Comparative Study on TCP SYN Flood DDoS Attack Detection: A Machine Learning Algorithm Based Approach

[1]S. SUMATHI,[2]R. RAJESH

[1] Department of Computer Science & Engineering,
University V.O.C College of Engineering, Thoothukudi – 628008, INDIA.

[2] Department of Engineering Design,
Indian Institute of Technology Madras, Chennai – 600036, INDIA.

Abstract: - A most common attack on the internet network is a Distributed Denial of Service (DDoS) attack, which involves occupying computational resources and bandwidth to suppress services to potential clients. The attack scenario is to massively flood the packets. The attack is called a denial of service (DoS) if the attack originates from a single server, and a distributed denial of service (DDoS) if the attack originates from multiple servers. Control and mitigation of DDoS attacks have been a research goal for many scholars for over a decade, and they have achieved in delivering a few major DDoS detection and protection techniques. In the current state of internet use, how quickly and early a DDoS attack can be detected in broadcasting network transactions remains a key research goal. After the development of a machine learning algorithm, many potential methods of DDoS attack detection have been developed. The work presents the results of various experiments carried out using data mining and machine learning algorithms as well as a combination of these algorithms on the commonly available dataset named CAIDA for TCP SYN flood attack detection. Also, this work analysis the various performance metrics such as false positive rate, precision, recall, F-measure and receiver operating characteristic (ROC) using various machine learning algorithm. One-R(OR) with an ideal FPR value of 0.05 and recall value of 0.95,decision stump(DS) with an ideal precision value of o.93,PART with an excellent F-measure value of 0.91 are some of the performance metric values while performing TCP SYN flood attack detection.

Key-Words: - DDoS, TCP SYN flood, Machine Learning.

Received: April 5, 2021. Revised: October 9, 2021. Accepted: October 30, 2021. Published: November 18, 2021.

1 Introduction

Networking, cloud computing, and internet services have become necessary because of the drastic development in the field of communication technologies. Various advancements in the field of communication guarantee the supply of sources and mechanisms such as remote access, file sharing, etc. The increased dependency on the internet in turn increases unauthorized users who in turn deny the mandatory services to normal users [1]. To ensure the quality of new services, a complex system made up of heterogeneous elements is proposed. These elements constantly interact with each other and also operates at a much higher speed. The usual problem faced by network operator is the unusual event which in turn exhibit malicious behavior. The challenge lies in anomaly detection and classification since it is very difficult to monitor the traffic. A distributed denial of service (DDoS) attack is a malicious internet attack that interrupts normal traffic by creating Internet flood traffic.

DDoS attacks can be carried out in the network and application layers. Usually, attackers perform DDoS attacks on the network layer. The network layer DDoS attacks include ICMP, SYN, and UDP flooding [2]. IP packets are exposed in network layer attacks and hence the attacker alters the packet header. Hence the source IP cannot be used to find the origin of the packet. Rewriting the source IP with a duplicate address is known as spoofing. IP traceback is used to find the origin of the attack that causes the traffic. Attackers exploit any attributes such as packet size, packet rate, bit rate, arrival time, etc., which consumes the available resources which in turn makes service unavailable to authorized users. Generally, DDoS attack packets have a high bit rate which performs network layer attacks. The DDoS attack contains four components are illustrated in Figure 1. The first element is the

victim where the target host is to be selected to obtain the resource from the attack. The next element is the presence of an attack daemon agent, which is also called an agent program, and its duty to attack the target victim. The attack daemons are organized in the host system. Both target and host system are affected by these daemons. The task of this attack daemon is to access the gain and infiltrate the host computer. The third component is the master program where it organizes the attack. Finally, the real attacker is present in the following step; it stays behind the scenes of the attack because of the usage of the control master program.

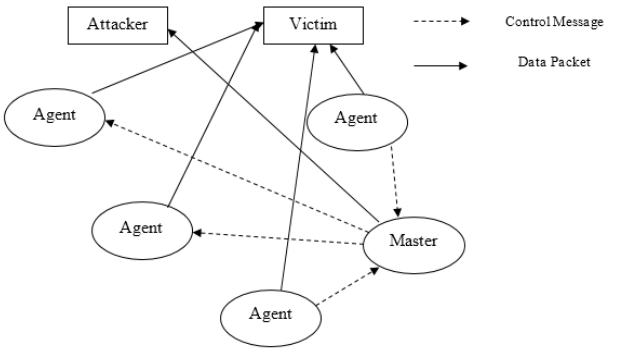

Figure 1. Distributed Denial of Service attack

TCP SYN FLOOD attack is one of the protocols-based DDOS attacks against networks [3]. A substantial space allocation feature in the queue of connections has been exploited in this attack. Multiple connection initialization put forth by the attacker never gets completed making the queue of connections indefinite. The transgressor sends multiple TCP connection requests using repeated SYN packets. Most often fake IP address is used to send these packets to all the ports of the targeted server. Targeted resources are consumed and this, in turn, makes the server unresponsive. In the case of a normal TCP three-way handshake, the connection is requested by sending synchronize message (SYN) to the server. The server acknowledges it by sending synchronize acknowledgment message to the client. Finally, the connection is established when the client responds with an acknowledgment (ACK) message.

In the case of the TCP SYN FLOOD attack, as shown in Figure 2, the attackers make use of fake IP addresses and send repeated SYN packets to all ports on a server. The server tries to establish a connection for these multiple requests with an SYN-ACK packet. The malignant client fails to send the expected ACK and in case if the IP address has been spoofed it never receives the SYN-ACK. The server under attack waits sometimes for acknowledgment of the SYN-ACK packet. Hence the server will not be able to close this connection and it stays open. This gradually leads to a large number of half-open connections and hence these attacks are also known as "half-open" attacks. In due course connection tables of the server gets filled denying authorized client services. This finally leads to server malfunction and crash.

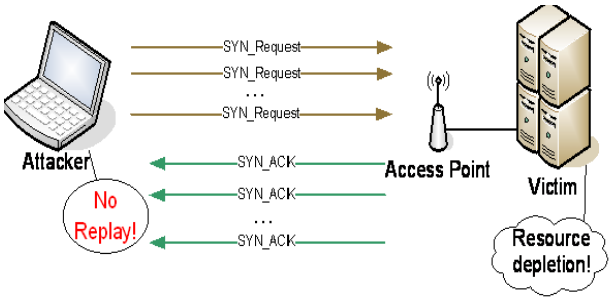

Figure 2. TCP SYN Flood Attack

The knowledge discovery in databases named data mining plays a significant role in attack detection enforcing cloud security. Data mining transfers raw data into organized information by using various types of classes such as classification, clustering, and association rule mining, etc. Data mining designs an intrusion detection system that retrieves the hidden information from the database [4]. Using data mining techniques, we can model the traffic patterns and use them for anomaly and misuse detection. Misuse detection is signature-based and only those intrusions whose signatures are available can be detected. Anomaly detection is the detection deviation from normal samples and models are detected. This detection performs better as it detects unknown and new attacks.

Machine learning algorithms can learn automatically and improve through the experience without exact programming [5]. It also makes accurate predictions using software applications. Designing an Intrusion Detection System using machine learning algorithms requires that the algorithms are trained to study the behavior of the system. This study is classified as supervised or unsupervised supervised machine learning has trained data classified as either normal or malicious [6]. While training, a model between classes and features is found using machine learning algorithms which are used to predict a new class of data termed testing data [7].

In this work conducted the study on different machine learning algorithms such as Naïve Bayes [8], Bayes Net [9], Naïve Bayes updateable [10], Function logistic [11], Multilayer perceptron [12],

Sequential minimal optimization [13], Simple logistic [14], Sequential minimal optimization [15], Voted perceptron [16], IBK [17], K-star [18], Locally weighted learning [19], Decision table [20], J-Rip [21], One R [22], PART [23], Decision stump [24], Hoeffding tree [25], J-48 [26], Logistic model tree [27], Random forest [28] and REP tree [29] to detect the DDoS attack detection.

2 Related Works

Reliability, availability, and security (RAS) are the main issues of cloud computing. The cloud service provider should be able to provide the intended services and be able to manage the security from serious threats. Cisco 2016 Annual Security Report [30] showed DoS attacks still top the External Challenges Faced. In September 1996, an SYN Flood attack was discovered, a smurf attack began in January 1998 and an HTTP flood was the modern DoS that began in 2004. DDoS attacks have two consequences: either they are unable to provide the service as specified in their QoS agreement, or their resources are compromised, allowing them to launch an attack against another site. Experts in the field recommend a comprehensive security architecture based on identification, which can be anomaly-based, signature-based, or a combination of the two. Because of the automatic classification, neural networks, radial basis functions, and genetic algorithms are progressively used in DoS detection.

A network traffic analysis-based anomaly-based DDoS detection method is suggested in [31]. This approach used a radial-based function (RBF) Neural Network, and they tested it on a UCLA dataset, achieving a 96 percent accuracy rate for a DDoS attack. In [32] each attack class, the propound model used a Naive Bayes Classifier with K2 Learning method on a reduced NSL KDDOS data set. Each layer is separately trained to detect a single type of attack class, and the result of one layer is used to improve the detection rate and for better categorization of both majority and minority attacks. The Hidden Naive Bayes Multiclass Classifier Model on network Intrusion Detection System for struggling progressively sophisticated network attacks used in [33].

In [34] has introduced a Probabilistic Neural Network-Based Attack Traffic Classification to detect different DDoS attacks, also focus on separating Flash Crowd Event from DoS Attacks. They used Bayes decision rule for Bayes inferences and Radial Basis Function Neural Network (RBFNN) for classifying DDoS attack traffic and normal traffic as part of their study. A neural network was used in [35] to detect the number of zombies involved in DDoS attacks. They aim to figure out the relationship between zombies and sample entropy using a feed-forward neural network.

In [36] used Artificial Neural Networks (ANN) to detect DDoS attacks, comparing the results with decision trees, ANN, entropy, and Bayesian methods. The authors identified users' requests to a specific resource and their communicative data. Then samples of such requests are sent to the detection systems to be judged for abnormalities. In [37] proposed the most frequently used kNN algorithm for detecting the different types of anomalies in the network. By using the kNN algorithm, a maximum number of bots in the network were identified. Accuracy was improved compared to any algorithm in detecting the unknown attacks. In [38] describes the detection of attacks using classification algorithms to monitor the incoming and outgoing packets in the network and also to compile the TCP SYN and ACK flags in the network. Some other applications of Machine Learning can be found in [42], [43], [44], [45], [46] and [47].

3 Experimental Results & Discussion of Performance Metrics

The CAIDA dataset is used in the experiment as the attack component. Data collected on the SSE network provided the normal traffic component. Classification of attack and normal traffic is done using an open-source tool called KNIME version 3. The different machine learning algorithms are used to analyze the DDoS attack detection. The efficiency of the algorithm analyzed based on different performance metrics is given below.

3.1 False-positive rate (FPR)

Machine learning models subsets are evaluated by means of an accuracy performance metric called False positive rate(FPR).In this,accuracy measurement is done by making comparisons between the ground truth and the models output.In the case of supervised learning,the underlying data is defined as well as described by the ground truth.FPR also termed as fall-out are the negative cases which are wrongly identified as positive cases.Positive class incorrect prediction is termed as false positive (FP) [38]. Negative class correct prediction is termed as True negative (TN). False-positive rate (FPR) is the FP value divided by the summation of FP and TN. This metric helps in

analyzing algorithm efficiency in detecting the TCP SYN flood attack.

Table 1 indicates that among the function classifiers SMO has ideal FPR. SGD and simple logistic perform at the same rate based on FPR. LWL has an FPR value of 0.08 and was found to perform better for SYN flood detection. One R has been identified as one of the good rule-based classifiers for TCP SYN flood detection. J-Rip and PART have an equal FPR of 0.16. The decision stump tree classifier has an ideal FPR value for DDoS attack detection. Figure 3 clearly shows onetime R and decision stump performs better with low FPR rate in detecting TCP SYN flood DDoS attack.

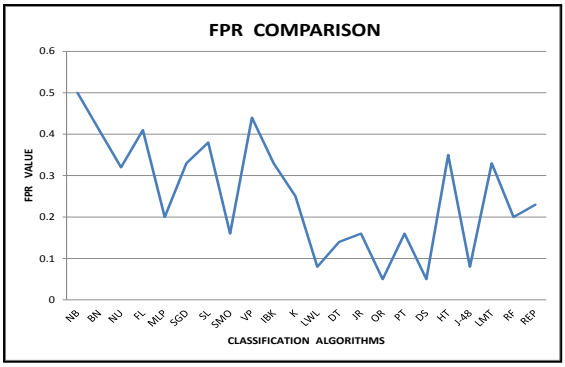

Figure 3. FPR Comparison for Data mining and Machine learning algorithms

3.2 Precision

Positive predictive value shortly named precision is one of the important evaluation metrics for data mining algorithms. Hence this metric plays a vital role in detecting flood attacks. It is the fraction of pertinent occurrence among the recovered occurrences. Precision is defined as the intersection of relevant and retrieved documents divided by the retrieved documents. In short, precision is the ratio between True Positive value and summation of True positive and False positive [39].

From Table 1 we can infer MLP has a perfect precision value of 0.89 among the function classifiers. LWL lazy classifier has a classic precision value for detecting TCP SYN flood attacks. Rule-based classifier Decision table (DT) has a fine precision value for DDoS attack detection. Decision stump and J-48 have an equivalent excellent precision value of 0.93 for layer 4 DDoS attack detection. It can be easily visualized from the below Figure 4 that the tree classifiers decision stump and J-48 performs better while precision is considered as an evaluation metric for TCP-SYN flood attack detection.

3.3 Precision

Recall commonly known as sensitivity is a quantitative evaluation metric. It is the ratio of retrieved relevant documents to the total relevant documents. In short, recall is defined as the ratio between the true positive and a total number of true positive and false negative [40]. Recall value estimates data mining algorithm efficiency in detecting TCP SYN attack.

From the above Table 1 we can infer the function classifier SMO has a satisfactory recall value to detect the flood-based attack. IBK Lazy Classifier has a recall value identical to SMO and performs better in detecting DDoS among the Lazy Classifiers. The Rule-based Classifier One R (OR) has an exemplary Recall value of 0.95 and achieves better DDoS detection among the Rule-based Classifiers. The Hoeffding tree classifier has an outstanding recall value among the tree classifiers in detecting the layer 4 DDoS attack. Figure 5 clearly shows that the Rule-based classifier one R has a high recall value of 0.95 and detects TCP-based DDoS attack efficiently.

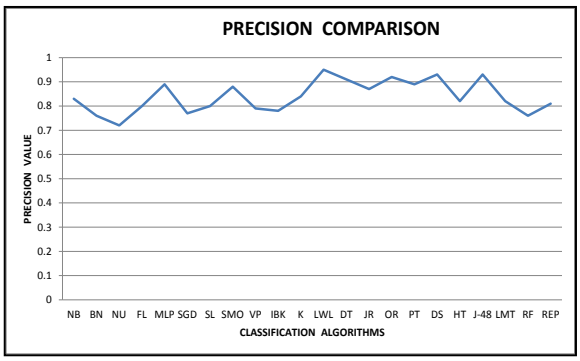

Figure 4. Precision Comparison graph for Data mining and Machine learning algorithms

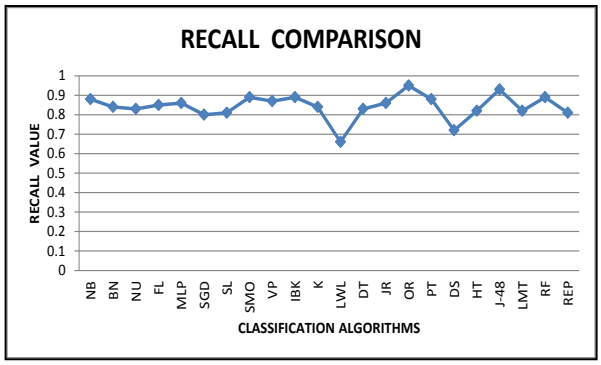

Figure 5. Recall Comparison graph for Data mining and Machine learning algorithms

3.4 F-measure

F-measure shortly named as F or F1 is an accuracy test metric [41]. It is proposed to balance precision and recall. 1 is the best F1 score where 0 is the worst F1 score. As the name implies F1 is a function of precision and recall. F-measure is used for binary classification evaluation, search engine evaluation etc. A model is said to be accurate if it has a high F-measure value. Hence, this is an indispensable measure in assessing the mining algorithm performance. F-measure is represented mathematically as a harmonic mean of recall and precision as follows

$$F\ measure = \frac{2 \times Precision \times Recall}{Precision + Recall}$$

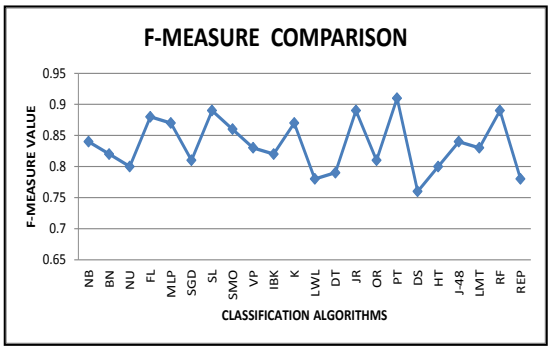

Figure 6. F - Comparison graph for Data mining and Machine learning algorithms

Table 1 shows that the simple logistic has a precise F-measure value for attack detection in a cloud-based environment. The K-Star Lazy Classifier has a first-rate F-measure value in DDoS attack identification. The PART Rule-based Classifier has a fabulous F-measure value of 0.91 and carries out DDoS-based attack detection in a systematic manner. The Random forest algorithm has an absolute F-measure value while diagnosing the TCP-based flood attack in a cloud scenario. Figure 6 indicates that the rule-based classifier PART has a good F-measure value and better detects the transport layer DDoS attacks.

3.5 Receiver operating characteristic (ROC)

ROC curve is a graphical chart for analyzing the capacity of the data mining algorithm. This curve is derived when TPR is plotted against FPR. This curve helps in the optimal selection of algorithms for TCP-SYN flood detection. If we have a greater area under the curve for a particular algorithm it means it performs better in attack detection.

Simple logistics accomplish an outrageous DDoS detection rate among the Function Classifiers with a ROC value of 0.89. The K-Star Lazy Classifier better catches the TCP-based DDoS attack packets with a ROC value of 0.87. PART has an impressive ROC value and hence detects the cloud-based Transport layer attack in a spectacular manner. The Random forest algorithm has a flawless ROC value and achieves flood attack detection at a faster rate. Figure 7 shows that PART has an ideal ROC value.

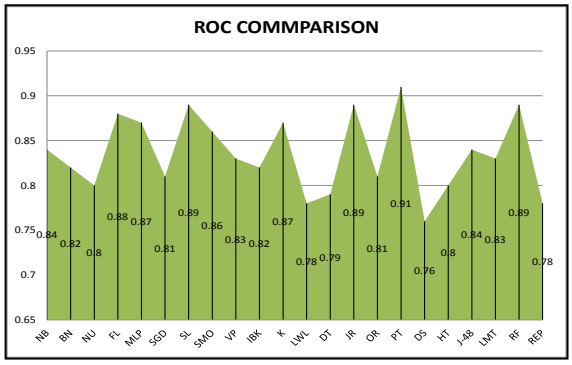

Figure 7. ROC Area Comparison graph for Data mining and Machine learning algorithms

Table 1. Experimental Results of Classification Algorithm Evaluation for TCP SYN Flood Attack

Algorithms	FPR Value	Precision Value	Recall Value	F-Value	ROC Area
Naïve Bayes (NB)	0.50	0.83	0.88	0.84	0.84
Bayes Net (BN)	0.41	0.76	0.84	0.82	0.82
Naïve Bayes updateable (NU)	0.32	0.72	0.83	0.80	0.80
Function logistic (FL)	0.41	0.80	0.85	0.88	0.88
Multilayer perceptron (MLP)	0.20	0.89	0.86	0.87	0.87

Algorithms	FPR Value	Precision Value	Recall Value	F-Value	ROC Area
Stochastic gradient descent (SGD)	0.33	0.77	0.80	0.81	0.81
Simple logistic (SL)	0.38	0.80	0.81	0.89	0.89
Sequential minimal optimization (SMO)	0.16	0.88	0.89	0.86	0.86
Voted perceptron (VP)	0.44	0.79	0.87	0.83	0.83
IBK	0.33	0.78	0.89	0.82	0.82
K-star (K)	0.25	0.84	0.84	0.87	0.87
Locally weighted learning (LWL)	0.08	0.95	0.66	0.78	0.78
Decision table (DT)	0.14	0.91	0.83	0.79	0.79
J-Rip (JR)	0.16	0.87	0.86	0.89	0.89
One R (OR)	0.05	0.92	0.95	0.81	0.81
PART (PT)	0.16	0.89	0.88	0.91	0.91
Decision stump (DS)	0.05	0.93	0.72	0.76	0.76
Hoeffding tree (HT)	0.35	0.82	0.82	0.80	0.80
J-48	0.08	0.93	0.93	0.84	0.84
(Logistic model tree) LMT	0.33	0.82	0.82	0.83	0.83
Random forest (RF)	0.20	0.76	0.89	0.89	0.89
REP tree (REP)	0.82	0.81	0.81	0.78	0.78

4 Conclusion

As detection of DDoS attack has become more common in a distributed environment like Cloud, and it is essential to detect the attacks which cause service unavailability of Cloud. To identify such attacks, machine learning models can be used to train and test the attack detection datasets. This article analyzed the TCP-SYN flood attack detection for the CAIDA data set. Experimental results and graphs reveal that the decision stump has an ideal FPR as well as precision value. Similarly, PART has a good ROC and F-measure value while One-R has an excellent Recall value. Decision stump, PART, and One-R show meritorious performance in detecting OSI fourth layer TCP flood attack in a cloud domain.

References

[1] R. Devi, R.K. Jha, A. Gupta, S. Jain, and P. Kumar "Implementation of Intrusion Detection System using Adaptive Neuro-Fuzzy Inference System for 5G wireless communication network," *AEU-International Journal of Electronics and Communications*, vol.74, pp. 94-106, 2017.

[2] S. Dash, R. K. Mishra, R. K. Das, and M. Panda "Comparison of AIS based Data Mining Algorithms for Intrusion Detection," *International Journal of Computer Science and Information Security*, vol.15, no.1, pp. 619, 2017.

[3] L. Zhang, Q. Deng, Y. Su, and Y. Hu, "A box-covering-based routing algorithm for large-scale SDNs," *IEEE Access*, vol. 5, no. 1, pp. 4048_4056, 2017.

[4] P. Wang, H.T. Lin, and T.S. Wang, "An improved ant colony system algorithm for solving the IP traceback problem," *Information Science*, vol. 326, pp. 172-187, 2016.

[5] G. Somani, M.S. Gaur, D. Sanghi, and M. Conti,"DDOS Attacks in Cloud Computing: Collateral Damage to Non-targets," *Computer Networks*, vol. 109, no. 2, 2016, pp. 157–171.

[6] Victor Chang, Yen-Hung Kuo, Muthu Ramachandran, "Cloud computing adoption framework: A security framework for businessclouds." *Future Generation Computer Systems*, Vol. 57, pp. 24-44, 2016.

[7] W. Cerroni, G. Moro, R. Pasolini, and M. Ramilli, "Decentralized detection of network attacks through P2P data clustering of SNMP data," *Computers & Security*, vol. 52, pp. 1–16, 2015

[8] K.Vembandasamy, R. Sasipriya, E. and Deepa, "Heart diseases detection using Naive Bayes algorithm. International Journal of Innovative Science," *Engineering & Technology*, vol.2, no.9, pp.441-444, 2015.

[9] V. Muralidharan, and V. Sugumaran, "A comparative study of Naïve Bayes classifier and Bayes net classifier for fault diagnosis of monoblock centrifugal pump using wavelet analysis," *Applied Soft Computing*, vol.12, no.8, pp.2023-2029, 2012.

[10] R. Saptono, M.E. Sulistyo, and N.S. Trihabsari, "Text Classification Using Naive Bayes Updateable Algorithm In SBMPTN Test Questions," *Telematika: Jurnal Informatika dan Teknologi Informasi*, vol. 13, no.2, pp.123-133. 2016.

[11] R. Real, A.M. Barbosa, and J.M. Vargas, "Obtaining environmental favourability functions from logistic regression," *Environmental and Ecological Statistics*, vol.13, no.2, pp.237-245, 2006.

[12] D.W. Ruck, S.K. Rogers, and M. Kabrisky, Feature selection using a multilayer perceptron. *Journal of Neural Network Computing*, vol. 2, no.2, pp.40-48, 1990.

[13] Q. Qian, R. Jin, J. Yi, L. Zhang, and S. Zhu, S. "Efficient distance metric learning by adaptive sampling and mini-batch stochastic gradient descent (SGD)," *Machine Learning*, vol. 99, no. 3, pp.353-372, 2015.

[14] H. Khalajzadeh, M. Mansouri, and M. Teshnehlab, "Face recognition using convolutional neural network and simple logistic classifier, In Soft Computing in Industrial Applications (pp. 197-207). Springer, Cham, 2014.

[15] L.J. Cao, S.S. Keerthi, C.J. Ong, J.Q. Zhang, U. Periyathamby, X.J. Fu, and H.P. Lee, "Parallel sequential minimal optimization for the training of support vector machines," *IEEE Trans. Neural Networks*, vol. 17, no.4, pp.1039-1049, 2006.

[16] Y. Freund, and R.E. Schapire, "Large margin classification using the perceptron algorithm," *Machine learning*, vol. 37, no.3, pp.277-296, 1999.

[17] G. MeeraGandhi, "Machine learning approach for attack prediction and classification using supervised learning algorithms," *Int. J. Comput. Sci. Commun*, vol.1, no.2, pp.247-250, 2010.

[18] S. Painuli, M. Elangovan, and V. Sugumaran, "Tool condition monitoring using K-star algorithm," *Expert Systems with Applications*, vol.41, no.6, pp.2638-2643, 2014.

[19] L. Jiang, Z. Cai, H. Zhang, and D. Wang, "Naive Bayes text classifiers: a locally weighted learning approach," *Journal of Experimental & Theoretical Artificial Intelligence*, vol.25, no.2, pp.273-286, 2013.

[20] M. Moshkov, and I. Chikalov, "On algorithm for constructing of decision trees with minimal depth," *Fundamenta Informaticae*, vol. 1, no. 3, pp.295-299, 2000.

[21] W. Shahzad, S. Asad, and M.A. Khan, "Feature subset selection using association rule mining and JRip classifier," *International Journal of Physical Sciences*, vol. 8, no.18, pp.885-896, 2013.

[22] G. MeeraGandhi, K. Appavoo, and S. Srivasta, "Effective network intrusion detection using classifiers decision trees and decision rules," *Int. J. Advanced network and application*, Vol. 2, 2010.

[23] D. Grose, R.B. Wilbur, and K. Schalber, "Events and telicity in classifier predicates: A reanalysis of body part classifier predicates in ASL," *Lingua*, vol.117, no.7, pp.1258-1284, 2007.

[24] A.Q. Ayinde, A.B. Adetunji, M. Bello, and O.A. Odeniyi, "Performance Evaluation of Naive Bayes and Decision Stump Algorithms in Mining Students' Educational Data," *International Journal of Computer Science Issues (IJCSI)*, vol.10, no.4, p.147, 2013.

[25] B.R. Prasad, and S. Agarwal, "Critical parameter analysis of Vertical Hoeffding Tree for optimized performance using SAMOA," *International Journal of Machine Learning and Cybernetics*, vol.8, no.4, pp.1389-1402, 2017.

[26] A.K. Yadav, and S.S. Chandel, "Solar energy potential assessment of western Himalayan Indian state of Himachal Pradesh using J48 algorithm of WEKA in ANN based prediction model," *Renewable Energy*, vol. 75, pp.675-693, 2015.

[27] T.D. Pham, D.T. Bui, K. Yoshino, and N.N. Le, "Optimized rule-based logistic model tree algorithm for mapping mangrove species using ALOS PALSAR imagery and GIS in the tropical region," *Environmental earth sciences*, vol.77, no.5, pp.1-13, 2018.

[28] M. Pal, "Random forest classifier for remote sensing classification," *International journal of remote sensing*, vol. 26, no.1, pp.217-222, 2005.

[29] M. Belouch, S. El Hadaj, and M. Idhammad, "A two-stage classifier approach using reptree algorithm for network intrusion detection," *International Journal of Advanced Computer Science and Applications*, vol. 8, no.6, pp.389-394, 2017.

[30] S. Baller, S. Dutta, and B. Lanvin, Global information technology report 2016. Geneva: Ouranos, 2016.

[31] R. Karimazad and A. Faraahi, "An anomaly-based method for DDOS attacks detection using rbf neural networks," in 2011 International Conference on Network and Electronics Engineering, IPCSIT, vol. 11 , 2011.

[32] J.K. Bains, K.K. Kaki, and K. Sharma, "Intrusion Detection System with Multi Layer using Bayesian Networks," *International Journal of Computer Applications*, vol. 67, no.5, 2013.

[33] V. Akilandeswari, S.M. Shalinie, Probabilistic neural network based attack traffic classification, in: Proceedings of the Fourth International Conference on Advanced Computing (ICoAC), Chennai, 13–15 Dec. 2012, pp.1–8.

[34] B.B. Gupta, C. Joshi, M. Misra, "ANN based scheme to predict number of zombies in a DDOS attack," *International Journal Network Security*, vol.13, no.3, pp. 216–225, 2011.

[35] J. Li, Y. Liu, and L. Gu, "DDOS attack detection based on neural network," in 2nd International Symposium on Aware Computing (ISAC),. IEEE, 2010, pp. 196–199.

[36] P. Xiao, W. Qu, H. Qi, and, Z. Li, "Detecting DDOS attacks against data center with correlation analysis," *Computer Communication*, vol. 67, pp. 66–74, 2015.

[37] Y.C. Wu, H.R. Tseng, W. Yang, and R.H. Jan, "DDOS detection and traceback with decision tree and grey relational analysis," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 7, no.2, pp.121-136, 2011.

[38] R. Singh, H. Kumar, and R. K. Singla, "An intrusion detection system using net- 1508 work traffic profiling and online sequential extreme learning machine," *Expert Systems with Applications,* vol.42, pp. 8609–8624, 2015.

[39] A. A. Ramaki, M. Amini, and R. E. Atani, "RTECA: Real time episode correlation algorithm for multi-step attack scenarios detection," *Comput. & Sec.*, vol. 49, pp. 206–219, 2015.

[40] A. Araar and R. Bouslama, "A comparative study of classification models for detection in ip networks intrusions." *Journal of Theoretical & Applied Information Technology*, vol. 64, no. 1, 2014

[41] Shaveta Gupta, Dinesh Grover and Abhinav Bhandari, "Detection Techniques against DDOS Attacks:A Comprehensive Review," *International Journal of Computer Applications*, Vol. 96. no.5. pp. 0975-8887, 2014.

[42] Keon Myung Lee, Jaesoo Yoo, Jiman Hong , "Conceptualization of an Autonomic Machine Learning Platform for Non-Expert Developers", WSEAS Transactions on Computers, pp.252-259, Volume 16, 2017

[43] Meera Sharma, Sonok Mahapatra, Adeethyia Shankar, Xiaodi Wang, "Predicting the Utilization of Mental Health Treatment with Various Machine Learning Algorithms", WSEAS Transactions on Computers, pp.285-291, Volume 19, 2020

[44] Adelina Aleksieva-Petrova, Veska Gancheva, Milen Petrov, "APTITUDE Framework for Learning Data Classification based on Machine Learning", International Journal of Circuits, Systems and Signal Processing, pp. 379-385,Volume 14, 2020

[45] Hossam Meshref, "Predicting Loan Approval of Bank Direct Marketing Data Using Ensemble Machine Learning Algorithms", International Journal of Circuits, Systems and Signal Processing, pp. 914-922, Volume 14, 2020

[46] Yanhong Zhao, Hanqiao Jiang, Hongqi Li, "Prediction of Casing Damage: A Data-Driven, Machine Learning Approach", International Journal of Circuits, Systems and Signal Processing, pp. 1047-1053, Volume 14, 2020

[47] Sussy Bayona-Oré, Rino Cerna, Eduardo Tirado Hinojoza, "Machine Learning for Price Prediction for Agricultural Products,WSEAS Transactions on Business and Economics", pp.969-977, Volume 18, 2021

Creative Commons Attribution License 4.0 (Attribution 4.0 International , CC BY 4.0)