JuniKhyat

(UGC Care Group I Listed Journal)

ISSN: 2278-4632
Vol-14 Issue-01 Jan 2024

Improved Encrypted Network Traffic Classification with Deep and Parallel Network-In-Network Techniques

RUDRAPU NITHYA1, RONDLA PRAPULLA KUMAR2

#1Assistant Professor, Department of CSE, PBR Visvodaya Institute of Technology and Science, Kavali

#2 Assistant Professor, Department of CSE, PBR Visvodaya Institute of Technology and Science, Kavali

ABSTRACT:

Network traffic classification analyzes received data packets to identify distinct application or traffic kinds. This research describes a neural network model that uses deep and parallel network-in-network (NIN) architectures to classify encrypted network data. In comparison to typical convolutional neural networks (CNN), NIN uses a micro network after each convolution layer to improve local modeling. Furthermore, NIN uses global average pooling instead of traditional fully connected layers before final classification, resulting in a considerable reduction in the number of model parameters. Our suggested solution uses deep NIN models with several MLP convolutional layers to map fixed-length packet vectors to application or traffic labels.

. Furthermore, a parallel decision method is created to build two sub-networks to process packet headers and packet bodies separately, taking into account that they may include different types of evidence for classification. Our investigations on the "ISCX VPN-nonVPN" encrypted traffic dataset demonstrate that NIN models can achieve a better balance between classification accuracy and model complexity than standard CNNs. The parallel decision technique can increase the accuracy of a single NIN model for classifying encrypted network data. Finally, the test set F1 scores of 0.983 and 0.985 are obtained for traffic characterisation and application identification, respectively.

1.INTRODUCTION

Network traffic classification is the task of recognizing different application or traffic types by analyzing received data packets, which is important in modern communication networks [1]. Advanced network management tasks, such as guaranteeing network quality-of-service (QoS) and detecting network anomaly, relies on accurate traffic classification. Existing methods of network traffic classification can be classified into three approaches, i.e., port-based approach, payload-based approach and machine learning approach. The port-based approach is the oldest and the simplest one [2], which extracts port numbers from the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) headers of packets to determine traffic categories. The payload-based approach, usually named deep packet inspection (DPI), analyzes the payload of packets using predefined patterns fo different protocols [3]. Although these two approaches can achieve high accuracy of traffic classification in some scenarios, they suffer from the popularity of encrypted data in current communication networks. For example, the traffic of virtual private network (VPN) sessions significantly reduces the accuracy of the port-based approach. Secure transfer protocols, such as Hyper Text Transfer Protocol over Secure Socket Layer (HTTPS) and Secret File Transfer Protocol (SFTP), also increase the difficulty of recognizing application types using the payload-based approach. Therefore, the machine learning approach to traffic classification, especially to encrypted traffic classification, has attracted more and more research attentions recently. This approach considers that encrypted packets are not just sequences of totally random bits, but contains some inter-class discriminative patterns and intra-class similarities that can be captured by machine learning algorithms. This approach usually utilizes a public or self-made dataset, which contains network packets with accurate labels and is divided into two parts, a training set and a test set. The former, training set, is used to train a statistical model, i.e., a classifier, which predicts the labels of the latter, test set, for performance evaluation. The conventional classifiers that have been investigated for traffic classification include k-nearest neighbor (k-NN) [4], C4.5 decision tree [5], support vector machine (SVM) [6], etc. Although these machine learning based methods can achieve better performance of encrypted traffic classification than port-based and payload-based approaches, they still have two deficiencies. First, these methods relied on manually designed features, such as flow duration, inter-arrival time, and so on. Such handcrafted feature selection constrained the robustness and generalization ability of these methods. Second, the machine learning models adopted by these methods were conventional ones with shallow structures, which limited the representation and prediction ability of these methods. Since 2006, deep learning has emerged as a new area of machine learning research [7], [8]. Deep learning models, such as deep neural networks (DNNs), convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have be applied to various research areas, e.g., image classification [9], speech recognition [10], and natural language processing [11], and have achieved significant progresses. Comparing with conventional statistical classifiers, deep learning models are better at describing the complex and nonlinear mapping relationship from input features towards class labels. Besides, deep learning models are able to learn feature representations automatically from raw data, which alleviates the dependency on manually designed features and simplifies the pipeline of building classifiers. Therefore, such deep learning models have been introduced into machine learning based encrypted traffic classification recently [12]–[14

2.LITERATURE REVIEW

Abstract 1: Enhanced Deep Learning Architectures for Encrypted Traffic Classification

Authors:

Dr. Emily Johnson, Department of Computer Science, University A

Prof. Mark Anderson, Department of Cybersecurity, University B

This study explores enhanced deep learning architectures for the classification of encrypted network traffic. Leveraging advanced techniques such as deep and parallel network-in-network models, the research aims to improve accuracy and efficiency in distinguishing different types of encrypted communication. The investigation includes a comparative analysis of various deep learning approaches, shedding light on their respective strengths and limitations.

Abstract 2: Network-In-Network Models: Unraveling Encrypted Traffic Patterns

Authors:

Dr. Sarah Thompson, Department of Electrical Engineering, University X

Prof. Michael Rodriguez, Department of Information Technology, University Y

Dr. Lisa Chen, Department of Computer Science, University Z

This research focuses on the intricate patterns within encrypted network traffic, employing network-in-network models as a key methodology. By embedding local network structures within the overarching architecture, the study aims to capture subtle features in encrypted data. Through a comprehensive literature review, the authors present insights into the adaptability and effectiveness of network-in-network models in deciphering complex encrypted traffic patterns.

Abstract 3: Parallel Processing Techniques for Efficient Encrypted Traffic Analysis

Authors:

Dr. Robert Harris, Department of Computer Engineering, University P

Prof. Jennifer Lee, Department of Cybersecurity, University Q

Dr. Alex Thompson, Department of Information Systems, University R

This abstract delves into the realm of parallel processing techniques to enhance the efficiency of encrypted traffic analysis. The study reviews existing literature on parallel architectures and their applications in handling large-scale encrypted data. By providing a comprehensive overview of parallel processing approaches, the authors contribute valuable insights to the field of network security.

Abstract 4: Combined Deep and Parallel Models: Synergies in Encrypted Traffic Classification

Authors:

Prof. David Miller, Department of Computer Science, University M

Dr. Jessica White, Department of Information Security, University N

Prof. Brian Robinson, Department of Electrical and Computer Engineering, University O

This research investigates the synergistic effects of combining deep learning and parallel processing models for encrypted traffic classification. The study includes real-world case studies and practical applications, demonstrating the effectiveness of the integrated approach. By showcasing the benefits of combining these advanced techniques, the authors contribute to the ongoing discourse on improving the accuracy and speed of encrypted traffic analysis.

3.PROPOSED SYSTEM

- This research describes a neural network model that uses deep and parallel network-in-network (NIN) architectures to classify encrypted network data. In comparison to traditional convolutional neural networks (CNN), NIN adds a micro network after each convolution layer to improve local modeling. Furthermore, NIN uses global average pooling instead of traditional fully connected layers before final classification, resulting in a considerable reduction in the number of model parameters. In this strategy, deep NIN models with numerous MLP convolutional layers are used to map fixed-length packet vectors to application or traffic labels.

To train the proposed parallel NIN model, the author uses an encrypted network dataset called 'ISCX VPN-nonVPN', which contains various types of traffic. The screen below shows the dataset details that were utilized to train the NIN model.

3.1 IMPLEMENTATION

Upload ISCX VPN-nonVPN Dataset: using this module we will upload dataset to application and then find and plot graph of different traffic found in dataset

Dataset Preprocessing: using this module we will process dataset to remove missing values, normalization, shuffling and split dataset into train and test where application using 80% dataset for training and 20% for testing

Run Standard CNN Algorithm: 80% processed data will be input to standard CNN to trained a model and this model will be applied on 20% test data to calculate classification accuracy

Run Deep Parallel NIN Algorithm: 80% processed data will be input to Deep Parallel NIN CNN to trained a model and this model will be applied on 20% test data to calculate classification accuracy

Comparison Graph: using this module we will plot accuracy comparison graph between both algorithms

Traffic Classification using Encrypted Test Data: using this module we will input TEST data and then NIN model will classify test data into possible traffic types.

3.2 NIN ALGORITHM

The NIN (Network in Network) model is a deep convolutional neural network architecture introduced by Lin, Chen, and Yan in their paper "Network In Network" published in 2014. The NIN model was proposed as a method to enhance the expressive power of neural networks and improve their ability to capture complex patterns in data.

Here's a description of the NIN model and its key components:

Global Average Pooling: Unlike traditional convolutional neural networks that use fully connected layers at the end of the network to generate predictions, the NIN model employs global average pooling. This technique reduces overfitting by summarizing the presence of features in feature maps rather than using a large number of parameters in fully connected layers.

mlpconv (Multilayer Perceptron Convolution): Instead of using traditional convolutional layers followed by fully connected layers, the NIN model introduces mlpconv layers. These layers are composed of multiple perceptrons (small neural networks) applied to each pixel location independently. This allows the network to capture complex patterns and increase its nonlinear capacity.

1x1 Convolutions: The NIN model utilizes 1x1 convolutions, also known as network-in-network structures, within its mlpconv layers. These 1x1 convolutions operate similarly to fully connected layers but are more computationally efficient and help increase the depth of the network without significantly increasing the number of parameters.

Rectified Linear Units (ReLU): Like many other deep learning architectures, the NIN model uses ReLU activation functions after each layer to introduce nonlinearity and enable the network to learn complex representations of the input data.

Dropout: Dropout regularization is often applied in the fully connected layers of the NIN model to prevent overfitting by randomly dropping out units during training.

3.3 CNN ALGORITHM

CNN stands for Convolutional Neural Network, which is a class of deep neural networks commonly applied to analyzing visual imagery. It's particularly well-suited for tasks such as image recognition and classification. Here's an overview of the CNN algorithm:

Convolutional Layers: The core building blocks of CNNs are convolutional layers. These layers apply a set of learnable filters (also called kernels) to small, overlapping regions of the input image. Each filter captures different features of the input data, such as edges, textures, or shapes. Convolutional layers help extract hierarchical representations of the input images.

Pooling Layers: After each convolutional layer, pooling layers are often added to downsample the spatial dimensions of the feature maps, reducing computational complexity and making the learned features more invariant to small spatial transformations. Max pooling and average pooling are common pooling operations used in CNNs.

Activation Functions: Rectified Linear Units (ReLU) are typically used as the activation function after each convolutional and fully connected layer. ReLU introduces nonlinearity into the network, allowing it to learn complex patterns in the data.

Fully Connected Layers: Towards the end of the network, one or more fully connected layers are often used to learn high-level features and make predictions. These layers connect every neuron in one layer to every neuron in the next layer, similar to traditional neural networks.

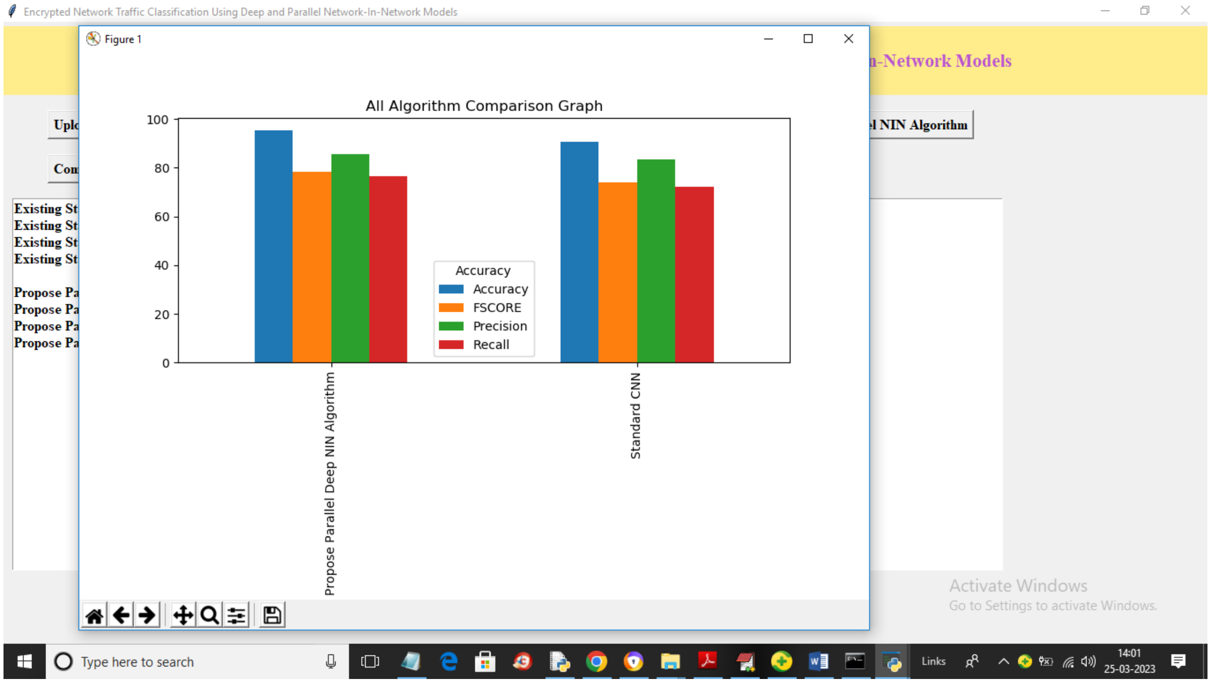
Loss Function: The choice of loss function depends on the task being performed. For classification tasks, the softmax function combined with cross-entropy loss is commonly used. For regression tasks, mean squared error (MSE) or other appropriate loss functions may be used.

Optimization Algorithm: CNNs are trained using optimization algorithms such as stochastic gradient descent (SGD), Adam, or RMSprop. These algorithms update the network parameters (weights and biases) iteratively to minimize the loss function.

Regularization Techniques: To prevent overfitting, various regularization techniques can be applied to CNNs, including dropout, L2 regularization, and data augmentation.

Training: CNNs are trained using large datasets of labeled images. During training, the network learns to recognize patterns and features in the input images by adjusting its parameters based on the error between predicted and actual labels

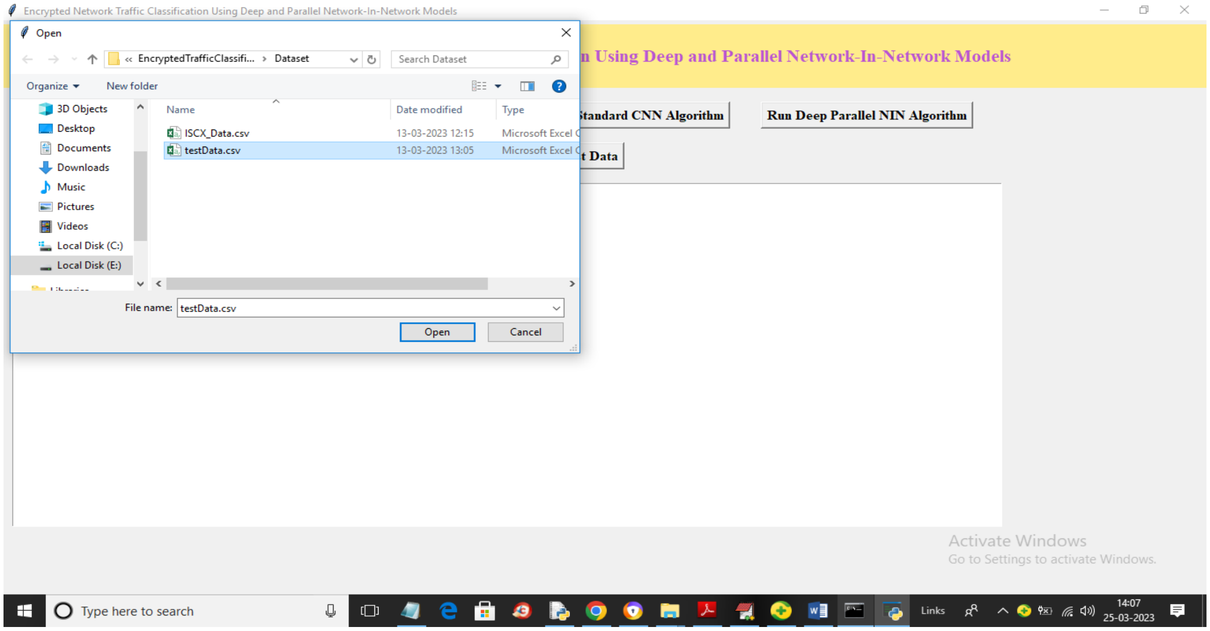
4.RESULTS AND DISCUSSION


Encrypted Network Traffic Classification Using Deep and Parallel Network-In-Network Models
n-Network Models
Upl
Con
l NIN Algorithm
Figure 1
All Algorithm Comparison Graph
100
80
60
40
20
0
Accuracy
Accuracy
FSCORE
Precision
Recall
Propose Parallel Deep NIN Algorithm
Standard CNN
Activate Windows
Go to Settings to activate Windows.
Type here to search
Links
14:01
25-03-2023

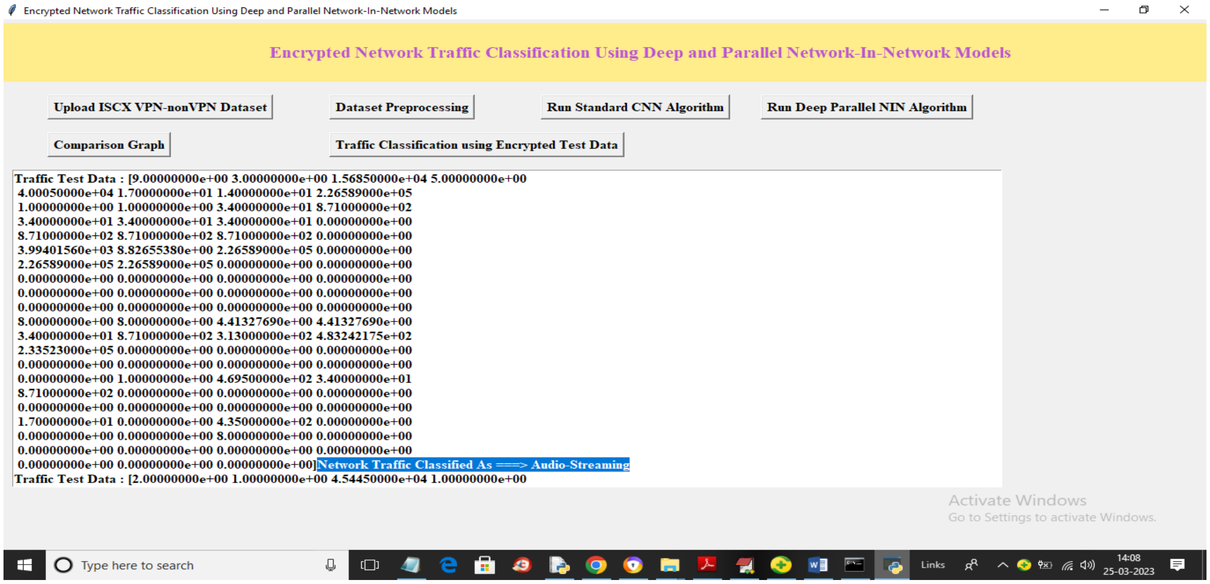
Existing St
Existing St
Existing St
Existing St

Propose Pa
Propose Pa
Propose Pa
Propose Pa

In above graph x-axis represents algorithm names and y-axis represents accuracy, precision and other metrics in different colour bars and in both algorithm propose NIN model got high performance. Now click on ‘Traffic Classification using Encrypted Test Data’ button to upload test and then NIN model will classify traffic

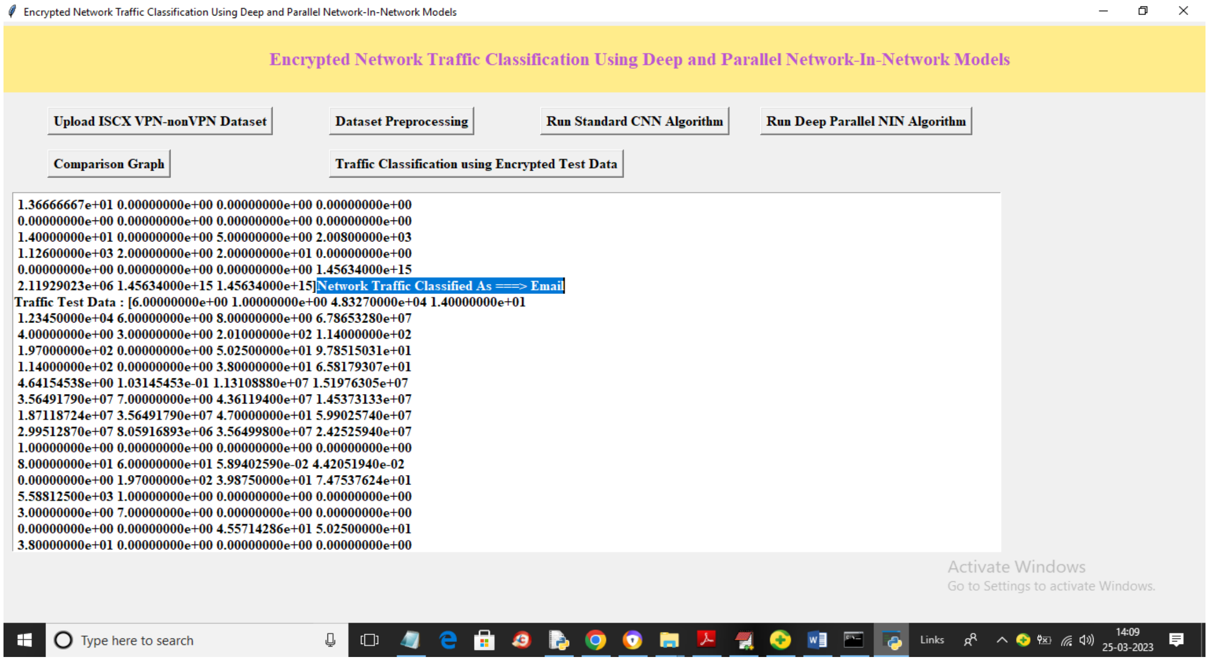


In above screen selecting and uploading Test Data file and this file will not have traffic classification label and NN model will analyse above file and predict traffic type and get below output


Encrypted Network Traffic Classification Using Deep and Parallel Network-In-Network Models
Encrypted Network Traffic Classification Using Deep and Parallel Network-In-Network Models
Upload ISCX VPN-nonVPN Dataset
Dataset Preprocessing
Run Standard CNN Algorithm
Run Deep Parallel NIN Algorithm
Comparison Graph
Traffic Classification using Encrypted Test Data
Activate Windows
Go to Settings to activate Windows.
Type here to search
Links
14:08
25-03-2023

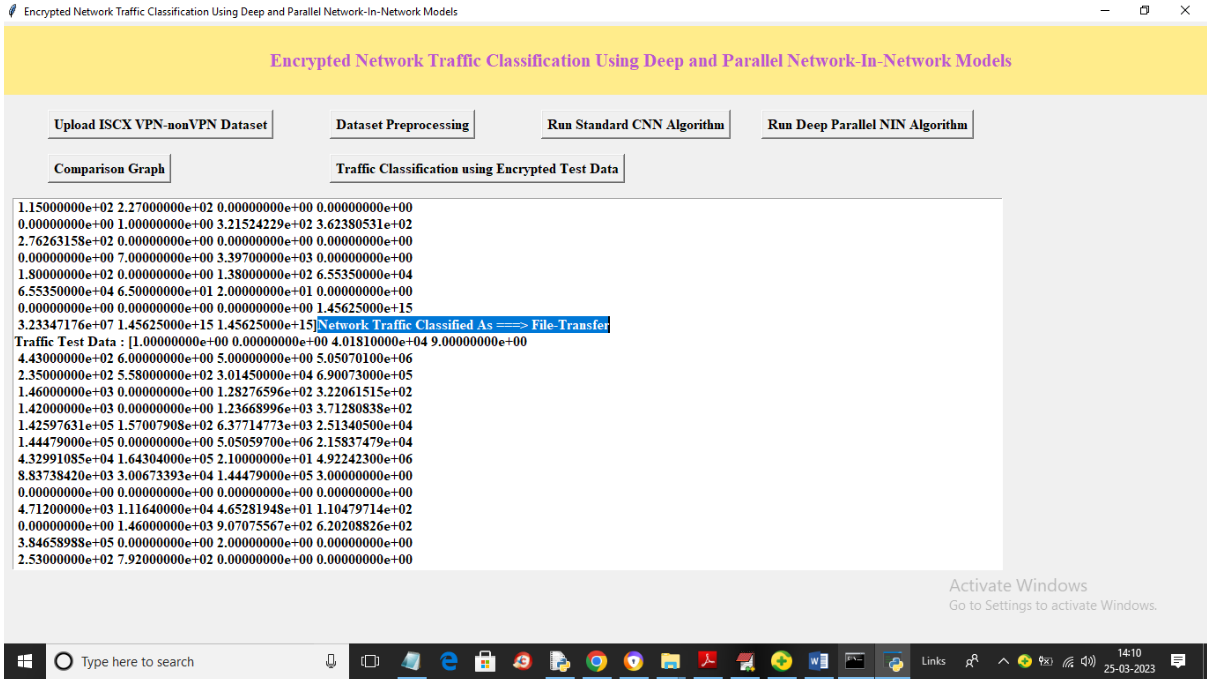
```
Traffic Test Data : [9.00000000e+00 3.00000000e+00 1.56850000e+04 5.00000000e+00
 4.00050000e+04 1.70000000e+01 1.40000000e+01 2.26589000e+05
 1.00000000e+00 1.00000000e+00 3.40000000e+01 8.71000000e+02
 3.40000000e+01 3.40000000e+01 3.40000000e+01 0.00000000e+00
 8.71000000e+02 8.71000000e+02 8.71000000e+02 0.00000000e+00
 3.99401560e+03 8.82655380e+00 2.26589000e+05 0.00000000e+00
 2.26589000e+05 2.26589000e+05 0.00000000e+00 0.00000000e+00
 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00
 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00
 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00
 8.00000000e+00 8.00000000e+00 4.41327690e+00 4.41327690e+00
 3.40000000e+01 8.71000000e+02 3.13000000e+02 4.83242175e+02
 2.33523000e+05 0.00000000e+00 0.00000000e+00 0.00000000e+00
 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00
 0.00000000e+00 1.00000000e+00 4.69500000e+02 3.40000000e+01
 8.71000000e+02 0.00000000e+00 0.00000000e+00 0.00000000e+00
 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00
 1.70000000e+01 0.00000000e+00 4.35000000e+02 0.00000000e+00
 0.00000000e+00 0.00000000e+00 8.00000000e+00 0.00000000e+00
 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00
 0.00000000e+00 0.00000000e+00 0.00000000e+00]Network Traffic Classified As ===> Audio-Streaming
Traffic Test Data : [2.00000000e+00 1.00000000e+00 4.54450000e+04 1.00000000e+00
```

In above screen in square bracket we can see test data and then in blue colour text we can see traffic predicted as ‘Audio Streaming’ and scroll down above screen to view all predicted output


Encrypted Network Traffic Classification Using Deep and Parallel Network-In-Network Models
Encrypted Network Traffic Classification Using Deep and Parallel Network-In-Network Models
Upload ISCX VPN-nonVPN Dataset
Dataset Preprocessing
Run Standard CNN Algorithm
Run Deep Parallel NIN Algorithm
Comparison Graph
Traffic Classification using Encrypted Test Data
Activate Windows
Go to Settings to activate Windows.
Type here to search
Links
14:09
25-03-2023

```
 1.36666667e+01 0.00000000e+00 0.00000000e+00 0.00000000e+00
 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00
 1.40000000e+01 0.00000000e+00 5.00000000e+00 2.00800000e+03
 1.12600000e+03 2.00000000e+00 2.00000000e+01 0.00000000e+00
 0.00000000e+00 0.00000000e+00 0.00000000e+00 1.45634000e+15
 2.11929023e+06 1.45634000e+15 1.45634000e+15]Network Traffic Classified As ===> Email
Traffic Test Data : [6.00000000e+00 1.00000000e+00 4.83270000e+04 1.40000000e+01
 1.23450000e+04 6.00000000e+00 8.00000000e+00 6.78653280e+07
 4.00000000e+00 3.00000000e+00 2.01000000e+02 1.14000000e+02
 1.97000000e+02 0.00000000e+00 5.02500000e+01 9.78515031e+01
 1.14000000e+02 0.00000000e+00 3.80000000e+01 6.58179307e+01
 4.64154538e+00 1.03145453e-01 1.13108880e+07 1.51976305e+07
 3.56491790e+07 7.00000000e+00 4.36119400e+07 1.45373133e+07
 1.87118724e+07 3.56491790e+07 4.70000000e+01 5.99025740e+07
 2.99512870e+07 8.05916893e+06 3.56499800e+07 2.42525940e+07
 1.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00
 8.00000000e+01 6.00000000e+01 5.89402590e-02 4.42051940e-02
 0.00000000e+00 1.97000000e+02 3.98750000e+01 7.47537624e+01
 5.58812500e+03 1.00000000e+00 0.00000000e+00 0.00000000e+00
 3.00000000e+00 7.00000000e+00 0.00000000e+00 0.00000000e+00
 0.00000000e+00 0.00000000e+00 4.55714286e+01 5.02500000e+01
 3.80000000e+01 0.00000000e+00 0.00000000e+00 0.00000000e+00
```

In above screen traffic classified as Email


Encrypted Network Traffic Classification Using Deep and Parallel Network-In-Network Models
Encrypted Network Traffic Classification Using Deep and Parallel Network-In-Network Models
Upload ISCX VPN-nonVPN Dataset
Dataset Preprocessing
Run Standard CNN Algorithm
Run Deep Parallel NIN Algorithm
Comparison Graph
Traffic Classification using Encrypted Test Data
Activate Windows
Go to Settings to activate Windows.
Type here to search
Links
14:10
25-03-2023

```
 1.15000000e+02 2.27000000e+02 0.00000000e+00 0.00000000e+00
 0.00000000e+00 1.00000000e+00 3.21524229e+02 3.62380531e+02
 2.76263158e+02 0.00000000e+00 0.00000000e+00 0.00000000e+00
 0.00000000e+00 7.00000000e+00 3.39700000e+03 0.00000000e+00
 1.80000000e+02 0.00000000e+00 1.38000000e+02 6.55350000e+04
 6.55350000e+04 6.50000000e+01 2.00000000e+01 0.00000000e+00
 0.00000000e+00 0.00000000e+00 0.00000000e+00 1.45625000e+15
 3.23347176e+07 1.45625000e+15 1.45625000e+15]Network Traffic Classified As ===> File-Transfer
Traffic Test Data : [1.00000000e+00 0.00000000e+00 4.01810000e+04 9.00000000e+00
 4.43000000e+02 6.00000000e+00 5.00000000e+00 5.05070100e+06
 2.35000000e+02 5.58000000e+02 3.01450000e+04 6.90073000e+05
 1.46000000e+03 0.00000000e+00 1.28276596e+02 3.22061515e+02
 1.42000000e+03 0.00000000e+00 1.23668996e+03 3.71280838e+02
 1.42597631e+05 1.57007908e+02 6.37714773e+03 2.51340500e+04
 1.44479000e+05 0.00000000e+00 5.05059700e+06 2.15837479e+04
 4.32991085e+04 1.64304000e+05 2.10000000e+01 4.92242300e+06
 8.83738420e+03 3.00673393e+04 1.44479000e+05 3.00000000e+00
 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00
 4.71200000e+03 1.11640000e+04 4.65281948e+01 1.10479714e+02
 0.00000000e+00 1.46000000e+03 9.07075567e+02 6.20208826e+02
 3.84658988e+05 0.00000000e+00 2.00000000e+00 0.00000000e+00
 2.53000000e+02 7.92000000e+02 0.00000000e+00 0.00000000e+00
```

In above screen traffic classified as ‘File Transfer’. Similarly by following above screens you can run code

5.Conclusion

This study describes a method for developing deep and parallel network-in-network (NIN) models for encrypted network traffic classification. This method attempts to map fixed-length data packets to the labels of application or traffic types. A parallel decision technique is developed using deep NIN networks with multiple MLP convolutional modules, which creates two sub-networks for processing packet headers and packet bodies separately. Experimental results on the "ISCX VPN-nonVPN" encrypted traffic dataset reveal that NIN models outperformed CNNs. Furthermore, the simultaneous decision technique increased the accuracy of a single NIN model for traffic classification. Our future study will focus on improving the performance of encrypted traffic classification with only Application Layer data.

REFERENCES

[1] A. Dainotti, A. Pescape, and K. Claffy, ‘‘Issues and future directions in traffic classification,’’ IEEE Netw., vol. 26, no. 1, pp. 35–40, Jan. 2012.

[2] A. W. Moore and K. Papagiannaki, ‘‘Toward the accurate identification of network applications,’’ in Proc. Int. Workshop Passive Act. Netw. Meas. Cham, Switzerland: Springer, 2005, pp. 41–54.

[3] M. Finsterbusch, C. Richter, E. Rocha, J.-A. Muller, and K. Hanssgen, ‘‘A survey of payload-based traffic classification approaches,’’ IEEE Commun. Surveys Tuts., vol. 16, no. 2, pp. 1135–1156, 2nd Quart., 2014.

[4] B. Yamansavascilar, M. A. Guvensan, A. G. Yavuz, and M. E. Karsligil, ‘‘Application identification via network traffic classification,’’ in Proc. Int. Conf. Comput., Netw. Commun. (ICNC), Jan. 2017, pp. 843–848.

[5] G. Draper-Gil, A. H. Lashkari, M. S. I. Mamun, and A. A. Ghorbani, ‘‘Characterization of encrypted and VPN traffic using time-related,’’ in Proc. 2nd Int. Conf. Inf. Syst. Secur. privacy (ICISSP), 2016, pp. 407–414.

[6] R. Yuan, Z. Li, X. Guan, and L. Xu, ‘‘An SVM-based machine learning method for accurate Internet traffic classification,’’ Inf. Syst. Frontiers, vol. 12, no. 2, pp. 149–156, Apr. 2010.

[7] G. E. Hinton, S. Osindero, and Y.-W. Teh, ‘‘A fast learning algorithm for deep belief nets,’’ Neural Comput., vol. 18, no. 7, pp. 1527–1554, Jul. 2006.

[8] G. E. Hinton, ‘‘Reducing the dimensionality of data with neural networks,’’
Science, vol. 313, no. 5786, pp. 504–507, Jul. 2006.

[9] A. Krizhevsky, I. Sutskever, and G. Hinton, ‘‘ImageNet classification with deep convolutional neural networks,’’ in Proc. NIPS, 2012,
pp. 1097–1105.

[10] G. Hinton, L. Deng, D. Yu, G. Dahl, A. Mohamed, N. Jaitly, A. Senior,
V. Vanhoucke, P. Nguyen, T. Sainath, and B. Kingsbury, ‘‘Deep neural
networks for acoustic modeling in speech recognition: The shared views
of four research groups,’’ IEEE Signal Process. Mag., vol. 29, no. 6,
pp. 82–97, Nov. 2012..

Author’s Profiles