Deep Learning Based Network Intrusion Detection System

[1]Lalitha V G, [2]Sandeep Varma N

[1]Student, [2]Assistant Professor
[1] Department of Information Science and Engineering,
[1]BMS College of Engineering, Bangalore, India

ABSTRACT : Increase in the network intrusion attacks has raised in the recent few years which has increased the focus on confidentiality and protection. As a result of high technology, internet security attacks are getting complicated and the present detection systems aren't adequate to deal with this problem. Smart and powerful intrusion disclosure system can be implemented to deal with this issue. In this suggested system, the deep structured learning approaches provide various methods and they can detect the intrusions in the network. CNN and LSTM are used to design a smart detection system that is capable enough to detect different network intrusions. Here we apply CNN and LSTM algorithms and train the model using NSL-KDD dataset. We then evaluate its performance of individual models. Our experimental outcomes show that the execution of the LSTM model is beyond that of the CNN model when tested on NSL-KDD dataset.

Index terms: Deep Learning, Intrusion Detection System, LTSM, CNN

I. INTRODUCTION

The System that observes the network and system behavior, finds if any abnormal behavior happens which results in responding immediately to it, is described as Intrusion Detection and Prevention System. Hackers can attack through different types of cyber-attacks and obtain the important data. These threats can be found out using intrusion detection methods and precaution methods are used to protect against the network intrusions. The solution is to deliver a complete study on intrusion detection, intrusion types and to find a quick action against intrusions and the issues faced by the intrusions.

Security infrastructure has the necessity for the addition of IDS because of the increased attack types. It promotes the security of the system due to increased network connection. Anomaly detection and misuse or signature-based detection are the two chief IDS techniques. The anomaly detection usually detects the abnormal pattern. Major models exhibited today are not capable of regulating the complex and dynamic nature of computer cyber attacked networks. This leads to a minimum rate of the false alarm, a high rate of detection and judicious communication and computation costs. Different traditional ways for detecting the malicious such as encryptions, access control mechanisms, firewalls and so on. But there exist few limits to protect the network completely.

In latest years, there has been a massive rise in the count of networked systems so it's important to consider the cyber security issues in which the hackers gain the confidential data and damage the infrastructure of the network. There are a number of types of attacks, where in day-to-day life new attacks are created by the attackers, due to these reasons the attacks should be identified correctly using intrusion detection systems and provide the prevention techniques. There are three main components in network security such as Data collection, Feature selection and Decision engine.

There are many more methods to increase the accuracy rate for finding intrusions in the networks in ML such as SVM, Naïve Bayes, Decision Trees etc., but there is a requirement of expert knowledge and involvement to process the extensive data. The low time consumption for training and providing a higher accuracy rate with different learning techniques for large data can be done by Deep Learning.

So, the intrusion detection and prevention can be implemented by using DL. The suggested system examines the deep structured learning methods to detect network intrusions appropriately and correctly and provides the prevention methods. In past years, developers were able to detect the intrusions and identify the abnormal behavior of traffic and identify the attack without knowing information regarding which type of attack pattern it is, this detection is done by using machine learning algorithms. Additional analysis on machine learning lately created a development in copying the human brain. The development in ML occurs through deep structured learning which has been predicted to induce a major amendment in the computer science sector and if each cyber security and deep learning area unit joined, it will offer us fantastic outcomes. Initially researchers selected numerous machine learning approaches to discover in addition as stop threats.

The project implements the Deep Learning based IDS and compares them in terms of its ability to classify the packet as valid (normal) or malicious (abnormal) packet (Binary Classification), detect the type of attack (Multi-class Classification) and alert the appropriate user about the intrusion occurring and the attack type.

II. LITERATURE SURVEY

[17] In the paper written by Farnazz proposed the intrusion detection system by using the KDD Dataset which observes the network and find out the abnormal activities carried out by the user over network using the Random forest classifier and tested the accuracy of the system over different stages to identify the issues in the network and ensured that the performance of the model is effective gives the foremost results.

[7] Aljawarneh presented a model which identifies intrusions in the network data, for which Meta heuristic data is considered. This model collects the important information from the data which performs the assessments to identify the abnormal activities in the data. The famous dataset called NSL KDD is applied for intrusion detection. The intrusion occurred in the network is determined by the degrees up for which the intrusion is present, by using this hybrid model.

[2] In this model the deep learning methods such as CNN and RNN are used to build a network intrusion detection model which is able to catch the abnormal activities happening in the network. Observes the functionality of the proposed system with different matrices and concludes that the proposed system gives the best result in detecting the intrusions in the network.

[3] In this paper, they presented the system which detects the intrusions in the network using deep learning, in this methodology applied deep structured neural networks to abstract options of network watching information and uses BP neural network as a prime stage classifier to categorize intrusion varieties the strategy was done using the KDDCUP99 dataset, dataset consist typical set of knowledge to be audited, which incorporates a large kind of intrusions simulated during a military network setting. The DBN based mostly feature learning method training on intrusion detection has more advantages than traditional feature learning. DBN based feature learning is the most widely used method for feature learning tasks in higher dimensions.

[1] Multi-Layer Perceptron, which is deep learning used to identify the intrusions in the network which is trained and tested using the model using kddcup99 dataset which shows the high accuracy. This model can identify the attacks such as DOS, Probe, R2L and U2R and can also protect the system. Data or the information is collected and stored in the csv file and added to this model to estimate the attack and in the second part the detected intrusions in the network are prevented by using the python script which runs in the background. The information from the classification portion via Multi-Layer Perceptron model is used to make the suitable decision for detecting the attacks. The main focus is to implement a detection and prevention of intrusions in the network.

[16] Niyaz presented the intrusion detection system which observes the network and detects the anonymous, unpredictable and abrupt attributes that are making impact for defaults in the system. A flexible detection of unknown information which is responsible for the defects in the system is done by using the deep learning techniques through the NSL-KDD dataset.

III. PROPOSED SYSTEM

The main focus of the suggested system is to identify the intrusions in the network using deep learning techniques. Deep networks are used for the model to train itself with patterns of anomalies and classification is done between the normal networks and the intrusions. In this system, the model detects the abnormal traffic in the network by using deep learning methods such as LSTM and CNN, it gives the output value as 0 and 1 in which 0 represents the normal traffic and 1 represents the intrusion. This project can be used as a springboard in the future to create a comprehensive real-time intrusion detection system and IPS.

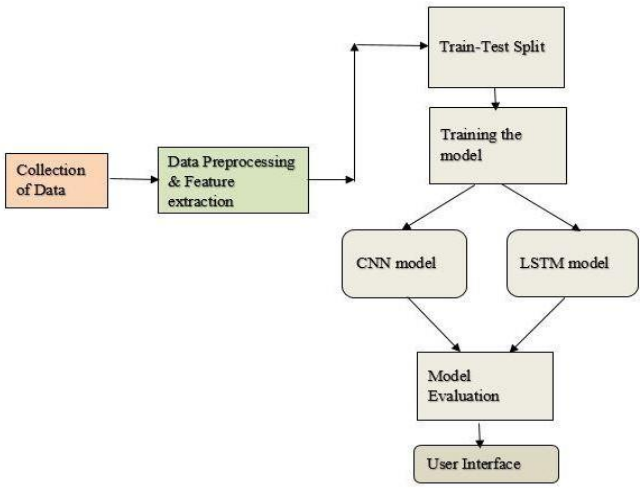

Fig. 1: Intrusion Detection System using Deep Leaning

The High-level design depicts the flow of process of our Deep learning model. Initially all datasets related to intrusion detection are imported and after Extracting the training Data from dataset the data preprocessing is being done and classified into normal and abnormal traffic based on the attributes in the dataset. All vectored information has been divided into two categories: validation data and training data. Using multiple categorization techniques to train models for detecting normal and attack_type. The classification models used are CNN and LSTM. The outputs from the classification model performs Prediction on test data using the models and calculates the Accuracy. So, based on the accuracy selects the best model and that is saved on the desk for future Predictions

IV. IMPLEMENTATION:

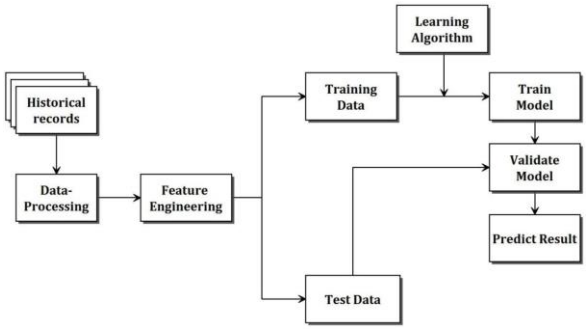

Fig. 2 Graphical Representation shows the process of creating a Deep Learning model

Collecting the Data: The dataset for this project was obtained from a legitimate source. Where the data is published for research purposes. The NSL-KDD dataset is used for intrusion detection. The size of dataset is 125973*42. It means that there are 125973 rows along with 42 Columns. There are 41 attributes in the dataset and the last column consists of attack type which contains 5 classes – normal, DoS, Probe, R2L, U2R.

Pre-processing the data: The data processing techniques are applied once the dataset is imported. Pre-processing data is viewed as critical in ability to provide highly accurate and better input for further more effective results in recognition. Obtaining all intrusion detection information in the dataset has been the first action in pre-processing. Initially we are checking for the null values in the dataset, the dataset used NSL-KDD is an advanced version of kddcup99, in which redundant data is removed. The label column which signifies, whether the packet is a normal or abnormal, is encoded with 1 and 0 respectively. Similarly, prototype state is converted from categorical data such as tcp, udp, icmp converted into numerical values like 1,2,3, etc. Few of the attack classes in the dataset are very less than the required numbers, i.e., the dataset is imbalanced for multi-class classification. Thus, those data points belonging to the minority data class is oversampled to increase their number which ultimately helps to predict the classes properly. The extraction and selection of features are done. The two approaches are crucial because they may be used to remove features that are unnecessary or redundant from the datasets. Before applying deep learning techniques, the subsequent step is to perform a basic quantitative analysis on intrusion detection criteria to assess the outcomes.

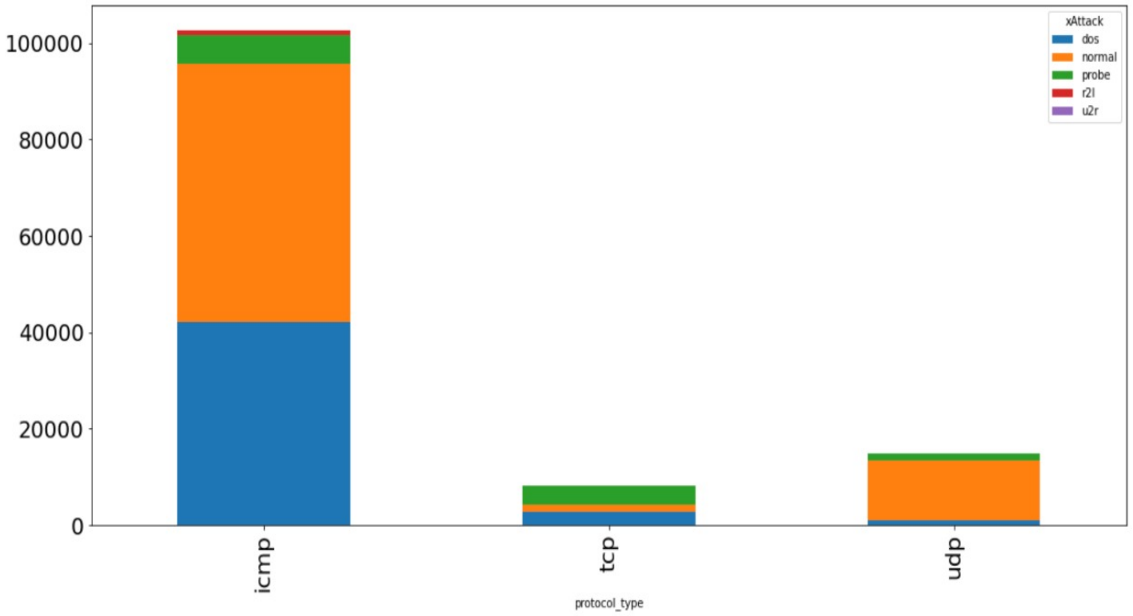

Fig. 3: Distribution of Normal and abnormal packets.

Classification/ Training the Model:

We used algorithms such as CNN, LSTM to Train and Test the data. Finally, potential to develop the framework using the classifier's reliability when predicting validation data, the optimum classifier was chosen.

Convolutional Neural Network is widely used algorithm and is one of the algorithm in deep learning algorithms which takes input as an image, allocates priorities to different scenarios and objects in the image and capable enough to modify one form to another form. The first time, the idea of CNN exercised for intrusion detection due to strong feature extraction potentials of the CNN and it can effectively extract the features of image data. To utilize the advantage of the CNN characteristics we transform the raw data into image data so that the CNN can be used classify the image to detect the intrusions in the network.

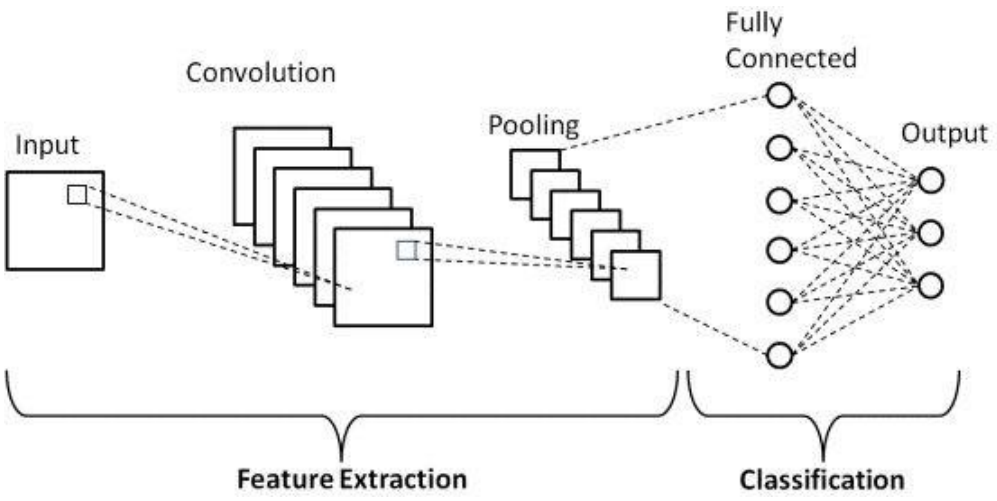

Fig. 4: Basic CNN architecture with five layers

Long Short Term Memory (LSTM): In deep learning we use LSTM means Long Short-Term Memory which is an artificial RNN i.e., Recurrent Neural Network architecture. In LSTM we have feedback connections instead of standard feedforward neural networks. It can process images as well as a set of images like a video or speech. LSTM is used in applications like speech recognition, handwriting recognition and anomaly detection in network traffic or Intrusion Detection Systems (IDS's). LSTM has the potential to remember the values of arbitrary intervals and is best suitable to classify and predict the known and unknown attacks in the network. So here we apply LSTM and train the model using Adam optimizer which can build an accurate IDS with high accuracy rate.

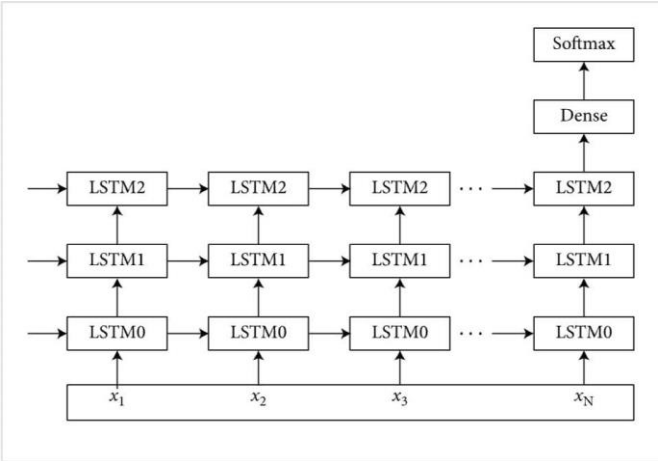

Fig. 5**.** Model building of LSTM model.

Data pre-processing was performed to transpose words into embedded integer vectors. Once the data had been split up in to the training and validation datasets, with scikit.learn train and test split function. Apply training models using various classification models that are used to identify intrusions in a network. The different classification models are the CNN and LSTM. Final results of the classification model make predictions about test data by applying the training models and calculate the accuracy. So based on the precision, we choose the best model and that will be saved on the folder for future predictions. The classifier that was chosen to build the model is known as the LSTM. After completing the training, the model recorded predictions from test data, in which they were then mapped into a confusion matrix.

V. RESULTS

The best model was saved and respected model graphs were generated. These results may occur to update the user of the model's prediction or used to construct a confusion matrix. Trainingand testing accuracy for the datasets are validated to evaluate or assess the models. Accuracy is estimated based upon the numerical illustration and measurements that follow. The general proportion of correct predictions, considering different performance measures, that is, Recall, Precision, and F1 measures, are calculated. False positive, True Negative, True Positive, and False Negative are denoted as FP, TN, TP, and FN, respectively. Where, preciseness measures what percentage positive predictions $\frac{TP}{TP+FP}$ are correct with the expression. Recall, measures how many positives were expected $\frac{\text{TP}}{\text{TP+FN}}$ properly and is calculated with the expression $\frac{2*Recall*Precision}{\text{Recall+Precision}}$. F-measure TP+FN could be a tool that evaluates precision and recall at the same time with the expression. Below figure depicts the Confusion Matrix for two algorithms. The Confusion matrix depicts how frequently a classification model (classifier) performs on avalidation dataset when the true values are available.

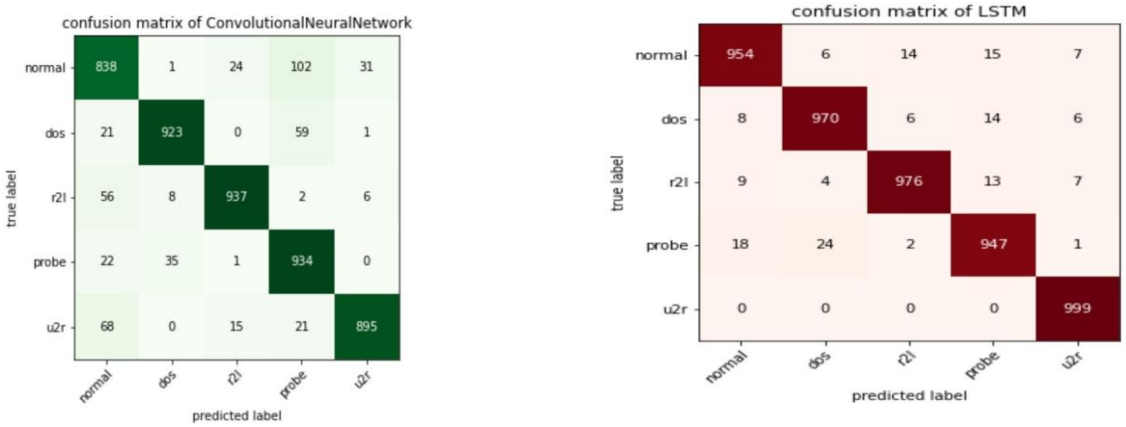

Fig.6 Confusion matrix of CNN and LSTM model.

The below shows the classification reports for the CNN and LSTM model which is further used for the analysis and to find out the best model by comparing the performance of the model.

	precision	recall	f1-score	support
normal	0.83	0.84	0.84	996
dos	0.95	0.92	0.94	1004
r2l	0.96	0.93	0.94	1009
probe	0.84	0.94	0.89	992
u2r	0.96	0.90	0.93	999
accuracy			0.91	5000
macro avg	0.91	0.91	0.91	5000
weighted avg	0.91	0.91	0.91	5000

Fig.7 Classification report for CNN model.

	precision	recall	f1-score	support
normal	0.96	0.96	0.96	996
dos	0.97	0.97	0.97	1004
r2l	0.98	0.97	0.97	1009
probe	0.96	0.95	0.96	992
u2r	0.98	1.00	0.99	999
accuracy			0.97	5000
macro avg	0.97	0.97	0.97	5000
weighted avg	0.97	0.97	0.97	5000

Fig.8 Classification report for LSTM model.

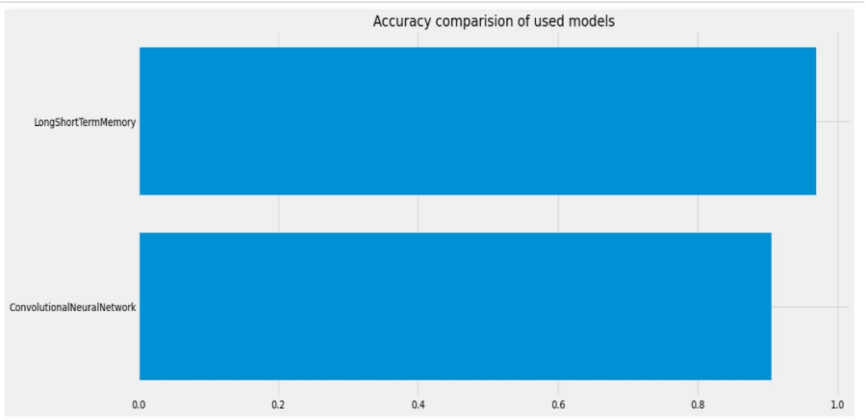

Fig.9 Accuracy results from two algorithms are depicted visually

Both the algorithms provided excellent accuracy against the testing data. Ultimately, two models were successful in detecting intrusions in the network. This Fig 15: highlights the algorithms' accuracies. As can be seen, the LSTM has the more accuracy with over 94 percent, followed by the CNN model. As a result, Long Short -Term Memory emerges as the preferable model among the two methods.

VI. CONCLUSION

The presented work is to increase the better efficiency of intrusion detection even though there are many IDS largely designed using machine learning algorithms that have not succeeded in providing powerful IDS to protect the system from the newly found attacks. In this proposed system we use CNN model and LSTM model to develop the intrusion detection system. By using the NSL-KDD dataset we carry out the classification method by applying CNN and LSTM algorithms and evaluated the models. The accuracy of the LSTM model shows the efficiency in intrusion detection when compared with CNN model and evaluation metrics also carried out to analyses the functionality of the model.

The LSTM model has the potential to learn the features extraction successfully from the dataset in the training period. This potentiality permits the models to separate effectively the normal traffic from the attacked network. Keras library and TensorFlow on Jupyter notebook (platform) are used to develop the presented architecture. We analyzed that accuracy and sensitivity are higher than the CNN model.

In future works, we can merge LSTM with CNN as a hybrid model to gain higher accuracy, make the system more effective and create a real-time system, the aforementioned models can be utilized as a benchmark.

VII. References

1. Kumar, S. Santosh, et al. "Intrusion Detection System Using Deep Learning – IJERT." Intrusion Detection System Using Deep Learning – IJERT, 27 Mar. 2021, Www.Ijert.Org/Intrusion-Detection-System-Using-Deep-Learning.
2. S. Al-Emadi, A. Al-Mohannadi and F. Al-Senaid, "Using Deep Learning Techniques for Network Intrusion Detection," 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), 2020, pp. 171-176, DOI: 10.1109/ICIoT48696.2020.9089524.
3. W. Peng, X. Kong, G. Peng, X. Li and Z. Wang, "Network Intrusion Detection Based on Deep Learning," 2019 International Conference on Communications, Information System and Computer Engineering (CISCE), 2019, pp. 431-435, DOI: 10.1109/CISCE.2019.00102.
4. Y. Xiao, C. Xing, T. Zhang and Z. Zhao, "An Intrusion Detection Model Based on Feature Reduction and Convolutional Neural Networks," in IEEE Access, vol. 7, pp. 42210-42219, 2019, DOI: 10.1109/ACCESS.2019.2904620.
5. Abdulhammed, Razan & Musafer, Hassan & Alessa, Ali & Faezipour, Miad & Abuzneid, Abdelshakour,"Features Dimensionality Reduction Approaches for Machine Learning Based Network Intrusion Detection", 2019. Electronics. 8. 322. 10.3390/electronics8030322.
6. Y.Dai, H. Li, Y. Qian, R. Yang and M. Zheng, "SMASH: A Malware Detection Method Based on Multi-Feature Ensemble Learning," in IEEE Access, vol. 7, pp. 112588-112597, 2019, DOI: 10.1109/ACCESS.2019.2934012.
7. Shadi Aljawarneh, Monther Aldwairi, Muneer Bani Yassein," Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model", 2018, Journal of Computational Science, Volume 25, 2018,Pages 152-160, ISSN 1877-7503, https://doi.org/10.1016/j.jocs.2017.03.006.
8. Zhou Qianru, Pezaros Dimitrios. 2018, "Evaluation of Machine Learning Classifiers for Zero-Day Intrusion Detection -- An Analysis on CIC-AWS-2018 dataset,".
9. Jackins, V., and D. Shalini Punithavathani. 2018, "An anomaly-based network intrusion detection system using ensemble clustering," International Journal of Enterprise Network Management, vol. 9.3-4, pp. 251-260.
10. H. Z. Jahromi and D. T. Delaney, "An Application Awareness Framework Based on SDN and Machine Learning: Defining the Roadmap and Challenges," 2018 10th International Conference on Communication Software and Networks (ICCSN), 2018, pp. 411-416, DOI: 10.1109/ICCSN.2018.8488328.
11. W. Leonard., "Resilient Cyber-Secure Systems And System Of Systems: Implications For The Department Of Defense, In Disciplinary Convergence in Systems Engineering Research", 2018, Springer, Cham. https://doi.org/10.1007/978-3-319-62217-0_11.
12. Bayar, Belhassen and Matthew C. Stamm. "Design Principles of Convolutional Neural Networks for Multimedia Forensics." Media Watermarking, Security, and Forensics (2017).
13. Alex Krizhevsky, Ilya Sutskever, and Geoffrey E. Hinton. 2017. "ImageNet classification with deep convolutional neural networks". Commun. ACM 60, 6 (June 2017), 84–90. https://doi.org/10.1145/3065386.
14. Vieira, Sandra et al. "Using deep learning to investigate the neuroimaging correlates of psychiatric and neurological disorders: Methods and applications." Neuroscience and biobehavioral reviews vol. 74,Pt A (2017): 58-75. doi:10.1016/j.neubiorev.2017.01.002.
15. Yoo, Youngjin et al. "Deep learning of joint myelin and T1w MRI features in normal-appearing brain tissue to distinguish between multiple sclerosis patients and healthy controls." NeuroImage. Clinical vol. 17 169-178. 14 Oct. 2017, doi:10.1016/j.nicl.2017.10.015.
16. Javaid, A. ., Q. . Niyaz, W. . Sun, and M. . Alam. "A Deep Learning Approach for Network Intrusion Detection System". EAI Endorsed Transactions on Security and Safety, vol. 3, no. 9, May 2016, p. e2, doi:10.4108/eai.3-12-2015.2262516.
17. Nabila Farnaaz, and M.A. Jabbar. "Random Forest Modeling for Network Intrusion Detection System" Procedia Computer Science, vol. 89, 2016. doi:10.1016/j.procs.2016.06.047
18. Z. Fuqun, ''Detection method of LSSVM network intrusion based on hybrid kernel function'', 2,015 Modern Electron. Techn., vol. 38, no. 21, pp. 96–99, 2015.