Deep Learning for Improving Attack Detection System Using CSE-CICIDS2018

*Abdulnaser A. Hagar[1,2], Bharti W. Gawali[2]

[1] Faculty of Administrative and Computer Sciences, Albaydha University, Albaydha, Yemen

[2] Department of Computer Science and Information Technology, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, India

ABSTRACT

Intrusion Detection Systems (IDS) are critical components of cyber security because they recognize network anomalies traffic. Severe security concerns are currently posed to the Internet and computer networks. These threats always evolve and will eventually mutate into new and undiscovered varieties. We propose putting it into action for deep learning algorithms to preserve network security. The class-imbalance problem was addressed by using upsampling and downsampling techniques. Deep Learning-IDS enhances the robustness, and the CSE-CICIDS2018 dataset tests it with 76 features. We use the models to examine the dataset performance, which is more reliable in intrusion detection. According to the testing data, each model has 14 types of attacks, and classification accuracy is higher than that of other deep learning methods. Convolutional Neural Networks (CNN) displayed the model's accuracy is 98.31%, which is better than those obtained using Long Short-Term Memory (LSTM) models, despite LSTM giving Loss less than CNN.

Keywords: Intrusion Detection, Cybersecurity, CNN, LSTM, RNN, CSE-CICIDS2018

Number: 10.14704/nq.2022.20.7.NQ33385 **Neuro Quantology 2022; 20(7):3064-3074**

1. INTRODUCTION

The amount of globally networked devices has grown dramatically due to the rapid development of Internet technologies. Faults or attacks always happen, resulting in a negative user experience and significant financial losses. People frequently use firewalls as the major protection to guarantee the system functionality, and Intrusion Detection Systems (IDS) as the next source to enhance and strengthen security, to avoid network attacks. Numerous studies on the backdrop problem have identified several concerns and challenges with IDS that require immediate and focused attention from researchers. Apart from the challenges, the real motivation and true reason behind this research are to propose a high performance with an effective and reliable CSE-CIC-IDS2018 dataset. Network traffics that is not normal hurts the network and departs significantly from regular network traffic patterns. Unusual network traffic might be caused by erroneous network operations or external network attacks. Using network sensors or sniffer software and network packets are recorded. After then, the data is filtered and reviewed. Filtering is accomplished by the use of filtering rules, followed by signature patterns compared to the signature database that is already available. The IDS sends out an alert at the point when a match is found in the putaway mark information base. Using an IDS model to sort network traffic into two categories: benign and malignant(Leevy & Khoshgoftaar, 2020).

Machine-Learning (ML) and Deep-Learning (DL) algorithms are used to analyze IDS datasets that include network traffic characteristics and labeled data. The dataset includes both normal and aberrant traffic, allowing the classifier to discover data patterns with a large enough sample size created from the data that trains and tests the classifier.

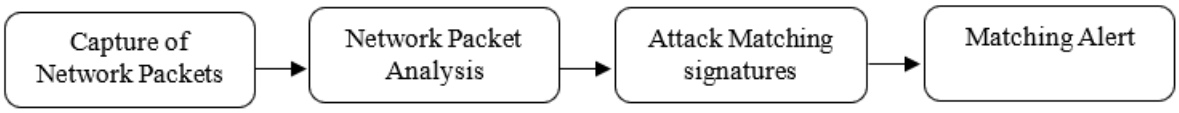

Figure 1 IDS Architecture

The diagram above in the figure1 depicts how the architecture of IDS functions. Initially, it captures the packets in the network where they are analyzed in the next stage, then attacks matching signatures are finalized before sending the alarm. Finally, a network traffic classification engine must discern between normal and abnormal traffic. (Ferrag et al., 2020). The classification process, which determines an IDS's detection performance, is the most essential of the abovementioned steps. The technique accomplishes categorization based on network traffic comparison to previously defined abnormal traffic signatures, whereas the latter method generally learns abnormal traffic characteristics.

Deep neural networks (also known as deep learning) have regained popularity among people in recent years, thanks to advances in computing capability and the explosion of information volume. Deep learning techniques are effective in various fields due to their great nonlinear fitting capabilities. When dealing with large amounts of data, deep learning approaches have a quicker processing time and are more accurate than traditional machine learning algorithms at learning the hidden layer represents features. The challenges and difficulties faced by IDS are the class-imbalance problems, Algorithms for detecting intrusions, Dataset deficiency or inadequacy, Data integration in various forms, and IDS testing and evaluation (Elaraby & Elmogy, 2016).

This research presents a deep learning strategy for implementing the dynamic IDS to overcome the issues above. The following are the major contributions: We go into the more difficult and practical topic of multi-classification.

Our experiment used the CSE-CICIDS2018 dataset, which reflects the most recent network traffic features. LSTM and CNN models are built to perform well in time-correlated sequences like network traffic. We employ an over-sampling technique to get more samples and downsampling to decrease the huge sample to make a semi-balanced dataset. The loss function is then optimized, making headway on the class-imbalance problem.

2. PROPOSED MODELS

This section explains the deep learning algorithms and the implementation of the proposed models.

2.1 Recurrent Neural Network

A Recurrent Neural Network (RNN) is a category of artificial neural network in which nodes exchange signals (feedback). This phrase refers to various designs that use this concept, including hierarchical RNNs, continuous-time RNNs, bi-directional RNNs, and the well-known LSTM network(Kim et al., 2019).

Long-term reliance is a problem that has been proposed to be solved using a particular recurrent neural network structure called LSTM. It extends the ordinary Recurrent Neural Network with the input, output, and forget gate (RNN). The gate removes unnecessary information from the neural network. The input feeds new data into the neural network, whereas the output decides the ultimate output because significant occasions in a period series may have unpredictable lags(Lin et al., 2019).

LSTM is perfectly matched to categorizing, analyzing, and making forecasts given time-series information. The performance of LSTM is developed with the convolution neural network (CNN)-based classifier, which is included with the embedding process involved in input, hidden, and output layers. Using cross-validation and an independent test, LSTM beat traditional Machine Learning classifiers with different pre-defined feature encodings(Kim et al., 2019).

Loukas et al. (Loukas et al., 2017) presented a method for detecting intrusions into the actual and virtual worlds. The system employs both MLP and recurrent neural network architectures, a departure from standard machine learning systems that use just one or the other (e.g., k-means clustering and SVM). Against a robotic vehicle, the system is tested against three

different attack types: attacks on the network interface, including malware, denial of service, and command injection. Taylor et al. (Taylor et al., 2016) suggested a study to identify anomalies depicted on an ANN. LSTM is trained to predict data values of the latest or new packet to find the attacks. Yin et al. (Yin et al., 2017) The NSLKDD dataset was utilized in that study to measure false positive rate, true positive rate, and accuracy. The performance is stated to be better with a learning rate of 0.1, 80 hidden nodes, and the benefits of an RNN for intrusion detection are also explored in the paper. Tang et al. (Tang et al., 2018) proposed an RNN for identifying the attack in software-defined in an alternate report. The report claims an 89 percent detection rate with few features. The network performance is measured using the NSLKDD dataset and four assessment metrics. Jiang et al. (Jiang et al., 2020) suggest a study to detect the attacks. Moreover, to evaluate the performance, they used the NSLKDD dataset. The LSTM found an accuracy rate of 98%.

2.2 Convolutional Neural Network

A CNN aims to learn the right representations of the incoming data attributes. Convolution nuclei are utilized to produce distinct feature maps in each CNN layer. Each next neuron area is connected to a function map neuron in the following layer. Furthermore, the nucleus is shared by all spatial positions of the inputs to generate the function diagram. For classification, one or more complete bound layers are employed for multiple Convolution and grouping layers (Kaur et al., 2020).

The number of forms of network traffic in the real world is substantially higher than two, making identification more difficult. Zhu et al. [6] used a Convolutional Neural Network to classify network traffic. Despite this, the experiment's precision remains questionable. Nasr et al. (Nasr et al., 2018) DeepCorr, a convolutional neural network-based intrusion detection system, was created to train a correlation function. According to experiments, DeepCorr has a true positive rate of close to 0.8 and a false positive rate of 10-3. Zhang et al. (Y. Zhang et al., 2019) Two neural network layers, the first of which is an enhanced LetNet-5 convolutional neural network, are suggested for anomalous traffic detection. During the second layer, long-term memory is employed. Zeng et al. (Zeng et al., 2019) provide a lightweight framework for identifying novel threats on the CICIDS2017 dataset; the performance was 94 percent better. The suggested system achieves good metrics when compared to other machine learning techniques. A convolutional autoencoder was employed by Yu et al. (Yu et al. 2019) to examine network intrusion using the Contagio-CTUUNB and CTUUNB datasets, two types of intrusion detection datasets. A Theano tool is used to design the neural network model. The learning rates are 0.001 for pretraining and 0.1 for fine-tuning. This dataset contains ROC curves with a value of 0.99 for six- and eight-class classifications. In addition, the study's binary classification accuracy is 99.59 percent, which is impressive. Fu et al. (Fu et al., 2016) established a system that uses a convolutional neural organization to catch the inborn examples of misrepresentation, particularly in detecting credit card fraud. For training and testing, Zhang et al. (Z. Zhang et al., 2018) Training and testing using commercial bank B2C online transaction data. There were two types of data: training and testing. According to the study, there is a 91% accuracy rate and a 94% recall. There was a 26% and a 2% rise in comparison to Fu et al. (Fu et al., 2016)

The powerful IDSs from high-dimensional data are examined in this part. A Network Intrusion Detection System (NIDS) is essential for network security since it aids in detecting and responding to hostile activity. An intrusion detection program's major goal is to ensure that IT workers are notified as soon as an attack or network incursion is suspected.

The Convolutional layers convert the input into a Convolution Neural network and output to the following line. Fully linked feed-forward neural networks can be employed to learn properties and recognize data. Given the large values of input involved with photographs, where every pixel is a unique vector, many neurons in a shallow architecture will be required. Different stages, including convolution, maximum grouping, and flattening, are frequently used in this network(Chockwanich & Visoottiviseth, 2019; Kaur et al., 2020; Leevy & Khoshgoftaar, 2020).

Convolution layer: the characteristics and patterns are derived from the data. Grouping: It minimizes the dimensionality of every feature

map but retains important information. Flatten: To insert data into the next layer, flatten it into a one-dimensional matrix. To make a single lengthy and flatten the output of the Convolutional layers with a feature vector. Fully Connected: These forms of layers are associated with each neuron to another neuron in the next layer.

2.3 CSE-CICIDS2018

For our proposed high-performance, efficient ID system, CSE-CICIDS2018 is preferred. CSE-CICIDS2018 Data generated by the Canadian Institute for Cybersecurity and Communications Security Establishment (CIC) were utilized in our experiment (CSE). Testing and evaluating network applications and lower-level network entities, as well as transitioning from static data to real-time traffic on Amazon's platform, is the ideal strategy (AWS) CSE-CIC-IDS2018. Network and system logs are included in the dataset (CIC-2018). Sub-datasets were gathered over ten days during CIC-2018. About 84 features are included in this dataset Using 14 attack types created using CICFlowMeter V3. These features allow packets and network traffic to be directed forward and backward (R. I. Farhan et al., 2020; Kim et al., 2019; Lin et al., 2019).

Attacks Profiles

Several various network attacks are included in the datasets, which include both benign (or "normal") network traffic and harmful (or "malicious") network activity. a short description of which follows(Basnet et al., 2019; Kumar et al., 2020):

Brute Force Attack: Most voguish attacks might be utilized not exclusively to break passwords but also to track down concealed pages and material. It's essentially a hit-or-miss strategy, with the unfortunate eventually succeeding.

Botnet: A botnet is a gathering of Internet-associated gadgets that a botnet proprietor uses to finish different exercises. It has the capability of stealing information. Deliver spam and allow access to restricted regions and admittance to the gadget and its connection to the assailant.

DoS Attack: The attacker intends to disable a system or network resource for a short period. It's regularly refined by immersing a computer or asset with superfluous solicitations to over-burden frameworks and keep some or all solicitations from being performed.

DDoS Attack: At the point when a casualty's data transfer capacity or assets are exhausted by countless frameworks, this happens. At the point when various commandeered frameworks (for instance, a botnet) flood the designated framework with network traffic, this is also known as a disavowal of administration attack.

Web Attack: New assault types arise daily as people and organizations seriously view security. We use SQL Injection, where an assailant makes a line of SQL orders and afterward utilizes it to constrain the data set to react with data, Cross-Site Scripting (XSS), where engineers neglect to test their code for the chance of content infusion, and Brute Force over HTTP, where an aggressor attempts a list of various of passwords to track down the manager's secret key.

Infiltration Attack: Privilege escalation usually happens later in the attack when the attacker has already conducted reconnaissance and successfully penetrated a system, allowing them access. After that, the attacker will have used lateral movement to traverse the compromised system and identify all the systems and devices of interest. The attacker wants a firm grip on the system at this point. In table 1, we can see the attack types for each category.

Table 1. CSE-CICIDS2018 Attack types

No.	Attack Type	Category
1	SSH-Bruteforce	Brute-force
2	FTP-BruteForce	
3	Botnet	Bot
4	DoS - Hulk	DoS attack
5	DoS - SlowHTTPTest	
6	DoS - Slowloris	
7	DoS - GoldenEye	
8	DDOS - HOIC	DDoS attack
9	DDOS - LOIC-UDP	
10	DDOS - LOIC-HTTP	
11	Brute Force - XSS	Web attack
12	Brute Force –Web	
13	SQL Injection	
14	Infiltration	Infiltration

2.4 Data Preprocessing

Big data datasets have frequently duplicated features, which lead to challenges for the analysis of big data and data modeling, especially in IDS. The CSE-CIC-IDS2018 dataset contains 84 features and 16233002 rows with ten CSV files; therefore, after reading all the files using pandas, we concatenate all files to one file. The shape of the dataset becomes 16233002 rows and 84 columns after concatenating. By seeing basic statistical details, after removing those eight features, the shape of the data set becomes 16,233,002 rows and 76 columns. In addition, we clean the dataset from null values and map for each class of attacks.

Moreover, we resample some classes using the bootstrapping method to regenerate samples by upsampling for each class and downsampling for one class (benign) to address the imbalance class issue. After preprocessing, the shape of the dataset became 3,835,577 rows and 76 features. Cleaning: Data preparation is divided into three stages(R. Farhan et al., 2020; Hagar et al., 2020):

Digitalizing: Identifying and correcting missing values in the data. Categorical features are converted to numerical values through the process of data preprocessing. Transforming: normalization may change the data's scale, type, and probability distribution.

3. EXPERIMENTAL RESULTS

In this experiment, the hyperparameters for CNN and LSTM that we have to streamline are hidden nodes "200", Loss "categorical_crossentropy", batch size "64", learning rate "0.0001", activation function "Softmax", and optimizer "Adam". We also noticed that the dataset has many samples for traffic in a network, which might distort the model's classification preference. As a result, we get 3,835,577 from the typical traffic shown in Table 1. Tabel 2 and 3 clarify the two models' results for each class (precision, recall, F1-score).

Table 2: Performance of LSTM on CICIDS2018 for 15 class

Class No.	precision	Recall	F1-score	Samples
0	1.00	0.94	0.97	1000000
1	1.00	1.00	1.00	286191
2	0.89	0.69	0.78	25000
3	0.79	0.90	0.84	25000
4	1.00	1.00	1.00	686012
5	1.00	0.99	1.00	10000
6	1.00	1.00	1.00	576191
7	1.00	1.00	1.00	41508
8	1.00	1.00	1.00	461912
9	1.00	1.00	1.00	139890
10	0.99	1.00	0.99	10990
11	1.00	1.00	1.00	193360
12	0.74	0.98	0.85	161934
13	0.91	0.94	0.93	30000
14	1.00	1.00	1.00	187589
				3835577

Table 3: Performance of CNN-CICIDS2018 for 15 classes

Class No.	Precision	Recall	F1-score	Samples
0	1.00	0.95	0.97	1000000
1	1.00	1.00	1.00	286191
2	0.88	0.76	0.81	25000
3	0.83	0.90	0.86	25000
4	1.00	1.00	1.00	686012
5	1.00	1.00	1.00	10000
6	1.00	1.00	1.00	576191
7	1.00	1.00	1.00	41508
8	1.00	1.00	1.00	461912
9	1.00	1.00	1.00	139890
10	1.00	1.00	1.00	10990
11	1.00	1.00	1.00	193360
12	0.75	0.99	0.85	161934
13	0.92	0.99	0.95	30000
14	1.00	1.00	1.00	187589
				3835577

Effects of Batch Size on Model Performance: One of the important parameters is the batch size in the model training process. Increasing the batch size within a suitable range can enhance memory utilization and increase the data processing speed. However, if it is increased to an excessive degree, it might severely reduce the speed of the process. A batch size of 64 was found to be optimal.

From table 2, table 3, and figure 2, 3, 4, and 5, The overall performance results based on accuracy, precision, recall, and F1-score, with the total epochs 50 and a batch size of 64 are used, which achieves the highest accuracy of 98.31% and Loss 0.2813 % by using the CICIDS2018 dataset based on CNN has been achieved. While the LSTM Accuracy was 98.15 % and a Loss of 0.0403 %.

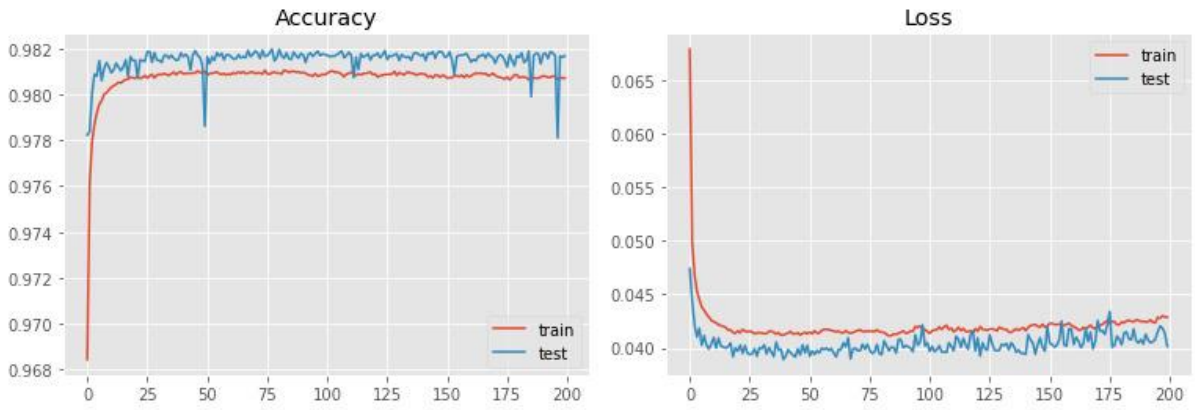

Figure 2 LSTM performance

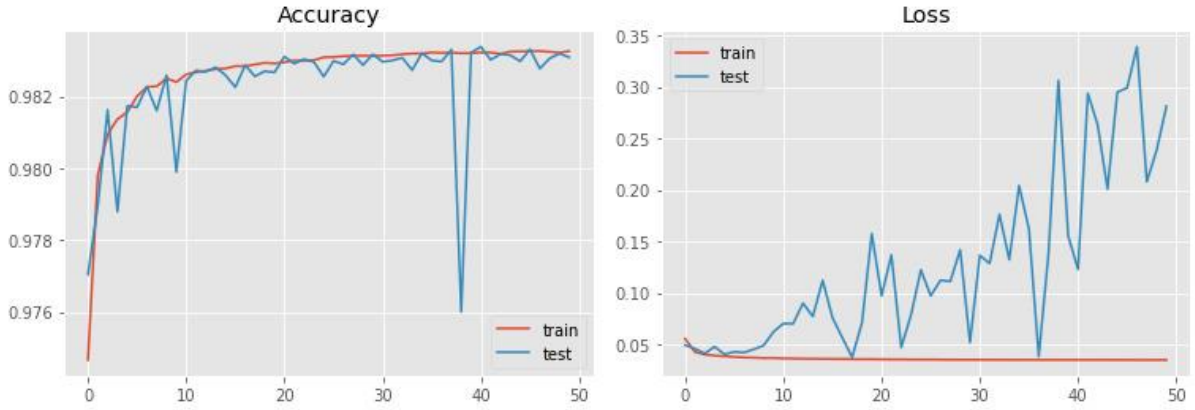

Figure 3 CNN performance

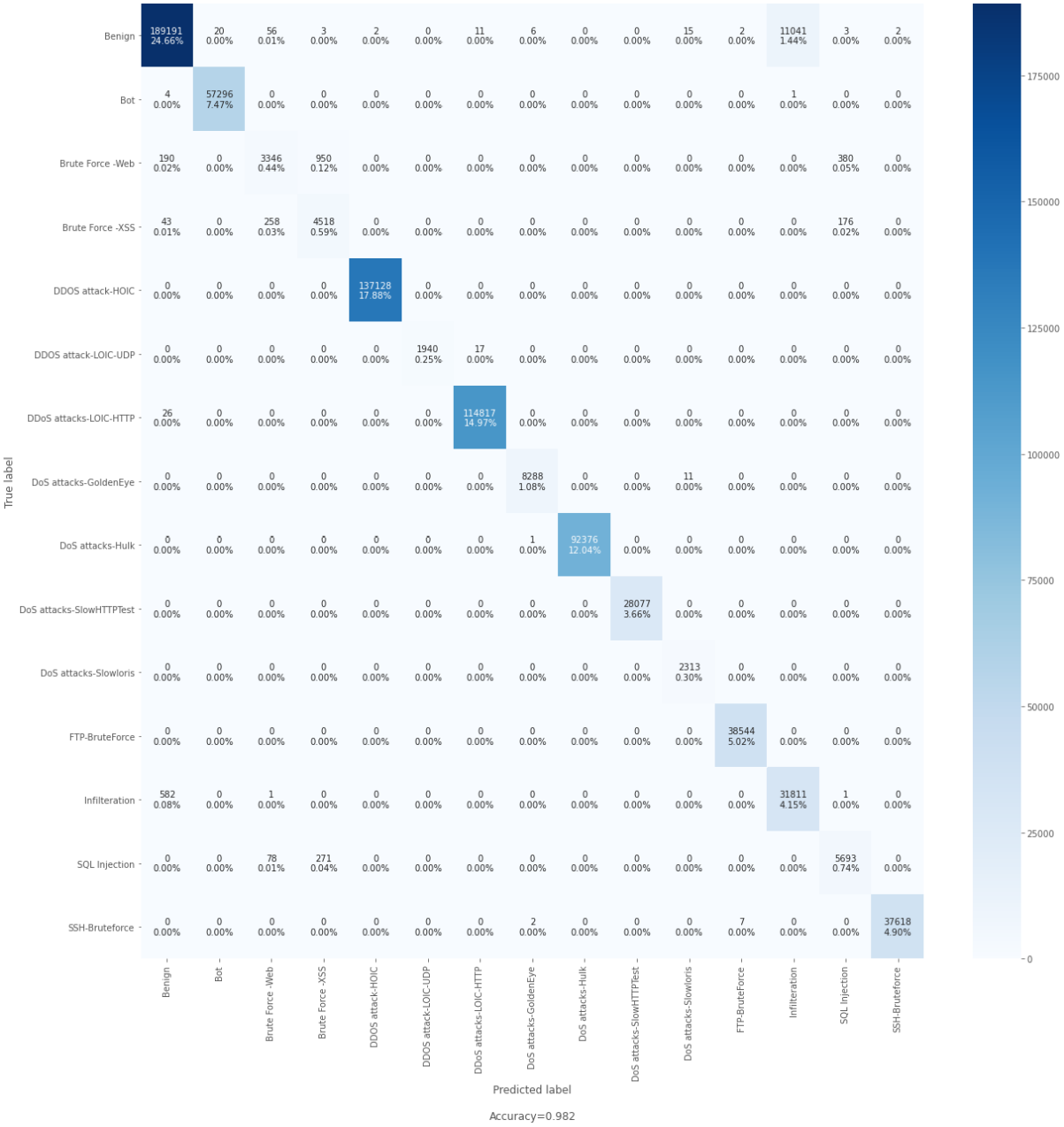

Figure 4 LSTM Confusion Matrix

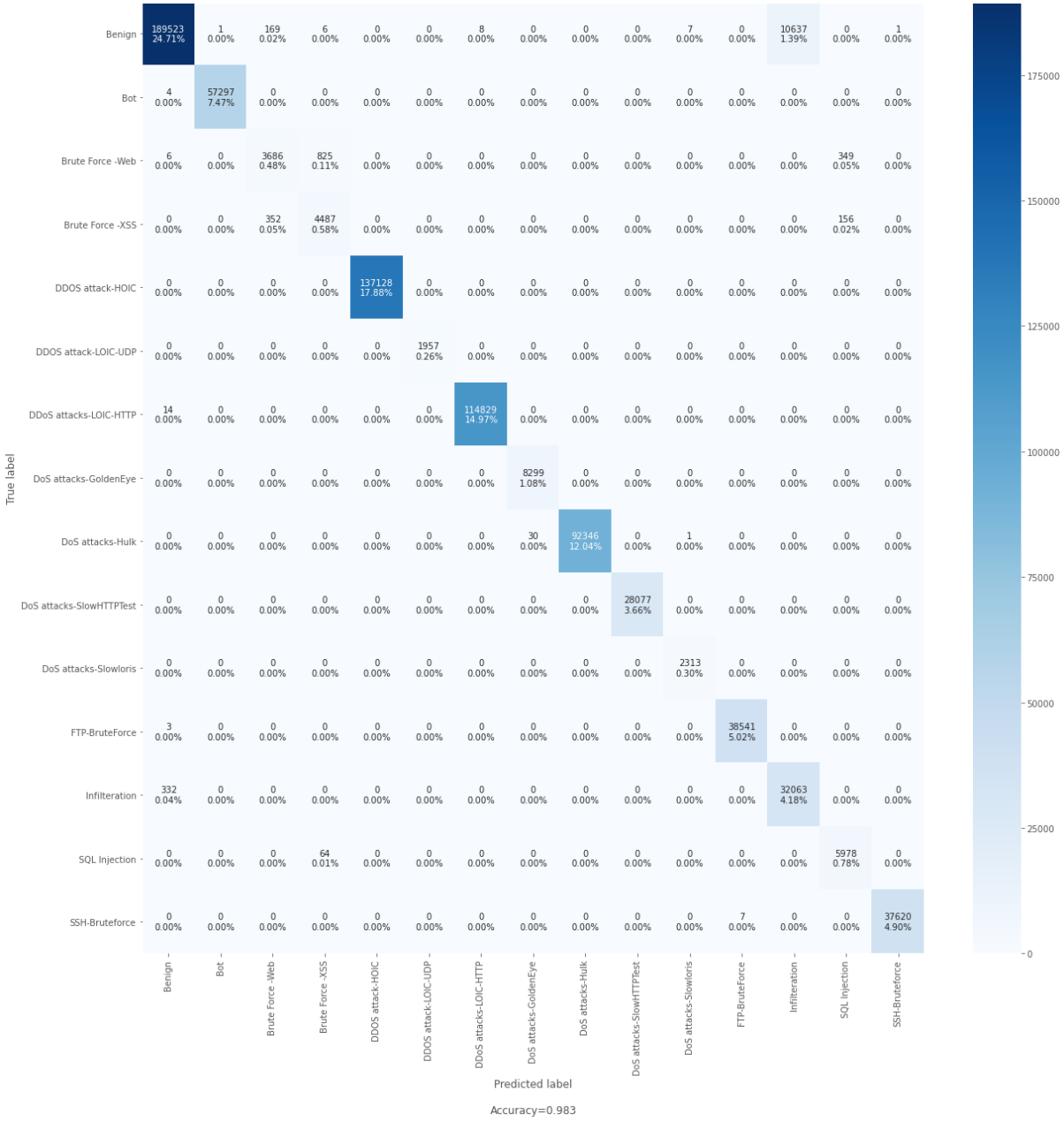

Figure 5 CNN Confusion Matrix

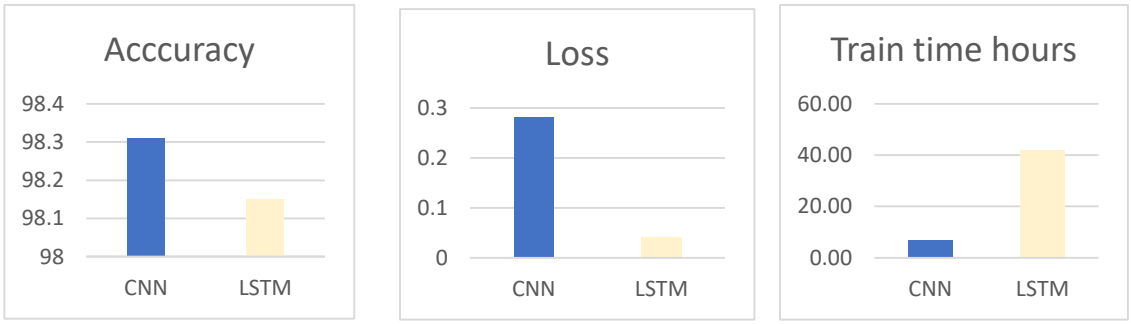

Figure 6 Accuracy, Loss, and Training time

4. DISCUSSION

The experimental results show that the training set has higher accuracy than the other Generative/ supervised Deep learning methods, even in the multiple classifications, based on the same CSE-CICIDS2018 dataset. Compared to other deep learning models, the model has a high detection rate for most attack types, which can be displayed in tables 2 and 3. The accuracy for the CIC-IDS2018 datasets has achieved nearly 98.31% by CNN and the Loss of 0.2813, while the Loss by LSTM is 0.0403, and the accuracy is 98.15%. The outcomes of the experiments suggest that our optimization is highly important. CNN is utilized to develop the network model to combat network traffic classification attacks and Challenges.

Furthermore, we discover that LSTM takes substantially longer to train than deep learning techniques, 41.81 hours, while CNN is 6.80 hours only. While training, our proposed models reduced the number of unbalanced samples in attack types and improved the model's performance if we compare them with the previous works. The CNN model performance for multi-classification outperforms other classification techniques.

5. CONCLUSION

CSE-CICIDS2018 dataset was used to analyze network traffic and improve attack detection system performance using Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM). TOur proposed models improve network attack detection and overcome class imbalance and accuracy issues. Our experiments used the most recent dataset, CSE-CIC-IDS-2018, to optimize the training process and improve the accuracy and loss function. In terms of traffic classification, the final trained models have high performance. The CNN displayed the model's accuracy is 98.31%, which is better than those obtained using RNN -LSTM models. Moreover, the LSTM takes more time in the training stage. On the other hand, the LSTM gives a Loss less than CNN.

We intend to use raw network traffic data instead of artificially extracted features in the future to allow deep neural networks to learn their features and allow the neural networks to reach their maximum potential.

REFERENCES

Basnet, R. B., Shash, R., Johnson, C., Walgren, L., & Doleck, T. (2019). Towards detecting and classifying network intrusion traffic using deep learning frameworks. *Journal of Internet Services and Information Security*, *9*(4), 1–17. https://doi.org/10.22667/JISIS.2019.11.30.001

Chockwanich, N., & Visoottiviseth, V. (2019). Intrusion Detection by Deep Learning with TensorFlow. *International Conference on Advanced Communication Technology, ICACT*, *2019-Febru*(February), 654–659. https://doi.org/10.23919/ICACT.2019.8701969

Elaraby, N. M., & Elmogy, M. (2016). Deep Learning : Effective Tool for Big Data Analytics. *International Journal of Computer Science Engineering*, *5*(05), 254–262.

Farhan, R. I., Maolood, A. T., & Hassan, N. F. (2020). Performance analysis of flow-based attacks detection on CSE-CIC-IDS2018 dataset using deep learning. *Indonesian Journal of Electrical Engineering and Computer Science*, *20*(3), 1413–1418. https://doi.org/10.11591/ijeecs.v20.i3.pp1413-1418

Farhan, R., Maolood, A., & Hassan, N. (2020). Optimized Deep Learning with Binary PSO for Intrusion Detection on CSE-CIC-IDS2018 Dataset. *Journal of Al-Qadisiyah for Computer Science and Mathematics*, *12*(3), Comp Page 16-27. https://qu.edu.iq/journalcm/index.php/journalcm/article/view/706

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, *50*, 102419. https://doi.org/10.1016/j.jisa.2019.102419

Fu, K., Cheng, D., Tu, Y., & B, L. Z. (2016). *Credit Card Fraud Detection Using Convolutional Neural Networks Kang*. 483–490. https://doi.org/10.1007/978-3-319-46675-0

Hagar, A. A., Chaudhary, D. G., Al-bakhrani, A. L. I. A., & GAWALI, B. W. (2020). *BIG DATA ANALYTIC USING MACHINE LEARNING ALGORITHMS FOR INTRUSION DETECTION SYSTEM : A SURVEY*. *10*(3), 6063–6084.

Jiang, F., Fu, Y., Gupta, B. B., Liang, Y., Rho, S., Lou,

F., Meng, F., & Tian, Z. (2020). Deep Learning Based Multi-Channel Intelligent Attack Detection for Data Security. *IEEE Transactions on Sustainable Computing*, *5*(2), 204–212. https://doi.org/10.1109/TSUSC.2018.2793284

Kaur, G., Habibi Lashkari, A., & Rahali, A. (2020). Intrusion Traffic Detection and Characterization using Deep Image Learning. *Proceedings - IEEE 18th International Conference on Dependable, Autonomic and Secure Computing, IEEE 18th International Conference on Pervasive Intelligence and Computing, IEEE 6th International Conference on Cloud and Big Data Computing and IEEE 5th Cybe*, 55–62. https://doi.org/10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00025

Kim, J., Shin, Y., & Choi, E. (2019). *An Intrusion Detection Model based on a Convolutional Neural Network*. *6*(4), 165–172.

Kumar, V., Choudhary, V., Sahrawat, V., & Kumar, V. (2020). *Detecting Intrusions and Attacks in the Network Traffic using Anomaly based Techniques*. *Icces*, 554–560.

Leevy, J. L., & Khoshgoftaar, T. M. (2020). A survey and analysis of intrusion detection models based on CSE-CIC-IDS2018 Big Data. *Journal of Big Data*, *7*(1). https://doi.org/10.1186/s40537-020-00382-x

Lin, P., Ye, K., & Xu, C. Z. (2019). Dynamic network anomaly detection system by using deep learning techniques. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 11513 LNCS*. Springer International Publishing. https://doi.org/10.1007/978-3-030-23502-4_12

Loukas, G., Vuong, T., Heartfield, R., Sakellari, G., Yoon, Y., & Gan, D. (2017). Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning. *IEEE Access*, *6*, 3491–3508. https://doi.org/10.1109/ACCESS.2017.2782159

Nasr, M., Bahramali, A., & Houmansadr, A. (2018). DeepCorr: Strong flow correlation aacks on tor using deep learning. *Proceedings of the ACM Conference on Computer and Communications Security*, 1962–1976. https://doi.org/10.1145/3243734.3243824

Tang, T. A., Ali, S., Zaidi, R., Mclernon, D., Mhamdi, L., & Ghogho, M. (2018). *Deep Recurrent Neural Network for Intrusion Detection in SDN-based Networks*.

Taylor, A., Leblanc, S., & Japkowicz, N. (2016). Anomaly detection in automobile control network data with long short-term memory networks. *Proceedings - 3rd IEEE International Conference on Data Science and Advanced Analytics, DSAA 2016*, 130–139. https://doi.org/10.1109/DSAA.2016.20

Yin, C., Zhu, Y., Fei, J., & He, X. (2017). *A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks*. *5*.

Yu, Y., Long, J., & Cai, Z. (2019). *Network Intrusion Detection through Stacking Dilated Convolutional Autoencoders*. *2017*, 1–8.

Zeng, Y., Gu, H., Wei, W., & Guo, Y. (2019). Deep-Full-Range: A Deep Learning Based Network Encrypted Traffic Classification and Intrusion Detection Framework. *IEEE Access*, *7*, 45182–45190. https://doi.org/10.1109/ACCESS.2019.2908225

Zhang, Y., Chen, X., Jin, L., Wang, X., & Guo, D. (2019). Network Intrusion Detection: Based on Deep Hierarchical Network and Original Flow Data. *IEEE Access*, *7*, 37004–37016. https://doi.org/10.1109/ACCESS.2019.2905041

Zhang, Z., Zhou, X., Zhang, X., Wang, L., & Wang, P. (2018). A Model Based on Convolutional Neural Network for Online Transaction Fraud Detection. *Security and Communication Networks*, *2018*. https://doi.org/10.1155/2018/5680264