CrossRef DOI of original article: 10.34257/GJCSTHVOL21IS3PG1

Efficient Network Traffic Classification and Visualizing Abnormal Part via Hybrid Deep Learning Approach: Xception + Bidirectional GRU

MinJong Cheon

Received: 6 June 2021 Accepted: 1 July 2021 Published: 15 July 2021

Abstract

Due to a rapid development in the field of information and communication, the information technologies yielded novel changes in both individual and organizational operations. Therefore, the accessibility of information became easier and more convenient than before, and malicious approaches such as hacking or spying aimed at various information kept increasing. With the aim of preventing malicious approaches, both classification and detecting malicious traffic are vital. Therefore, our research utilized various deep learning and machine learning models for better classification. The given dataset consists of normal and malicious data and these data types are png files. In order to achieve precise classification, our experiment consists of three steps. Firstly, only vanilla CNN was used for the classification and the highest score was 86.2

Index terms—

1 Introduction a) Background

nformation and communication have experienced rapid growth in many ways over the past three generations. In particular, as the 3V (Volume, Velocity, and Variety) of information intensifies, users' freedom to access quality information also increases. Information technologies have brought new changes in both information usage between individuals and in business operations, such as introducing computerization to corporate marketing methods and sales management (Sanaei & Sobhani, 2018). However, as the communication environment develops in this digital transformation process, malicious approaches such as hacking or spying aimed at user personal information, corporate confidentiality, and financial information become a problem (Layton, 2021).

Ransom DDos, which accounts for the largest number of DDoS attacks carried out in 2020, is also achieved through service paralysis attacks that drain the system's resources by creating huge amounts of packets, similar to conventional DDoS attacks, and bandwidth exhaustion attacks that exhaust TCP connections. In addition, numerous global hacking groups are openly attacking and threatening companies in the financial sector and manufacturing industries to compensate for money while hiding in the anonymity of virtual currency. Therefore, detecting large -scale broadband networks and analyzing harmful traffic in advance, along with intrusion detection systems operating on a specific network or set list, is an important technology that can block malicious attacks from the source (Williams, 2021). We call data which causes security problems with bad intentions 'malicious traffic'. Malicious traffic causes security problems for individuals, businesses or countries and damages the device. In order to detect malicious traffic, there must be a technology which can distinguish between normal traffic and malicious traffic (Rose, 2021). The graph below shows a share of global web application attack traffic as of April 2018, by originating country (Statista, 2021). Most existing studies classified malicious and normal traffic with csv type files. Therefore, there were limited ways to classify malicious and normal traffic. More AI models can be used by using image files, not just csv files. In order to use more AI models, this study classified malicious and normal traffic with image data, allowing various deep learning models such as CNN, Xception and BI-GRU to be applied. To optimize image files for deep learning models, we preprocessed the images and applied them to diverse AI models. First of all, we applied CNN based models and altered the optimizers such as adam, nadam, sgd, rmsprop in order to find the best optimizers. Secondly, we extracted the features from the image data through

CNN and applied it to tree-based Machine learning models, such as Decision Tree Classifier, Random Forest Classifier and Extra Tree Classifier. Lastly, a hybrid deep learning based approach was used, which combines CNNbased Xception and RNN-based BI-GRU.

2 c) Related Works

Mohiuddin Ahmed and Abdun Naser Mahmood developed a framework for collective anomaly detection using k-means model, to discover abnormal traffics that look legitimate but are in fact targeted to disrupt normal computing environments (in this paper, DoS attack). The experiment results are based on a widely accepted DARPA dataset for intrusion detection from MIT Lincoln Laboratory. Input data extracted from network traffic, <SrcIP, DstIP, Protocol, Payload Length> is used for clustering and the data showed high probability of being DoS attack. CAD's key idea is that a group of traffic flows collectively. The paper identified DoS and other similar attacks as collective anomaly based on x-means clustering, a variant of k-means algo and eight times faster than k-means. CAD's accuracy was compared against CBLOF, LDCOF and k-means algorithms, and the result was 97%, 85%, 93% and 83% respectively (Ahmed & Mahmood, 2014).

Radford et al. demonstrated that network behaviors can be learned from traffic metadata using LSTM RNNs (which is able to detect patterns of traffic indicative of malicious computer system use without the assistance of labeled training data and visibility into each machine's internal state or processes) applied for anomaly detection. The research was motivated by cyber security (whose applications have been shifted from signature based matching methods to machine learning and statistical models) and NLP (communications between networked devices are captured in ordered sequence and the team expected its rule to be similar to grammar). They used a dataset that represents seven days of simulated network traffic with attack behaviors (such as infiltration, DoS, DDoS and SSH attack), from IDS tasks from the University of New Brunswick's Canadian Institute for Cyber security and ISCX. In methodology, each LSTM layer is composed of 50 hidden cells with linear activation, linear activation on the first layer and rectified linear activation on the second layer. Initial embedding layer projects input sequence from V unique tokens into a dense 100dimensional vector space. Entire dataset was trained with a ten-token sliding window, where each model was trained to predict the subsequent (eleventh) token. As a result, models based on proto-byte sequences produce higher AUC scores than any model based on service port sequence (Radford et al., 2018). R.Yuan, Z.Li and X.Guan proposed SVM-based ML model for internet traffic classification. The data has been obtained from a backbone router of the campus network of the author's university, 8-hour traffic data on a Gbps Ethernet link within a week. The packets were separated into unidirectional flow depending on five tuples (srcIP, desIP, Prot, srcPort, desPort) and combined into bi-directional flows from the overlapping time spans of the flows. 19 parameters were computed from the packet headers to be the discriminators for the classification algorithms and all parameters are obtainable in real time from the packet header, without storing the packet. SVM model classified the data with 19 parameters, which has been pretreated using logarithm function. 10-fold cross validation analyzed 4 kernel functions' accuracy and RBF showed highest accuracy, 93.38%. The classes with more training samples (WWW and service) had low false negative ratios (0.20% and 0.00% respectively), which is comparatively smaller than classes with fewer training samples. To find an optimizing discriminator, a sequential forward selection method was used and the weighted average of classification accuracy across all traffic classes is 99.42%. 99.42% accuracy has been achieved with regular biased training, 97.17% with unbiased sample. RBF kernel based SVM model is also applicable to encrypted network traffic and real-time traffic identification. Since supervised machine learning has inadequacy in that it requires a large labeled dataset, they look forward to combining supervised and unsupervised machine learning with feature parameters obtainable early in the traffic flow for fleet and precise internet traffic classification (Yuan et al., 2008).

As crimes in computer networks expand, realtime analysis has become essential in network intrusion detection systems (IDS). Enhanced encryption and new ways of avoiding detection led to the need for exquisite classification technology. Traditional method (port based classification) and its advanced method (payload based classification) both showed shortage and thus researchers started to utilize ML in IDS to detect malicious activities.

3 Materials and Methods

4 a) Data Description

The dataset is collected from the kaggle website, which is available at https://www.kaggle.com/ sohelranaccse-lab/trffffffffffffffff/metadata. This dataset is described in the research paper "Intrusion Detection using Network Traffic Profiling and Machine Learning for IoT Applications". The given data source includes 856 photos of 518 malicious traffic photos and 338 normal traffic photos. It is supposed to perform binary classification. As the dataset contains less images for the deep learning algorithms, we utilized image data generator function from the Keras for the data augmentation. Furthermore, all of the images in the dataset were divided into 255 for the standardi zation (MALICIOUS NETWORK TRAFFIC PCAPS-202, 2021). Convolutional neural network (CNN) is one of the main artificial intelligence(AI) models to recognize and classify images. When the CNN model classifies an image, the image is used as an input and the feature values are extracted by the CNN model as output. Some neurons in the previous layer are connected to individual neurons in the next layer and this local correlation is called the receptive field and forms a weight vector. The regional features are extracted by using a receptive field. Since neurons in the plane share the same weight, similar features at different regions of the input data can be searched. Filter or kernel is the weight vector of CNN which slides the input vector to create the feature map. The method of sliding the filter horizontally and vertically to make weight vectors is called convolutional operation. The convolutional operation extracts features from the input image in a single layer which is representing a unique feature. Due to the local receptive field, the number of parameters to train decreases a lot. Once a feature is detected, the exact region of a feature becomes less important. Then, the pooling layer reduces trainable parameters in order to speed up the operation, prevent over fitting problems and enable translation invariance. At last, a fully connected layer, which has the same shape as a deep neural network (DNN), executes classification (Indolia et al., 2018). Vanila neural network, so called as an artificial neural network (ANN) or deep neural network (DNN) mainly consists of 3 different layers, including input layers, hidden layers, and output layers. However, as the ANN and DNN have lower performance in computer vision and natural language processing (NLP), novel algorithms were invented for the higher accompli-shment. CNN is the most widely used for computer vision and RNN for the NLP. LSTM and GRU algorithms are representative models of the RNN and they have achieved better performance compared to the vanilla RNN (Cheon et al., 2021). GRU is mainly composed of two gates; reset gate and update gate. The reset gate aims to reset the historical information from the previous hidden layers (Cho et al., 2014). Therefore, after multiplying the value (0, 1) by the previous hidden layer, the sigmoid function is utilized as an activation function of the output. The update gate determines a proportion of both present and past information and the output from the update gate regulates the amount of information at present. In the candidate hidden state, it determines what to erase from the previous time step by multiplying the reset gate and the previous hidden state. Lastly, for the final hidden state, it aims to calculate the hidden layer at the present point by combining the result of the update gate and the result of the candidate hidden state (Chung et al., 2014)..

5 Proposed Model

With the aim of enhancing the performance of our model, we combined Xception model, which is a transfer learning method pre-trained with imagenet dataset, and bidirectional GRU. As the bidirectional model allows an end to end training of whole parameters in the model, it has been utilized for the elevated performance. A lambda layer is used for combining the Xception model and bidirectional GRU because the output dimension of the Xception model and the input dimension of the bidirectional GRU are not compatible. The Nadam and binary cross entropy were utilized as optimizer and loss function, respectively.

IV.

6 Results

7 a) Comparison of accuracy scores

Accuracy scores were derived from the diverse machine learning and deep learning algorithms. In the first experiment, accuracy scores for each optimizer, 'Nadam', 'rmsprop', 'adam' and 'SGD' are extracted from the vanilla CNN and the highest one is 86.2% from 'Nadam' optimizer. Various machine learning classifiers were used instead of fully connected layers of the vanilla CNN for the second experiment. Decision tree classifier brought out 71%, random forest classifier yielded 86% and extra tree classifier achieved 87% of accuracy score. Lastly, while the Xception model with 'adam' attained 62 % of accuracy score, the 'Xception + Bi-GRU' model brought out a 95.6% accuracy score, which was the highest one. Furthermore, as shown by the two graphs below, training accuracy is gradually increasing while training loss is gradually decreasing, which shows that training is done flawlessly.

8 Discussion & Limitation

Although our experiment was successful, there exist several limitations. Even though deep learning methods and machine learning methods are utilized for various approaches, only tree based machine learning models were used for the classification. Furthermore, another limitation lies on the given dataset which contains relatively fewer images for the deep learning models. For instance, other traffic dataset contains numerous samples of normal traffic data while involving less samples of malicious traffic. Therefore, previous researches conducted classification with anomaly detection algorithms such as local outlier or isolation forest. However, the dataset we used in our experiment has a restriction in that the number of samples is small for both normal and malicious dataset, which hampers us to construct the deep learning models for the anomaly detection.

9 Principal Finding

When it comes to detecting malicious network traffic, we suggest the Xception + Bi-GRU model since it demonstrates a higher accuracy score (95.6%) than other models. The model showed the highest accuracy score, 4% higher than Extra Tree Classifier and 5% higher than the most sophisticated CNN + Machine Learning models. This experiment conducts technical significance by successfully combining CNN based Xception and RNN based Bi-GRU. Our research revealed that hybrid deep learning models surpass the vanilla models when detecting malicious traffic. Furthermore, we detected and visualized the abnormal part of the malicious image via Grad-Cam which made our research have a considerable outcome compared to other existing research.

10 VI.

11 Conclusion

Proposed hybrid model 'Xception + BI-GRU' brought out the highest accuracy score compared to any other AI models. This model showed an accuracy of about 95 percent in classifying the given dataset. With Grad -Cam, we can visualize the reason why our model classified images into specific classes. Our research achieved meaningful results but there also exist several limitations. For combining deep learning and machine learning models for hybrid approach, only tree-based machine learning models were used. In addition, our given dataset contains relatively few images for training the deep learning models, which is not sufficient condition for the adequate experiment. In addition, due to this lack of dataset, we could not apply anomaly detection algorithms which were mainly used in the previous research. Despite these limitations, our experiment reveals that the hybrid model yields a higher accuracy score than implementing a deep learning model solely. Furthermore, Grad-Cam differentiated our research from other research through visualizing the anomaly part of the malicious data. For further research, [1,2]

1

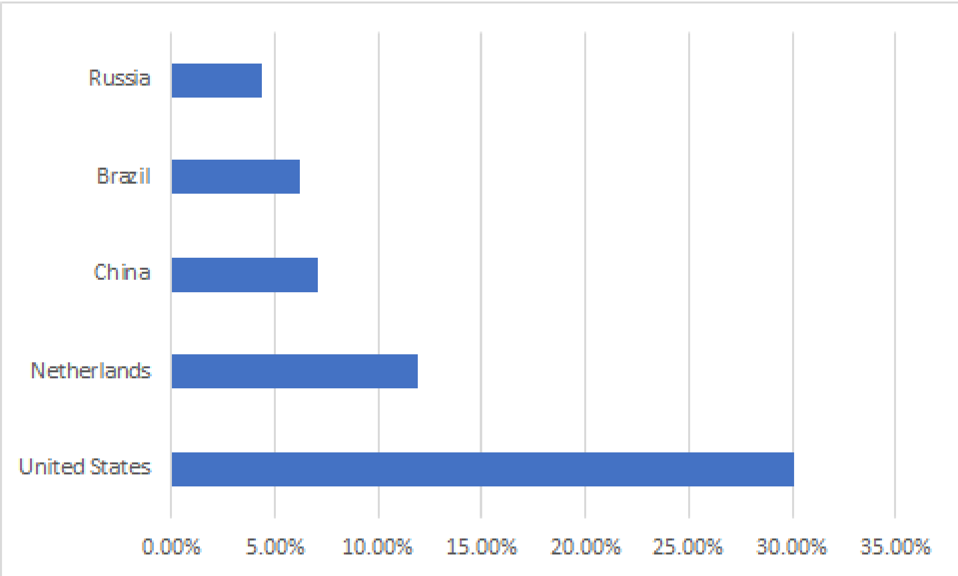
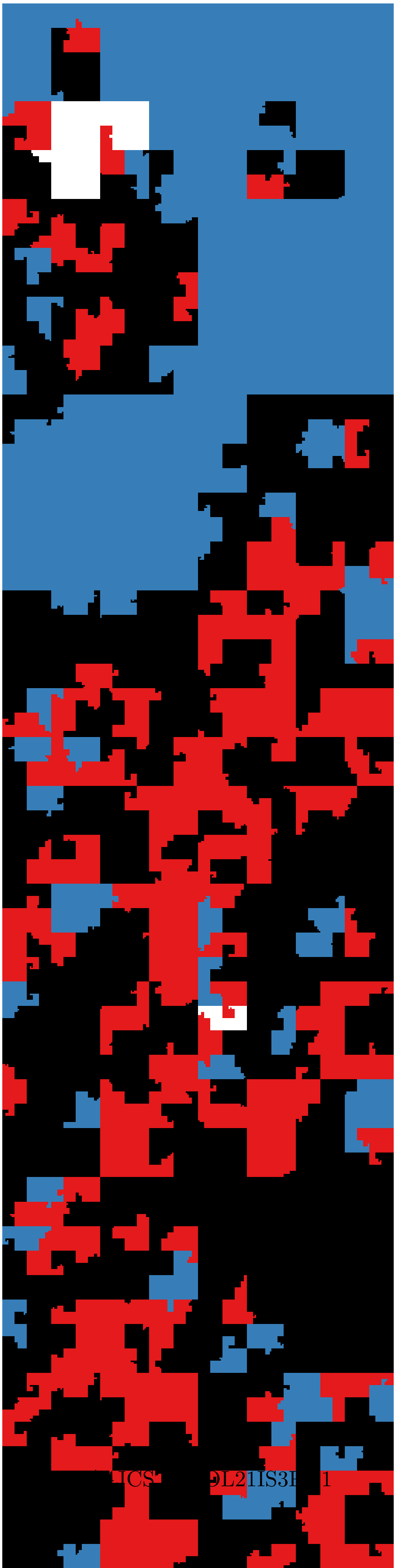
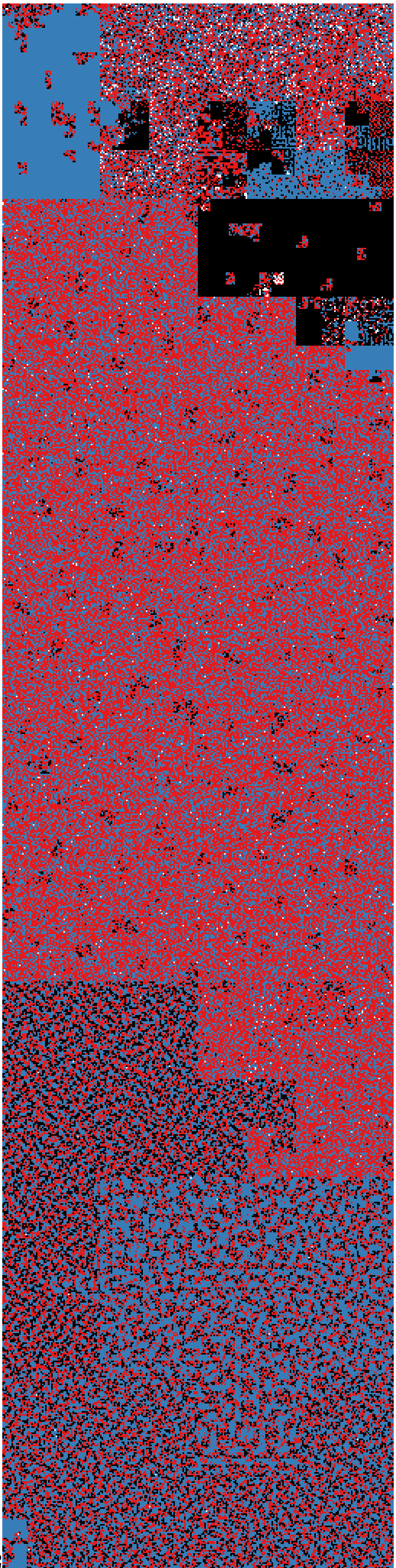
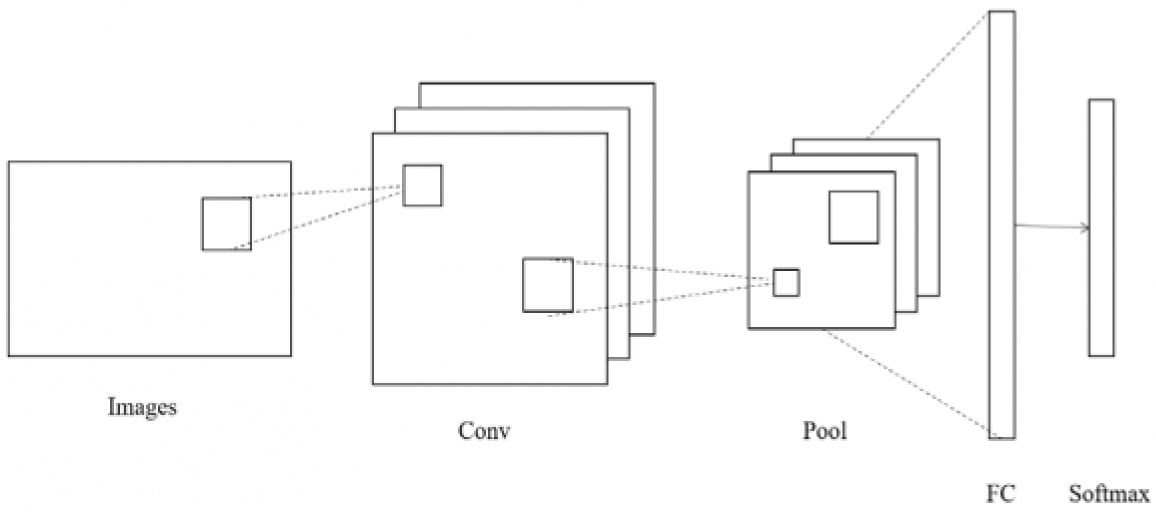


Figure 1: Figure 1 :



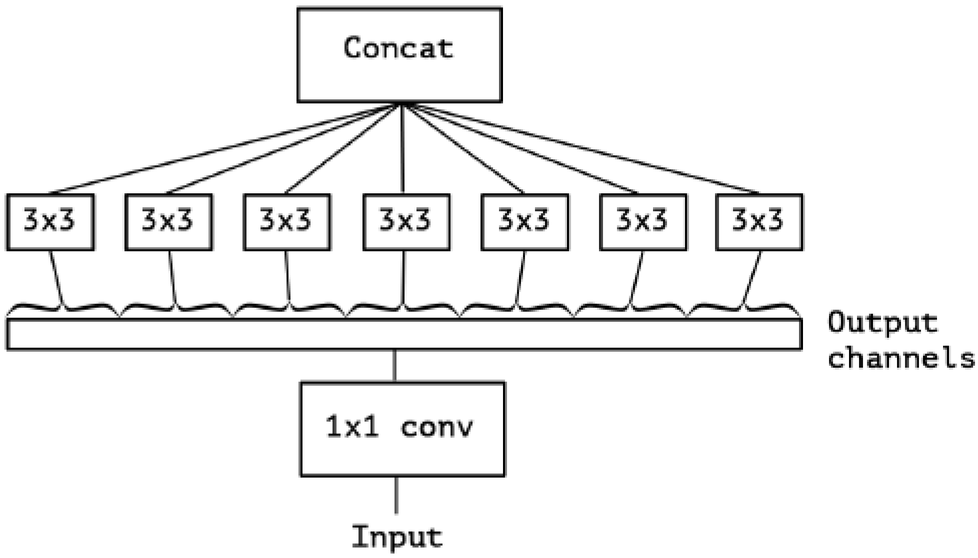


2



3

Figure 4: Figure 3 :



4

Figure 5: Figure 4 :

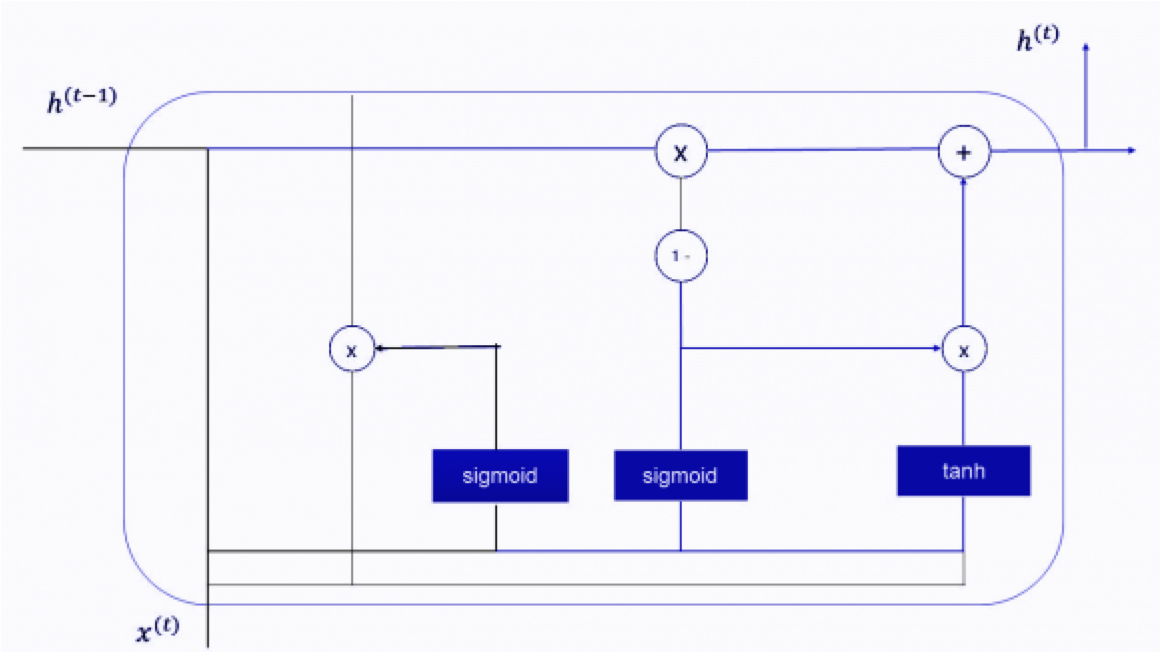
5 

Figure 6: Figure 5 :

6 

Figure 7: Figure 6 :

7

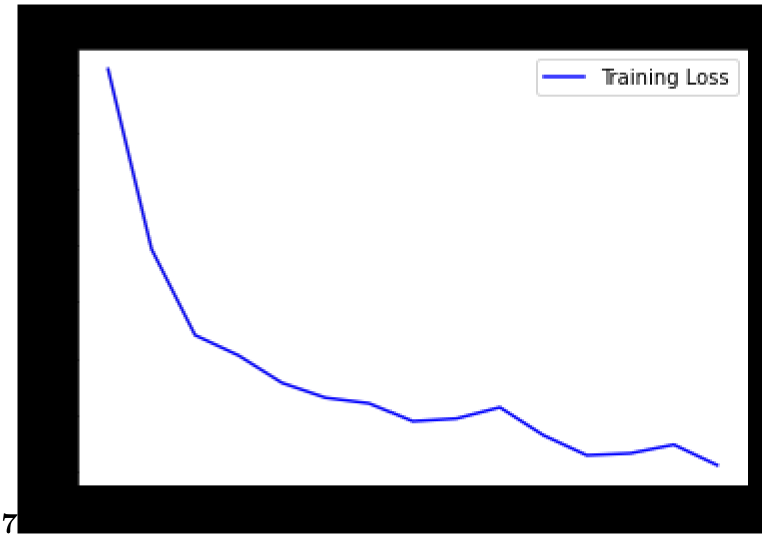


Figure 8: Figure 7 :

89

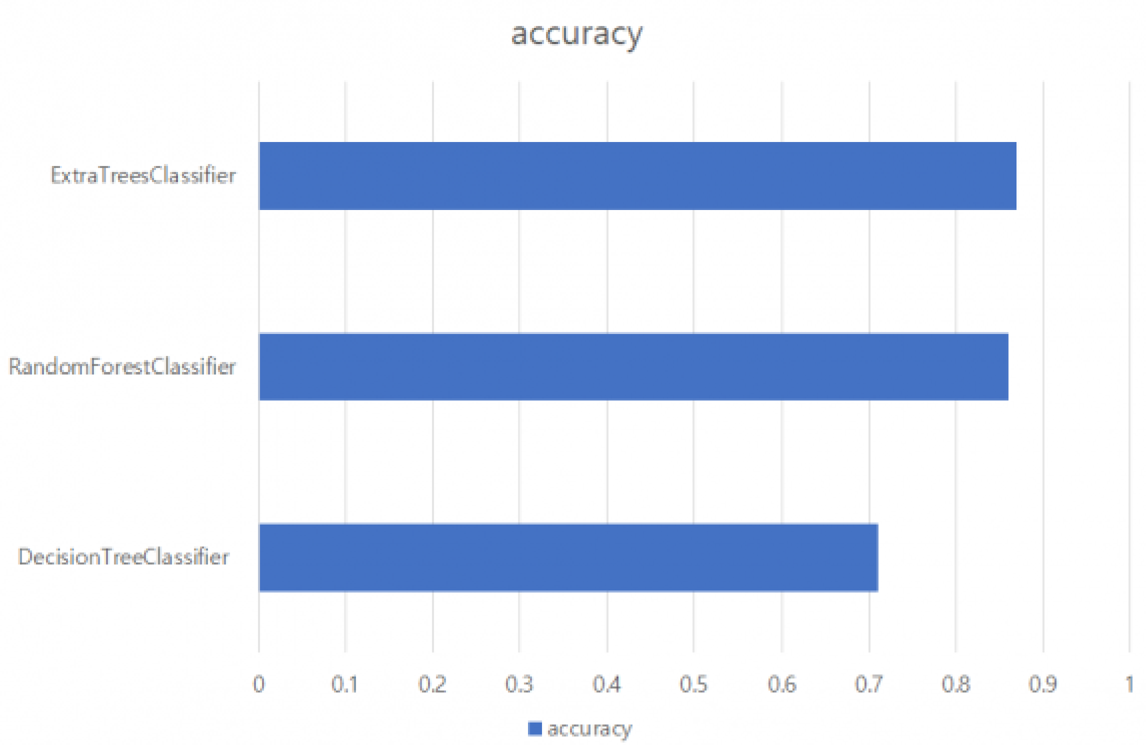
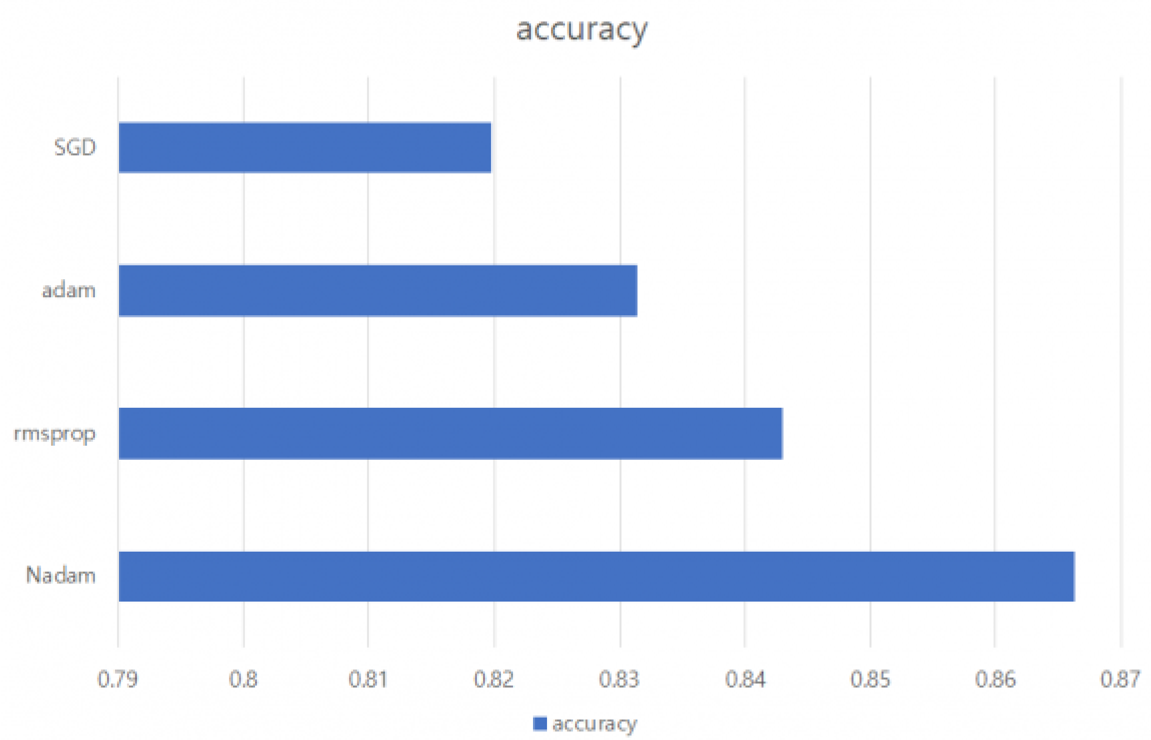


Figure 9: Figure 8 :Figure 9 :



10

Figure 10: Figure 10 :

we would attain higher accuracy scores and also construct a CNN based anomaly detection model.

[] , 10.1109/cvpr.2019.00066. https://doi.org/10.1109/cvpr.2019.00066

[Al Khater and Overill ()] N Al Khater , R E Overill . *Network traffic classification techniques and challenges*, 2015. 2015.

[Yuan et al. ()] 'An SVMbased machine learning method for accurate internet traffic classification'. R Yuan , Z Li , X Guan , L Xu . 10.1007/s10796-008-9131-2. https://doi.org/10.1007/s10796-008-9131-2 *Information Systems Frontiers* 2008. 12 (2) p. .

[Cheon et al. ()] 'Deep learning based hybrid approach of detecting fraudulent transactions'. M J Cheon , D H Lee , H S Joo , O Lee . *Journal of Theoretical and Applied Information Technology* 2021. 99 (16) p. .

[Chung et al. ()] *Empirical evaluation of gated recurrent neural networks on sequence modeling*, J Chung , C Gulcehre , K Cho , Y Bengio . arXiv:1412.3555. 2014. (arXiv preprint)

[Selvaraju et al. ()] 'Grad-cam: Visual explanations from deep networks via gradientbased localization'. R R Selvaraju , M Cogswell , A Das , R Vedantam , D Parikh , D Batra . *Proceedings of the IEEE international conference on computer vision*, (the IEEE international conference on computer vision) 2017. p. .

[Layton (2021)] *Hackers Are Targeting U.S. Banks, And Hardware May Give Them An Open Door*, R Layton . https://www.forbes.com/sites/roslynlayton/2021/03/17/hackers-are-targeting-us-banks-and-hardware-may-give-them-an-open-door/ 2021. March 19.

[Indolia et al. ()] S Indolia , A K Goswami , S Mishra , P Asopa . 10.1016/j.procs.2018.05.069. https://doi.org/10.1016/j.procs.2018.05.069 *Conceptual Understanding of Convolutional Neural Network-A Deep Learning Approach. Procedia Computer Science*, 2018. 132 p. .

[Sanaei and Sobhani ()] 'Information technology and e-business marketing strategy'. M R Sanaei , F M Sobhani . 10.1007/s10799-018-0289-0. https://doi.org/10.1007/s10799-018-0289-0 *Information Technology and Management* 2018. 19 (3) p. .

[Rose et al. ()] 'Intrusion Detection using Network Traffic Profiling and Machine Learning for IoT'. J R Rose , M Swann , G Bendiab , S Shiaeles , N Kolokotronis . 10.1109/netsoft51509.2021.9492685. https://doi.org/10.1109/netsoft51509.2021.9492685 *IEEE 7th International Conference on Network Softwarization (NetSoft)*, 2021. 2021.

[Statista et al. ()] 'Learning Channel-Wise Interactions for Binary Convolutional Neural Networks'. ; Z Statista , J Lu , C Tao , J Zhou , Q Tian . https://www.statista.com/statistics/276425/internet-attack-traffic-by-originating-country/Wang *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2021. January 25. 2018. 2019. 2019. (Leading source countries of web application attack traffic)

[Cho et al. ()] *Learning phrase representations using RNN encoder-decoder for statistical machine translation*, K Cho , B Van Merriënboer , C Gulcehre , D Bahdanau , F Bougares , H Schwenk , Y Bengio . arXiv:1406.1078. 2014. (arXiv preprint)

[Ahmed and Mahmood ()] 'Network traffic analysis based on collective anomaly detection'. M Ahmed , A N Mahmood . 10.1109/iciea.2014.6931337. https://doi.org/10.1109/iciea.2014.6931337 *9th IEEE Conference on Industrial Electronics and Applications*, 2014. 2014.

[Radford et al. ()] B J Radford , L M Apolonio , A J Trias , J A Simpson . arXiv:1803.10769. *Network traffic anomaly detection using recurrent neural networks*, 2018. (arXiv preprint)

[Tenth International Conference on Digital Information Management (ICDIM)] 10.1109/icdim.2015.7381869. https://doi.org/10.1109/icdim.2015.7381869 *Tenth International Conference on Digital Information Management (ICDIM)*,

[Williams (2021)] S Williams . https://securitybrief.co.nz/story/apac-top-target-for-network-ddos-attacks *APAC top target for network DDoS attacks -report. Security Brief*, 2021. September 6.