INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact Factor: 6.078

(Volume 7, Issue 3 - V7I3-1760)

Available online at: https://www.ijariit.com

A study on network intrusion detection system

Vasumathi A. K.
19201008@vcew.ac.in
Vivekanandha College of Engineering for Women, Namakkal, Tamil Nadu

V. Banupriya
banupriya@vcew.ac.in
Vivekanandha College of Engineering for Women, Namakkal, Tamil Nadu

ABSTRACT

In this study, we have tried to survey the methods to detect network intrusions. The Intrusion detection system is important in computer networks for protecting the data. There are several algorithms using neural networks, deep learning, and machine learning to detect intrusion detection in the system. There are many methods for detecting intrusions by ensemble methods, classifiers, anomaly detection giving accuracy according to the methods. The goal of the study is to give a comparison of the methods for an accuracy rate of low rate false alarm and high detection rate. Also, the data sets used in the methods.

Keywords: *Network Intrusion Detection System, Machine Learning Ensemble Method, Dataset, Classifiers.*

1. INTRODUCTION

Nowadays there is a vast use of the internet and networking hence there is a need for security for the internet in personal use or organizational use. Many approaches and methods have been researched and developed to improve the detection rate and performance of intrusion detection systems. Machine learning the study that gives computers the ability to learn without being explicitly programmed. Deep learning a part of the broader family of machine learning methods based on artificial neural networks with representation learning. The differences are Machine learning uses algorithms to parse data, learn from the data and make informed decisions based on what it has learned. Deep learning structures algorithms in layers to create an Artificial Neural Network that can learn and make an intelligent decision on its own.

1.1 Intrusion Detection System

The Intrusion detection system is a necessity when it is clear that intrusion prevention systems such as encryption, firewall and access control are not sufficient in the security of the computer network security.

There are types of intrusion detection which differ in range of scope from single computer to large networks. The classifications are Network Intrusion Detection Systems (NIDS) and Host Based Intrusion Detection Systems (HIDS).

The system that monitors important operating system files is an example of HIDS. The system that analyzes incoming network traffic is an example of NIDS.

Network Intrusion Detection Systems (NIDS): These are placed at a strategic point within to monitor the traffic to and from all the devices on the network, it analyzes the traffic passing and matches the traffic in the subnet, once an attack is sensed it alerts the abnormal behavior to the administrator.

1.2 Datasets

In the past few decades, data mining and machine learning techniques have been extensively researched in developing intrusion detection systems using different intrusion detection datasets. There was the1998 DARPA Intrusion Detection Evaluation Program was prepared and managed by MIT Lincoln Labs. The main objective was to survey and evaluate research in intrusion detection.

1.3 KDD Cup 1999 Data

This is the dataset used for the Third International Knowledge Discovery and Data Mining Tools Competition, this database contains a standard set of data that is to be audited, which includes a wide variety of intrusions simulated in a military network environment.

1.4 NSL-KDD Data

These dataset are used in many of the machine learning methods. NSL-KDD dataset does not include redundant records in the train set; hence the classifiers will not be biased towards frequent records. The number of records in the NSL-KDD train and test sets are reasonable, which makes this dataset affordable to run the experiments on complete set.

Data files in NSL-KDD are KDDTrain+.ARFF, KDDTrain+.TXT, KDDTrain+_20Percent.ARFF, and KDDTrain+_20Percent.TXT, even KDDTrain+.ARFF, KDDTrain+.TXT, KDDTrain+_21Percent.ARFF, and KDDTrain+_21Percent.TXT. There are 41 features of NSL-KDD dataset.

1.5 USNW NB15 Data:

It was created in 2015 by the IXIA Perfect Storm tool in the Cyber Range Lab of the Australian Centre for Cyber Security (ACCS) for generating a hybrid of real modern normal activities and a synthetic contemporary attack behavior, which is widely used in the intrusion detection experiments.

Table 1: Features of NSL-KDD Dataset

Number	Feature	Type of feature	Number	Feature	Type of feature
1	Duration	numeric	22	Is_guest_login	nominal
2	Protocol_type	nominal	23	Count	numeric
3	Service	nominal	24	Srv_count	numeric
4	Flag	nominal	25	Serror_rate	numeric
5	Src_bytes	numeric	26	Srv_serror_rate	numeric
6	Dst_bytes	numeric	27	Rerror_rate	numeric
7	Land	nominal	28	Srv_reerror_rate	numeric
8	Wrong_fragment	numeric	29	Same_srv_rate	numeric
9	Urgent	numeric	30	Diff_srv_rate	numeric
10	Hot	numeric	31	Srv_diff_host_rate	numeric
11	Num_failed_logins	numeric	32	Dst_host _count	numeric
12	Logged_in	nominal	33	Dst_host_srv_count	numeric
13	Num_compromised	numeric	34	Dst_host_same_srv_rate	numeric
14	Root_shell	numeric	35	Dst_host_diff_srv_rate	numeric
15	Su_attempted	numeric	36	Dst_host_same_src_port_rate	numeric
16	Num_root	numeric	37	Dst_host_srv_diff_host_rate	numeric
17	Num_file_creations	numeric	38	Dst_host_serror_rate	numeric
18	Num_shells	numeric	39	Dst_host_srv_serror_rate	numeric
19	Num_access_files	numeric	40	Dst_host_rerror_rate	numeric
20	Num_outbound_cmds	numeric	41	Dst_host_srv_rerror_rate	numeric
21	Is_host_login	nominal			

2. NETWORK INTRUSIONS

Network intrusions are any forcible or unauthorized activity on a digital network, as there will be many devices interconnected in the networks. Such unauthorized activities are almost imperiling the security of networks and their data. Online brands, advertisements and companies are the common subject of attacks.to help with these there is necessity to know the types of attacks and intrusion techniques to identify and prevent them from the system.

2.1 Network Intrusion Attacks

There are basic intrusion attacks DoS, Remote to User, User to Super user and Probing which are commonly evaluated in DARPA. The attacks present in NSL-KDD datasets are Probe DoS, U2R and R2L. Even in the KDD99 Dataset attack records are Probe, DoS, U2R and R2L. in the UNSW NB15 also has same attacks as in KDD99 and NSL-KDD, but there are more records of different types of network intrusions which can be explained and datasets can be trained to detect them and prevent them.

Some of the types of attacks are

a. Fuzzers: Fuzzers are cyber-attack and testing procedures where the assailant endeavors security in an application, frameworks or a network by strengthen it with repeated random inputs to crash the network.

b. Backdoor: The backdoor attack is a type of malware that get unauthorized access to a website by the cyber criminals. The malware is entered to the system through the backdoor and makes its way to the organizations private or secure and sensitive data including the personal identifiable information.

c. DoS: Denial of Service (DoS) is network intrusion that is common and it consumes all of the computer's memory and eventually crashes the system by sending the repeated requests, which have to be rejected by the server and which makes the memory full by such request.

d. Probe: Probe is an attack which is intentionally crafted so the target detects and reports the attack with a recognizable fingerprint in the report. A network probe is just a messenger, which delivers a question and return with information really fast. A network administrator to monitor performance in real time is crucial.

e. R2L and U2R: Remote to local attack is widely launched by an attacker to gain unauthorized access to a victim machine in the entire network. Alike U2R User to Root attack is generally launched for illegally obtaining the root's privileges when legally accessing a local machine.

f. Worms: Worm is a cyber-attack that spreads copies of itself from computer to computer. It can replicate itself in the network, and it does not need to attach itself to a software program which can cause damage.

3. MACHINE LEARNING ALGORITHMS FOR NETWORK INTRUSION DETECTION

3.1 AdaBoost-Based Algorithm

An AdaBoost Adaptive-Boosting, by Yoau Freud and Robert Schapire, is a machine learning algorithm. AdaBoost can be used in conjunction with many other types of learning algorithms to improve performances. The output of weak learners is combined into weighted sum that represent final output of the boosted classifier. AdaBoost is adaptive algorithm which means, succeeding weak learners are tweaked in the favor of those instances misclassified by previous classifiers. It is the best-out-of-the-box classifier, when it is used with the decision tree learning. Information gathered at each stage of the AdaBooost algorithm about, relative hardness of each training sample being fed into the tree growing algorithm usually are used to focus on the examples which are considered to be hard to classify. AdaBoost is a successful boosting algorithm developed for binary classification; most of the methods built on this algorithm are stochastic gradient boost machines. In AdaBoost a weak classifier is prepared on the training data by using the weighted samples. The misclassification rate is calculated for the trained model which is modified to use the weights of the training instances. Then, stage value is calculated for the trained model which will provide a weighting for any predictions that the model makes. Thereafter, the training weights are updated by gibing more weight to incorrectly predicted instances and less weight to correct prediction of instances. Hence, AdaBoost ensemble weak models that are being added linearly and train the weighted training data. This process will continue until a pre-set number of weak learners have been created. Making predictions with this algorithm are made by calculating the weighted average of the weak classifiers. The data preparations for AdaBoost are quality data, outliners and noisy data. The advantage of applying the AdaBoost algorithm to intrusion detection corrects the misclassification made by the weak learners and would be less susceptible to over-fitting than most of the algorithms. It is encouraging in the case of recognition performances. If the weak classifiers are used this algorithm is very fast. In [3] decision, rules are provided for both the features that is categorical and continuous, a simple over-fitting handling is used to improve learning results. AdaBoost algorithm results as a low false-alarm rate combined high detection rate and it is faster than the other algorithms in learning stage.

3.2 Feature Extraction Based Algorithms

This is an algorithm to represent feature space used in classification. Feature extraction which is to transform the original feature space to a smaller feature spaces to reduce the dimension [7]. The dimension reduction techniques are widely applied to solve real problems. It is one of the dimension reduction methods which can produce a new set of features by transforming the original input variables. The feature extraction method proposes a Local Latent Semantic Indexing by Singular Value Decomposition (SVD) and Local Kernel Principal Component Analysis (LKPCA) based methods which introduces class information to feature extraction techniques. The most used feature extraction algorithm is Local Semantic Indexing which is an automatic method that transforms the original textual data to a smaller semantic space by taking advantage of some of the implicit higher order structure in association with the words. The transformation is done by applying the truncated Singular Value Decomposition (SVD), as SVD is an optimal linear transformation for dimensionality reduction. Feature Extraction method using SVD, LSI has also an advantage of yielding Zero-mean and uncorrected features. Principal Component Analysis (PCA) is also a feature extraction method which can only extract the linear structure information in the data set. The feature extraction selection method LSI, KPCA is used to improve the performances of Intrusion Detection System. It remarkably increases the classification performances. It also has an advantage as it reduces the computational time.

3.3 Extreme Learning Machines

Extreme Learning Machine (ELM) was invented by G. Huang in 2006, which is based on feed forward neural network. This algorithm provides a far better generalization performance at extremely fast learning speed. Extreme Learning Machine is an algorithm for single hidden layer feed forward neural network, which is predicated on verifiable risk minimization theory. Its learning process needs only single layer iteration. Multiple iterations and local minimization are avoided in this algorithm. The ELM approaches an incredible reduced training time, indeed at the expense of easy online updating and a large initial processing requirement. The characteristics of ELM as given in [4] are it controls its training in one pass, by using the Moore Penrose pseudo inverse to solve a least square equation. The weights are adjusted only between the hidden layer and output nodes. The weights which are between the input nodes and their hidden layers in addition to any of bias values will be randomly and statically assigned till all the weights belong to same continuous probability density function. These attributes which has two effects, one ELM completes its training much faster than normal machine learning and it also avoids local minima concerns. Second effect is processing requirement for the faster training is effectively greater than for a comparably sized machine learning process. The major difference of ELM from Neural Network is ELM does not require gradient–based back propagation to process. These are not accurate as normal Neural Network, but ELM can be used while dealing with the problems that require real-time retraining of the network. An optimal classification of an ELM in a Network Intrusion Detection System part requires an Online Sequential update function which allows for tuning of the Intrusion Detection System in a real time as the system baseline changes. In [8] Online Sequential Extreme Learning OS-ELM is used for processing the Network traffic dataset to detect intrusions. This algorithm is fast and accurate single hidden layer feed forward neural network which can process a network traffic instances one by one or in bits. OS-ELM overcomes the slow learning limitations of feed forward neural network; this provides good generalization performance with fast learning speed. The approximation and classification problem can be solved by using Fuzzy OS-ELM. It is found as one of the emerging classification technique. It can process large data set in less time which makes it good expectant for Intrusion Detection System.

3.4 An Ensemble Method

An ensemble method is techniques that makes multiple models and so combine them to supply improved results. It produces more accurate solutions than one model would produce. Voting and average based ensemble methods are two of the simplest ensemble methods, both are easy to grasp and use. In [11] voting ensemble method is employed. Voting is employed for classification and averaging is employed for regression. There are many methods of voting Majority Voting, Weighted Voting, Simple Averaging and Weighted Averaging. In [15] the voting method is applied to urge more accurate result instead of a single model. They have used Logistic Regression (LR), Decision Tree (DT), Support Vector Machine (SVM) and many more. Using this as single model as input of voting ensemble methods, it can be called as Base Model too. In voting ensemble model, it is prepared for multiple classification models using the training dataset. In [9] a single classifier was selected as base classifier, where the ensemble model was built by using one of the two ensemble technique bagging and boosting. In [5] ensemble method is proposed in contrary with single model incremental classification. They have discussed about adaptive ensemble mode for classification. They have used a new unlabeled instances classified by the weighted voting among the classifiers. The result indicates the ensemble model trained with a fixed number of class labels shows great robustness to learn and classify new class concepts in each test data stream and it outperforms the other two traditional supervised baseline algorithms the ensemble model shows most accuracy rates which is followed by its performance of decision tree classifiers, KNN model achieving the last position in classification performances on each of the selected test set. Ensemble model has great flexibility and adaptableness in novel class detection in data stream environments compared with the standard decision tree and KNN classifiers. In [9] they were ready to propose ensemble models for having high accuracy and low false accuracy rate, there was a best performance produced. They worked on 35 features subset and were able to score 84.25% accuracy and 2.79% FAR. The limitation was it had been used on one dataset to evaluate the built classifiers. In [15] traditional base level machine learning algorithms are not enough, even deep learning methods would produce poor results. In such cases voting ensemble machine learning method has ability to get better detection rate to form potential models.

4. ARTIFICIAL NEURAL NETWORK ALGORITHMS

4.1 Feed Forward Neural Network

Feed Forward Neural Network algorithm is a synthetic Neural Network algorithm where the connections between the nodes don't form a cycle; it is different from its descendant's recurrent neural network. Feed Forward is that the simplest form of ANN technique, the information in a system moves in barely one direction forward, from the input nodes, through the hidden nodes then to the output nodes. There are no loops in the network. The Feed Forward network consists of multilayered neurons. The first layer of neural network has neurons, which are extremely applied input signals. Other layers receive their inputs only from their previous layer of network along with single bias signal source. Feed Forward network further more can be divide as function approximation and Pattern Classification.

4.2 Pattern Recognition

Pattern Recognition is a technique in finding regularities and similarities in data using machine learning. These are trained from labeled training data. It is an assignment of label to a given input value. It gives an efficient algorithm for recognition intelligence applications like image processing, segmentation, Radar Signal Classification which are used in large data set.

The design rules of pattern recognition are Statistical Approach and Structural Approach. Pattern recognition is one of the mostly used for Character Recognition and Image Classification. The Pattern Recognition neural network algorithm is similar to Feed Forward Artificial Neural Network, which can be used to train that classifies the input data. In [12] Feed Forward and Pattern Recognition Neural Network Algorithm with Bayesian Regularization and Scaled Conjugate Gradient training functions to detect intrusion in the network.

4.3 Convolution Neural Network

Convolution Neural Network in an evolution of deep learning that constructs an excellent with the time of deep learning. Convolution neural network could be a deep learning algorithm that takes in an input image, assigned vital numerous objects within the image and ready to differentiate one from another. In convolution neural network preprocessing is lower as compared with the other neural network algorithms the design is analogous compared with connectivity of pattern of nerve cell in human brain. Convolution neural network is very important when deign of an architect which may be good at learning features but it is also scalable to massive data sets. In [14] end-to-end semi-supervised network training classifier of convolution neural network and multilayered feature of convolution neural network to detect network, when the number of iterations is 50, the error value is the smallest, it meets the detection requirement. In [18] they have proposed deep learning give efficient and flexible intrusion detection system using one-dimensional CNN. One-dimensional CNN used for supervised learning on time series data. This technique establish a machine learning based model on the One-dimensional CNN by serializing Transmission Control Protocol and Internet Protocol packets in a predetermined time range as an invasion internet traffic model for the intrusion detection system, where the normal and abnormal network traffics are categorized and labeled for supervised learning in the One-dimensional CNN. In [18] it is evaluated on UNSW_N15 data set. The use of this method gives robustness in the performance with in a large amount of data and giving a computational benefit.

5. COMPARISONS

As surveyed in these different algorithms from the literatures, a comparison table can be drawn.

Table 2: Comparison table

Sl. No	Title and Authors	Advantages	Disadvantages

1	Using Genetic Algorithm For Network Intrusion Detection. Wei LI	Helpful for identification of complex anomalous behaviors	Parameters should be adjusted according to the application environment of the system and the organization's security policy
2	Intrusion Detection: Support Vector Machines and Neural Networks. Srinivas Mukkamala, Guadalupe Janoski, Andrew Sung	Efficient and highly accurate classifiers	The margin of the accuracy is small and may not be statistically significant
3	Ada-Boost Based Algorithm for Network Intrusion Detection. Weiming Hu, Wei Hu, Steve Maybank	It has a very low false alarm rates.	It is not amenable to incremental learning
4	The Application of Extreme Learning Machines to the Network Intrusion Detection Problem. Gideon Creech, Frank Jiang	It offers significant flexibility and long term sustainability to all types of IDS	Selecting representative samples and removing duplicates is extremely complex.
5	An Adaptive Ensemble classifier for mining concept drifting data streams. Dewan Md. Farid, Li Zhang, Alamgir Hossain, Chowdhury Mofizur Rahman, Rebecca Strachan, Graham Sexton, Keshav Dahal	Ensemble classifier efficiently detects the arrival of novel class instances and improves the classification accuracy.	Challenges in data stream classification such as infinite length, limited labeled data, concept drifting and concept evolution
7	Feature Extraction based Approaches for Improving the Performance of Intrusion Detection Systems Long-Sheng Chen, Jhih-Siang Syu	By introducing class information to feature extraction methods can keep the classification performance and reduce the computational time	It cannot be generalized for multi class classification.
8	An intrusion detection system using network traffic profiling and online sequential extreme learning machine	It performs best among studied classifiers for multiclass NSL-KDD datasets	IDS with memory and time constrains find it difficult to process whole dataset.
9	Improving performance of intrusion detection system using ensemble methods and feature selection. Ngoc Tu Pham, Ernest Foo , Suriadi Suriadi.	Techniques reduce the number of irrelevant features and classification accuracy	Only one dataset was used to evaluate the built classifier
11	Intrusion Detection systems using Real-Valued Negative Selection Algorithm with Optimized Detectors Fatemeh Selahshoor, , Hamid Jazayeriy, Hesam Omranpour	To reduce false alarm rate and increase the true positive rate.	Related to overlapping samples where its expression is nor accurate
12	A Feed-Forward and Pattern Recognition ANN Model for Network Intrusion Detection. Ahmed Iqbal, Shabib Aftab.	The Feed-Forward and Pattern Recognition ANN Model for Network Intrusion Detection performed with different performance measures on different intrusion attacks	Both the networks need to be further tunes and used for diverse intrusion datasets
13	On the Feasibility of Deep Learning in Sensor Network Intrusion Detection Safa Otoum , Burak Kantarci and Hussein T. Mouftah	It shows the adaptive machine learning based IDS solution performs at the same rate as the deep learning solution.	To work on larger networks

14	Wireless Network Intrusion Detection Based on Improved Convolutional Neural Network Hongyu Yang and Fengyan Wang	The accuracy and true positive rate of intrusion detection are higher	To improve the generalization ability and effectiveness of the intrusion detection model
15	Network Intrusion Detection System Using Voting Ensemble Machine Learning. Md. Raihan-Al-Masud, Hossen Asiful Mustafa	Compared to SVM, DBN the detection rate is much higher in case of DoS, Probe, U2R and normal traffic detection.	To improve detection rate of R2L
16	Network Intrusion Detection using Supervised Machine Learning Technique with Feature Selection.	The best classifier with higher accuracy and success rate.	Detecting new attacks or zero day attack still remains a research
18	1D CNN based Network Intrusion Detection with Normalization on Imbalanced Data. Meliboev Azizjon, Alikhanov Jumabek, Wooseong Kim	1D CNN 3 layer model outperforms achieving highest accuracy.	The imbalanced data problem leads to poor performance in neural network models
19	Network intrusion detection system using supervised learning paradigm J. Olamantanmi Mebawondua, Olufunso D. Alowolodub , Jacob O. Mebawondua , Adebayo O. Adetunmbi	The method is adopted and cold be used for real time intrusion detection	It fails to test the performance of the model using different number of attributes

6. CONCLUSION

As per the survey it can be concluded the algorithms for network intrusion detection system can be developed using these methods accordingly to get a better accuracy level for the data sets as mentioned above.

7. REFERENCES

[1] Wei Li. "Using Genetic Algorithm for Network Intrusion Detection". https://www.researchgate.net/publication/228695376.

[2] Mukkamala, S.et al. "Intrusion detection using neural networks and support vector machines", IJCNN'02 (cCat.No.02CH37290) 2 (2002): 1702-1707 vol.2. [3] W.Hu and S.Maybank. " AdaBoost-Based Algorithm for Network Intrusion Detection." In IEEE Transactions on Systems, man and Cybernetics, Part B (Cybernetics), vol. 38, no.2, pp.577-583, April 2008,doi: 10.1109/TSMCB.2007.914695.

[3] Creech, Gideon & Jiang, Frank. (2012). "The Application of Extreme Learning Machines to the Network Intrusion Detection Problem". 1479. 1506-1511. 10.1063/1.4756450.

[4] Dewan Md. Farid, Li Zhang, Alamgir Hossain, Choudury Mofizur Rahman, Rebecca Strachan,Graham Sexton, Keshav Dahal. " An Adaptive Ensemble classifier for mining concept drifting data streams". Expert Systems with Applications: An International Journal November 2013 https://doi.org/10.1016/j.eswa.2013.05.001

[5] L.Dali et al.," A survey of intrusion detection system," (WSWAN), Sousse, 2015, pp.1-6, doi: 10.1109/WSWAN. 2015.7210351.

[6] Chen, Long-Shen & Syu, J.-S. (2015). Feature Extraction based Approaches for Improving the Performance of IntrusionDetection Systems. Lecture Notes in Engineering and Computer Science. 1. 289-291.

[7] Raman Singh, Harish Kumar, R.K.Singla, An intrusion detection system using traffic profiling and online sequential extreme learning machine, Expert Systems with Application, Volume 42, Issue 22, 2015, Pages 8609-8624, ISSN 0957-4174, https://doi.org/j.eswa.2015.07.015.

[8] Ngoc Tu Pham, Ernest Foo, Suriadi Suriadi. Improving performance of intrusion detection system using ensemble methods and feature selection. ACSW '18: Proceedings of the Australasian Computer Science Week MulticonferenceJanuary 2018 Article No.: 2 Pages 1-6https://doi.org/10.1145/3167918.3167951

[9] S.Osken, E. N. Yildirim, G.Kataras and L. Cuhaci, "Intrusion Detection System with Deep Learning: A Systematic Mapping Study," 2019 Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science (EBBT), Istanbul, Turkey, 2019, pp.1-4, doi:10.1109/EBBT.2019.8742081

[10] F.Selahshoor, H. Jazayeriy and H.Omranpour, " Intrusion Detection system using Real-Valued Negative Selection Algorithm with Optimised Detectors," 2019 5th Iranian Conference on Signal Processing and Intelligent System (ICSPIS), Shahrood, Iran, 2019, pp. 1-5,doi: 10.1109/ICSPIS48872.2019.9066040.

[11] Iqbal, Ahmed & Aftab, Shabib. (2019). A Feed-Forward and Pattern Recognition ANN Model for Network Intrusion Detection. International Journal of Computer Network and Information Security. 11.19-25. 10.5815/ijcnis.2019.04.03.

[12] S. Otoum, B. Kantarci and H. T. Mouftah, " On the Feasibility of Deep Learning in Sensor Network Intrusion Detection," in IEEE Networking Letters, vol. 1, no. 2, pp. 68-71, June 2019, doi: 10.1109/LNET.2019.29011792

[13] H. Yang and F. Wang, "Wireless Network Intrusion Detection Based on Improved Convolutional Neural Network," in IEEE Access, vol. 7, pp. 64366-64374, 2019, doi: 10.1109/ACCESS.2019.2917299.
[14] M. Raihan-Al-Masud and H. A. Mustafa, " Network Intrusion Detection System Using Voting Ensemble Machine Learning", 2019 IEEE International Conference on Telecommunications and Photonics (ICTP), Dhaka, Bangladesh, 2019, pp. 1-4,doi: 10.1109/ICTP48844.2019.9041736
[15] K. A. Taher, B. Mohammed Yasin Jisan and M.M. Rahman, " Network Intrusion Detection using Supervised Machine Learning Technique with Feature Selection", 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), Dahka, Bangladesh, 2019,pp. 643-646, doi: 10.1109/ICREST.2019.8644161.
[16] Shafee, Ahmed & Baza, Mohamed & Talbert, Douglas & Fouda, Mostafa & Nabil, Mahmoud & Mahmoud, Mohamed. (2019). "Mimic Learning to Generate a Shareable Network Intrusion Detection Model".
[17] M. Azizjon, A. Jumabek and W. Kim, " 1D CNN based network intrusion detection with normalization on imbalanced data" , 2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Fukuoka, Japan, 2020, pp. 218-224, doi: 10.1109/ICAIIC48513.2020.9064976.
[18] J. Olamantanmi Mebawondu, Olufunso D. Alowolodu, Jacob O. Mebawondu, Adebayo O. Adetunmbi, "Network intrusion detection system using supervised learning paradigm", Scientific African, Volume 9, 2020, e00497, ISSN 2468-2276, https://doi.org/10.1016/j.sciaf.2020.e00497.

BIOGRAPHY

Vasumathi A K
Vivekanandha College of Engineering for Women, Namakkal, Tamil Nadu, India

V Banupriya
Vivekanandha College of Engineering for Women, Namakkal, Tamil Nadu, India

