Weinberger, K. Q. (2017). Densely connected convolutional networks. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 4700-4708).
6. Yuan, C., Xia, Z., Jiang, L., Cao, Y., Wu, Q. J., & Sun, X. (2019). Fingerprint liveness detection using an improved CNN with image scale equalization. *IEEE Access*, *7*, 26953-26966.
7. Siddiqui, M. S. B., Islam, M. M., & Alam, M. G. R. (2024). An Extensive Study on D2C: Overfitting Remediation in Deep Learning Using a Decentralized Approach. *arXiv preprint arXiv:2411.15876*.
8. Iliyasu, A. S., & Deng, H. (2019). Semi-supervised encrypted traffic classification with deep convolutional generative adversarial networks. *Ieee Access*, *8*, 118-126.
9. Wang, Y., Gu, H. W., Yin, X. L., Geng, T., Long, W., Fu, H., & She, Y. (2024). Deep leaning in food safety and authenticity detection: An integrative review and future prospects. *Trends in Food Science & Technology*, 104396.
10. Luo, J., Chen, Z., Chen, W., Lu, H., & Lyu, F. (2025). A study on the application of the T5 large language model in encrypted traffic classification. *Peer-to-Peer Networking and Applications*, *18*(1), 1-13.
11. Chin, T. W., Morcos, A. S., & Marculescu, D. (2020). Pareco: Pareto-aware channel optimization for slimmable neural networks. *arXiv preprint arXiv:2007.11752*, *1*.
12. Lin, G., Chen, F., Zhang, Z., Zhang, A., Wang, X., & Zhou, C. (2023y). DenseNeXt: An Efficient Backbone for Image Classification. In *2023 15th International Conference on Advanced Computational Intelligence (ICACI)* (pp. 1-6). IEEE.
13. Roy, A. G., Navab, N., & Wachinger, C. (2018). Concurrent spatial and channel 'squeeze & excitation'in fully convolutional networks. In *Medical Image Computing and Computer Assisted Intervention–MICCAI 2018: 21st International Conference, Granada, Spain, September 16-20, 2018, Proceedings, Part I* (pp. 421-429). Springer International Publishing.

14. Yu, D., Yang, J., Zhang, Y., & Yu, S. (2021). Additive DenseNet: Dense connections based on simple addition operations. *Journal of Intelligent & Fuzzy Systems*, *40*(3), 5015-5025.

15. Wang, W., Hu, Y., Zou, T., Liu, H., Wang, J., & Wang, X. (2020). A new image classification approach via improved MobileNet models with local receptive field expansion in shallow layers. *Computational Intelligence and Neuroscience*, *2020*(1), 8817849.

16. Azar, J., Makhoul, A., & Couturier, R. (2020). Using DenseNet for IoT multivariate time series classification. In *2020 IEEE Symposium on Computers and Communications (ISCC)* (pp. 1-6). IEEE.

17. Yin, L., Hong, P., Zheng, G., Chen, H., & Deng, W. (2022). A novel image recognition method based on DenseNet and DPRN. *Applied Sciences*, *12*(9), 4232.

18. Silivery, A. K., Rao, K. R. M., & Kumar, S. L. (2024). Rap-Densenet Framework for Network Attack Detection and Classification. *Journal of Information & Knowledge Management*, 2450033.

19. Cao, Y., Liu, Z., Zhang, Z., Wang, R. L., Jia, M., & Gao, S. (2023). Dendritic Learning-Based DenseNet for Classification. In *2023 15th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC)* (pp. 112-115). IEEE.

20. Chu, H. C., Chang, L. L., & Chiang, H. C. (2022). A Traffic Classification Method for Internet Application Services Based on DNN. In *2022 International Conference on Electrical, Computer and Energy Technologies (ICECET)* (pp. 1-6). IEEE.

21. Choubey, R. N., Amar, L., Khare, S., & Venkanna, U. (2019, December). Internet traffic classifier using artificial neural network and 1D-CNN. In *2019 International Conference on Information Technology (ICIT)* (pp. 291-296). IEEE.

22. Shahraki, A., Abbasi, M., Taherkordi, A., & Kaosar, M. (2021, August). Internet traffic classification using an ensemble of deep convolutional neural networks. In *Proceedings of the 4th FlexNets Workshop on Flexible Networks Artificial Intelligence Supported Network Flexibility and Agility* (pp. 38-43).

23. 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.

24. Shapira, T., and Shavitt, Y. (2021). FlowPic: A generic representation for encrypted traffic classification and applications identification. *IEEE Transactions on Network and Service Management*, 18(2), 1218-1232.