International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 10 | Oct -2020 ISSN: 2582-3930

HYBRID CLASSIFICATION BASED INTRUSION DETECTION SYSTEM FOR CLOUD NETWORK

Dheeraj Kumar, Rajan Sachdeva

Research Schloar (M.Tech CSE)
H.O.D. Computer Science and Engineering
Guru Gobind Singh College of Modern Technology, Kharar, S.A.S. Nagar, Punjab 140301

Abstract: Cloud computing is a wide field through which the uses of resources can be performed efficiently. The cloud service users can share cloud resources anytime, anywhere. However, networking is the most important platform for getting information in the cloud. The attacker in the cloud is harmful as these malicious users extract the useful information of the cloud users. The Intrusion Detection System (IDS) is one of the best solutions, which tracks the network and follow the secure route. In this paper, the selection of a secure route is performed using a Support Vector Machine (SVM) with Artificial Neural Network (ANN) approach. The nodes properties are optimized and selection of desired or most useful features have been performed using Cuckoo Search (CS) and SVM approach. The detection of the abnormal node that is the DDoS affected node has been performed using the ANN approach. The experiment reveals that the detection rate of 97.04 % has been obtained.

Keywords: Intrusion Detection System, Cuckoo Search, Support Vector Machine, Artificial Neural Network

I. Introduction

Cloud computing the concept of "cloud computing", according to which the programs are run and produce results in a standard web-window browser on the local PC, with all applications and their data necessary for work are located on a remote server on the Internet [1]. Computers that perform these calculations are called the “computing cloud." In this case, the load between computers included in the "computing cloud" is distributed automatically [2].

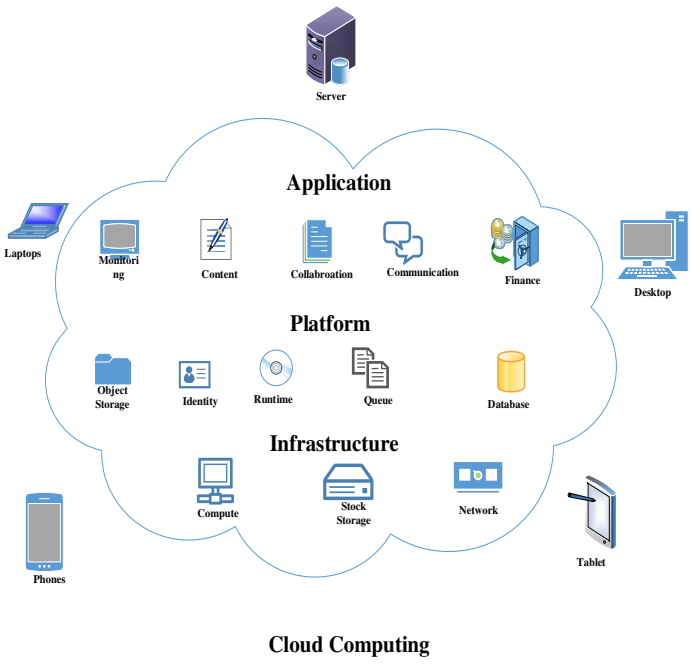

Figure 1: Cloud Computing Environment

Cloud security is one of the most important issues that have been involved in many research and many efforts have been made by developers over the past few years [3]. Intrusion Detection Systems (IDS) has been investigated for some years back to provide security of cloud data against various attacks. According to the design and applications IDS can be categorized into different types (i) host-based intrusion detection systems (HIDS), (ii) network-based intrusion detection systems (NIDS)[4]. Also, based on the structure of the cloud, IDS can be segregated as:

i. software-based IDs
ii. and hardware-based IDS
iii. VM based IDS

Currently, numerous commercial and open-source IDS network have emerged and have been extensively used in practice to detect malicious behavior against the

defended environment [5]. A well-known example of existing IDS solutions is F-Secure Linux Security. Effective IDS should be able to detect different types of attacks, along with all possible variations appear in the network [6]. IDS must detect not an only malicious node but also the normal node. Therefore, it is necessary to design a robust security cloud system against different attacks [7].

The main aim of this paper is to secure cloud network against Distribution Denial of Services (DDoS) attack using IDS approach in hybridization with SM with ANN classifier.

II. Related Work

Security in the cloud environment is one of the biggest obstacles to cloud-based applications. The utilization of a wireless network for data uploading and downloading can intercept network attacks and hence modify the data. The cloud follows distributed technology; therefore, vulnerable to attacks by malware. The emergence of IDS has become a key component in the network protection infrastructure and a necessary way to protect against system attacks. Distributed Denial of Service (DDoS) attacks are a big problem for a computer user who is connected to the Internet. A survey has been conducted to know the performance of IDS networks using distinct approaches [8]. **Velliangiri and Premalatha (2019) have used** Radial basis function neural network (RBF-NN) as a classification approach to distinguish the normal node from the attacker node, particularly for DDoS attack. The network has been learnt the properties of the nodes based on the trial and the error concept [9]. **Mayuranathan, et al. (2019)** have presented a feature extraction based IDS system against DDoS attack. Random Harmony Search (RHS) has been used as a feature selection approach that helps to increase the accuracy of the system. The selected features are applied as input to the Restricted Boltzmann Machines (RBM) as a deep learning approach that has been used for the detection and identification of DDoS attack [10]. **Rawashdeh et al. (2018)** have presented an IDS system against DDoS attack specifically in the hypervisor layer. This network has been used to identify the unwanted activities performed by virtual machines. The detection system has been designed by combining the PSO (Particle Swarm Optimization) approach with ANN (Artificial Neural Network). The results reveal that the DDoS attack has been detected with less false alarm rate and with high detection accuracy [11]. **Alzahrani et al. (2018)** presented a security system for the detection of DDoS attacker node in the cloud environment. Signature-based approach along with ANN has been used for the detection of unknown DDoS attack. The signature-based approach is used to identify the behaviour of the DDoS attacker node. In case of unknown features of DDoS attack, ANN network has been initiated for the detection of the attack. According to which the signature database has been updated for the future use. The detection rate using a hybrid approach of signature with ANN of 98.16 % has been attained [12]. **Abusitta et al.(2018)** have designed a defence system against DDoS attack in virtual cloud environment. The designed model is capable of monitoring as well as to measure the influence on the collected data after the resource adjustment. This process has been used to improve the detection accuracy under dynamic cloud environments [13]. **Nathiya, and Suseendran (2018)** have presented an IDS based monitoring system for DDoS attack. This approach helps to identify the known and unknown DDoS attack during the VM migration in the cloud. The intruder has been detected using the classification approach and resends a message to the administrator of the cloud. The classification of the attacker has been performed using distinct classifiers such as Naive Bayes, decision tree and SVM. Among all algorithms decision tree perform better with higher accuracy of about 99.3 % [14].

III. Proposed Work

The working process along with the mechanism used for the monitoring and detection of DDoS attack is described in this section. The entire process consists of n number of users, who send requests to their allocated sub-servers. If several users send requests to the same server, then the task of the server is to maintain the uploaded data. The balancing of the load has been performed using CS with SVM and ANN approach. The properties of the data have been optimized using CS as an optimization algorithm with a novel healthy function. The working of the proposed work is depicted in Figure 2.

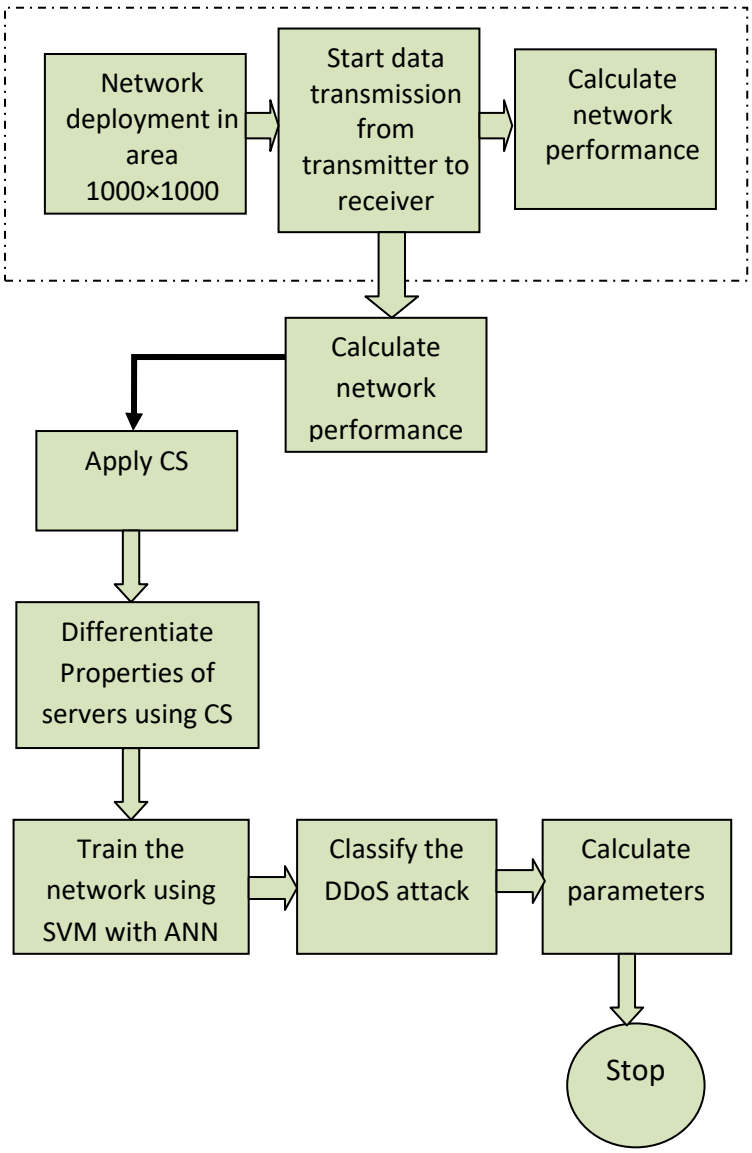

Figure 2: Proposed Work

The server properties are classified into two groups based on their properties normal and abnormal server. Based on these properties, SVM is used to train the system. Based upon their kernel function best nodes or servers are being selected, which is known as support vector. SVM helps to discard un-useful nodes and select only appropriate nodes. The selection of best nodes using SVM has increased the training as well as the detection capability of the network, which is being performed using the ANN technique. The trained ANN structure is shown in Figure 4.9.

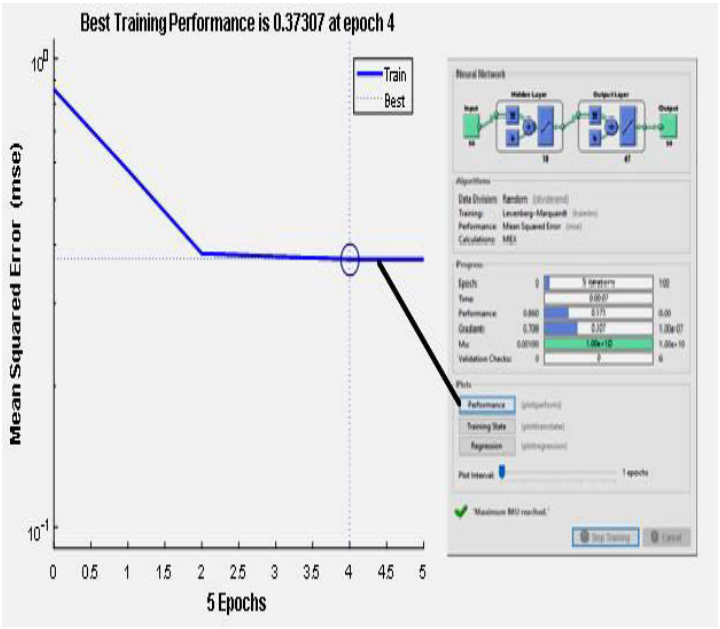

Figure 3: ANN training with MSE

The training using the ANN structure consists of three layers as depicted in Figure 3. From the graph, it is seen that the training has been done with Minimum Mean Square Error (MSE) of 0.3707. After training, testing has been performed and the performance has been analyzed in terms of parameters as discussed in the following section.

IV. Result and discussion

The performance of the proposed work has been discussed in this section in terms of PDR, throughput, energy consumption and detection rate.

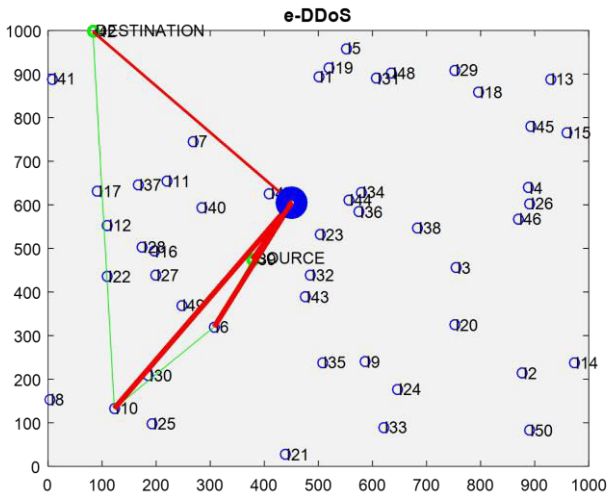

Figure 4: Cloud network

Figure 4 illustrated the designed cloud network comprises of 50 number of nodes as service providers. The DDoS attacker has been inserted as denoted by the blue circle.

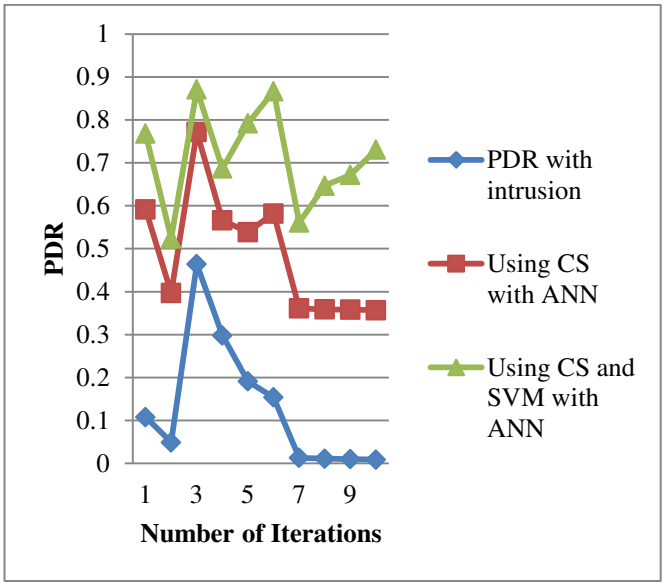

Figure 5: Comparison of PDR

The comparison of PDR values analyzed during the communication process in the presence of DDoS attacker node as well as when the network is prevented from the attacker using CS with ANN and CS with SVM & ANN approach. The analyzed values are depicted in ion Figure 5. From the figure, it is seen that the data has been delivered with high rate while CS with SVM and ANN approach has been used. This is due to the proper selection of servers.

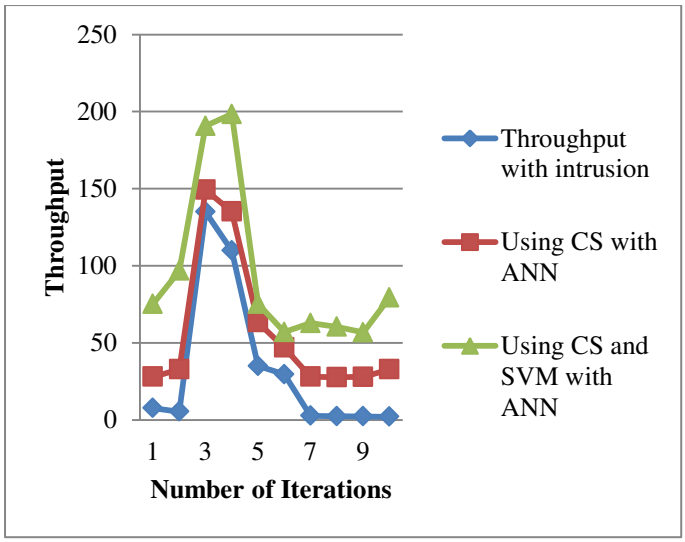

Figure 6: Comparison of Throughput

The throughput analyzed in three different scenarios is depicted in Figure 6. The graph shows an improved throughput compared to the existing CS with ANN and in the presence of an attacker node.

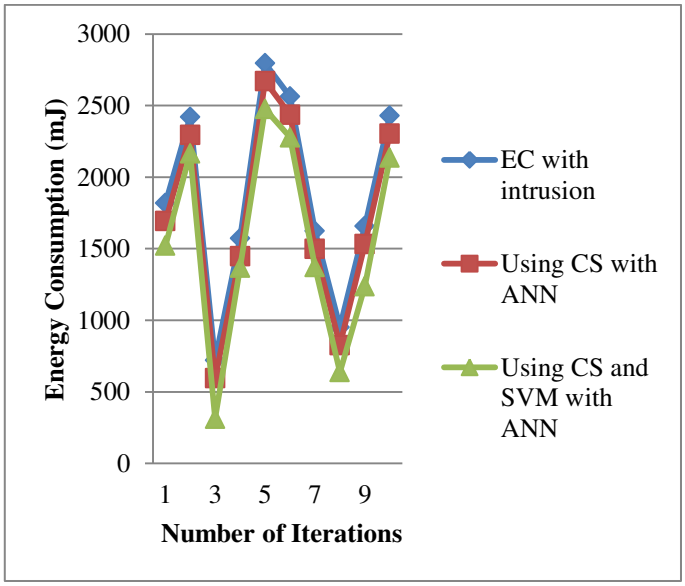

Figure 7: Comparison of Energy Consumption

The energy consumed during the entire communication process is shown in Figure 7. The average energy consumed in the presence of attacker node, CS with ANN and CS with SVM & ANN is 1855.89 mJ, 1730.54 mJ, and 1551.04 mJ respectively. Thus there is an improvement of energy-saving 16.43 %, and 6.75 % against without prevention and while using CS with Ann approach.

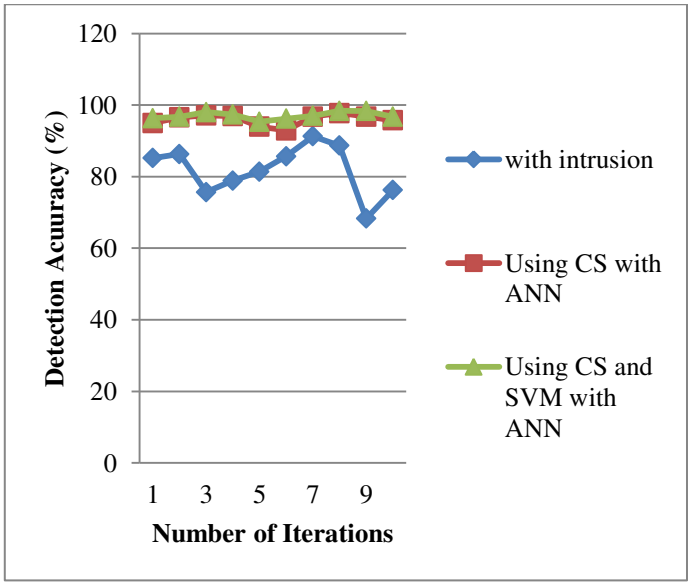

Figure 8: detection Accuracy

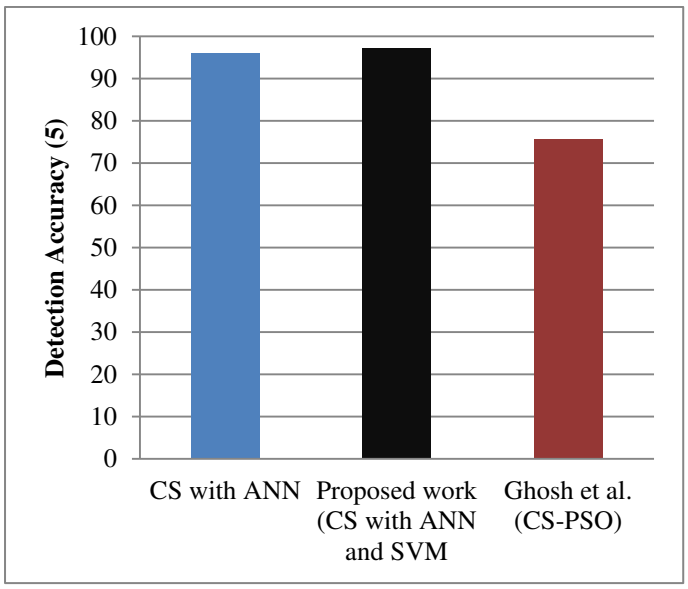

Figure 9: Comparison of Detection accuracy

Figure 9 represents the comparison graph plotted between proposed work CS with ANN, CS with ANN and SVM against the existing work performed by Ghosh et al. (CS-PSO) in 2019. From the graph, it is shown that by utilizing an optimization algorithm along with hybridizing classification technique the detection accuracy enhanced by 28.53 %.

V. Conclusion

This paper presented a hybrid classification approaches SVM with ANN for the protection of cloud network against DDoS attack in integration with Cuckoo Search algorithm. In this paper, the network has been designed for 50 number of cloud servers and trained the system using SVM with the ANN approach. Due to the availability of a number of network attacks such as IP spoofing, malware and DDoS attack, user data is not protected. As the data is confidential and need protection. Therefore, a security system must be designed that can effectively work for the detection of the attack. From the experiment, the results have been computed using CS with SVM and CS with SVM & ANN approach to determine the detection efficiency of the algorithm used. It has been concluded that the optimization with a hybrid classification approach performs well and provide detection accuracy of 97.04 %.

References

[1]. Bakshi, A., & Dujodwala, Y. B. (2010, February). Securing cloud from ddos attacks using intrusion detection system in virtual machine. In *2010 Second International Conference on Communication Software and Networks* (pp. 260-264). IEEE.

[2]. Kumar, N., & Sharma, S. (2013, July). Study of intrusion detection system for DDoS attacks in cloud computing. In *2013 Tenth International Conference on Wireless and Optical Communications Networks (WOCN)* (pp. 1-5). IEEE.

[3]. Aishwarya, R., & Malliga, S. (2014, April). Intrusion detection system-An efficient way to thwart against Dos/DDos attack in the cloud environment. In *2014 International Conference on Recent Trends in Information Technology* (pp. 1-6). Ieee.

[4]. Roschke, S., Cheng, F., & Meinel, C. (2009, December). Intrusion detection in the cloud. In *2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing* (pp. 729-734). IEEE.

[5]. Alqahtani, S. M., Al Balushi, M., & John, R. (2014, March). An intelligent intrusion detection system for cloud computing (SIDSCC). In *2014 International Conference on Computational Science and Computational Intelligence* (Vol. 2, pp. 135-141). IEEE.

[6]. Modi, C., Patel, D., Borisanya, B., Patel, A., & Rajarajan, M. (2012, October). A novel framework for intrusion detection in cloud. In *Proceedings of the fifth international conference on security of information and networks* (pp. 67-74).

[7]. Dhage, S. N., Meshram, B. B., Rawat, R., Padawe, S., Paingaokar, M., & Misra, A. (2011, February). Intrusion detection system in cloud computing environment. In *Proceedings of the International Conference & Workshop on Emerging Trends in Technology* (pp. 235-239).

[8]. Prabadevi, B., & Jeyanthi, N. (2014, June). Distributed Denial of service Attacks and its effects on Cloud Environment-a Survey. In *The 2014 International Symposium on Networks, Computers and Communications* (pp. 1-5). IEEE.

[9]. Velliangiri, S., & Premalatha, J. (2019). Intrusion detection of distributed denial of service attack in cloud. *Cluster Computing*, *22*(5), 10615-10623.

[10]. Mayuranathan, M., Murugan, M., & Dhanakoti, V. (2019). Best features based intrusion detection system by RBM model for detecting DDoS in cloud environment. *Journal*

of Ambient Intelligence and Humanized Computing, 1-11.

[11]. Rawashdeh, A., Alkasassbeh, M., & Al-Hawawreh, M. (2018). An anomaly-based approach for DDoS attack detection in cloud environment. *International Journal of Computer Applications in Technology*, *57*(4), 312-324.

[12]. Alzahrani, S., & Hong, L. (2018, July). Detection of distributed denial of service (DDoS) attacks using artificial intelligence on cloud. In *2018 IEEE World Congress on Services (SERVICES)* (pp. 35-36). IEEE.

[13]. Abusitta, A., Bellaiche, M., & Dagenais, M. (2018). An SVM-based framework for detecting DoS attacks in virtualized clouds under changing environment. *Journal of Cloud Computing*, *7*(1), 1-18.

[14]. Nathiya, T., & Suseendran, G. (2018). An Effective Way of Cloud Intrusion Detection System Using Decision tree, Support Vector Machine and Naïve Bayes Algorithm. *International Journal of Recent Technology and Engineering*, *7*, 38-42.