JCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Special Issue-10, May 2019 E-ISSN: 2347-2693

A Detection and Prevention of Ddos Attacks

Anjulee Gupta[1*], **Brajesh Patel**[2]

[1,2]Dept. of Computer Science, Shri Ram Institute of Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Jabalpur, India

DOI: https://doi.org/10.26438/ijcse/v7si10.131134 | Available online at: www.ijcseonline.org

***Abstract*—**Nowadays, cloud computing is very important because of its benefits. But it is also prone to attacks due to vulnerabilities of the websites. DDoS is distributed denial of service where Trojan infected computers are used to target a system to cause traffic jams and genuine users can not able get the service of websites. DDOS affects internet services like e-commerce, e-banking, education, medicine, reservations, agriculture etc. In this way both the end systems are controlled by hackers. There are three categories – volume-based attacks, protocol attacks and application attacks. The companies they are implementing no. of solutions to defend the attacks and continuously updating their techniques but attackers also updating their techniques and methods of attacks. So, in this paper the system is made to collect data online and with the help of association rule mining ddos attack are detected and prevented. Here techniques are used to properly detect attackers and genuine users so that cloud services can be given the users.

***Keywords*—**Component, Formatting, Style, Styling, Insert (key words)

I. INTRODUCTION

Cloud computing is not free from threats still it is used by users and becoming very famous. Nowadays cyber system is very much prone to network attacks done by attackers is affecting all over the world. It is easy to implement but difficult to detect and defence it [1]. A DDoS attack is done through multiple computers to engage the services given by the websites, so that the genuine users cannot able to get the services. Ddos attacks are done through zombies i.e. compromise computers in well organised network can be controlled remotely, so that huge number of fake requests can be sent. This is an abnormal behaviour of receiving requests which can slow down the performance of network and users can not able to get the services of the websites. With passing time attacks are getting sophisticated, complicated and increases its strength. Though there are many solutions, still we must develop the sophisticated tools to detect and prevent these attacks.

The key contributions of this paper are-

1. To understand the source of attacks.
2. To collect all the IP address of the sources.
3. To identify an attack with IP address and block it from sending requests.
4. To protect the system and to provide the services to the legitimate users.
5. To provide smooth working of network with cloud services in near future. [2]

II. EXISTING SYSTEM

The paper says that in 2011, internet security had Trojan threats for online shopping. This attack with the help of computer virus, they able to transfer to android mobile. The author has used –

1. Detection techniques: -
   i) Anomaly detection: -This detection is done on the bases of user's behaviour and system resources. It is only used to detect any attack or intrusion by summarising activity rule. Different kinds are-statistical analysis, Bayesian reasoning, model predictive, data mining and machine learning anomaly detection.
   ii) Misuse detection: - It is to detect ddos attack by using knowledge or pattern matching of requests sent to get services. and normal behaviour of network. It checks the incoming intrusion to the actual behaviour of information database. It is divided into few kinds – expert system, characteristic analysis, conditional probability and keyboard monitoring misuse detection.

2. Data mining techniques: -
   i) Classification analysis algorithm: - in this algorithm comparison done on the bases of data stored and given condition. By auditing data users are determined whether they are legal or not. Then data are instructed to learn the learning to predict unknown data.

ii) Correlation analysis algorithm: -This algorithm is based on relationship between two things. The aim is to search any relations between two data.

iii) Series analysis: - It uses database records in terms of windows. They try to find some sequences with some rules during audit. This helps in choosing effective intrusion detection model [3].

In this paper attack is detected by detection engines, which match the pattern based on some rules. It says that it is better to join data mining than using single method. Data mining with set theory, genetic algorithm, immune algorithm improves universality, real time character and reliability. So, the techniques used are-

1. Improved FP-growth algorithm: - FP growth algorithm uses divide and conquer strategy by divide compressed databases and do mining frequently. In this frequent pattern is produced is called FP-tree. It generates thousands of FP tree and conditional FP tree where top-down and bottom -up navigation is done. In the paper author is using single chain structure of polymeric chain which is unidirectional and each node is pointing towards parent node. It saves time, increases efficiency and growth of pattern pools quickly.
2. FCM network intrusion detection technique based on statistical binning: - FCM is a process based on dividing cluster without instructions. It is time consuming and frequently need to update. So, author has given another model of FCM with statistical binning where cluster division is marked and recorded. According to the binning the clusters are updated and improves the speed of data processing. [4]

Rule mining helps in making decision in selecting crops, resources etc with the help of patterns, associations, correlations, informal structures in a network. Since this can be used in market analysis, fraud detection, customer preservation. So, association mining helps in many business decision making processes. [5]

Here cloud computing is talked about that it has 4 models – private, public, community and hybrid). On these cloud security is very important. So, to secure data from data loss, infected applications and integrity some techniques must be used. To stop hyper jacking on cloud security set is created using encryption and decryption using advanced encryption standards using Rijndael ciphers. Authentication and encryption uses-

1. Authentication using chap: - whenever a client request for a service to the server, then server sends challenge message to the client. Now client acknowledge the message and send it again. The server matches the response value to hash value. If values match, then a service is granted otherwise it is terminated.
2. Encryption using AES-Rijndael Encryption algorithm: - in this algorithm encryption – decryption is used. The data entered in the form of plaintexts and mapped into state bytes. Iterative block ciphers are calculated and round key is also used by 4 iterative rounds.

Simulations are done on Linux platforms –

1. AES encryption: - It is based on dynamic response of stimulus of threat level. This environment is maintained by AEScrypt with C++ libraries. Testing is done by pen testing.
2. Honeyd: - Linux and Java is used to set up the environment at kernel level. ARP spoofing is very important. Two phases are used to tandem for sequential execution and concept of multithreading is used. [6]

In this paper, ddos attack was prevented by machine learning algorithms. Attack was divided into three types-

1. Network based: - It works on network and their hosts in network traffic.
2. Host based: - It checks for abnormal activities on each host.
3. Hybrid based: - It works on host and user properties within network, applications, files and system resources.

Research is done on three phases –

1. Predictions of ML classification algorithms on NSL-KDD dataset comparison: - Data is analysed by two-class classification models which give two values as a output. This algorithm is good to predicts results on basis of dataset.
2. Identified and analysed features in the dataset with greatest predictive power and compared prediction: - In this phase best features are identified. It filters important features to get results fast.
3. Cloud web service suitable for mobile/ desktop/ web application: - Network traffic are checked by web service. For better flexibility, combination of non-supervised learning, k-means clustering is used.

The author says that cloud needs protection in any way. For this deep learning, deep network, data analysis is required. [7]

The author proposed cracking algorithm to prevent ddos attack. Since security is very important in cloud computing. Attack can be done by many ways-

1. Sending unlimited packets to the server.
2. Malwares are used.
3. Application flood.

So, their cracking algorithm have following steps-

1. Packet filter: - It is to transfer of packets from one node to another on internet. If the packet matches it is dropped otherwise it is rejected. During attack packets are dropped due to long delay, client gets service late. In this

system first packet will get delayed and rest will be protected, which will give proper service to the client.

2. Mac generator: - It distinguishes genuine users from attack. It is a systematic process which shares a secret key between two party. Here because of key verification of genuine user and attack are identified. Since attackers does not receive the MAC so it is easy to identify the attackers.
3. IP handler: - Attackers also uses genuine users then the system uses Delicit Round Robin algorithm to collect request. If attackers send request very fast, then it drops excess traffic and IP address are blacklisted.

There is comparison between requested IP with stored IP if it matches then avail services otherwise denial. [8]

Association rule mining used either online data or can use KDDCup99 data set to prevent ddos attack. Attackers send request to the server and when server tries to send request it find no users. Server must wait for timeout or connection to be close. Mean a while attacker send so many requests that server gets filled with bogus request. So, the supermarket uses scanner to collect transactions and collect information so that attacks can be prevented. Weka 3.6.2 version is used to prevent attack with association rule mining. [9]

Since cloud computing depends on demand, resources, services which reduces cost and convenience. So, when software defined network came into market there is a breakthrough in network virtualization and cloud computing. The author worked on: -

1. Virtual resource management technology research based on open stack: - Open stack is an open source technology which provides software to construct and manage private and public cloud. Due to its elasticity, reliability and computing power it is becoming very famous. It is consisting of modules which can manage, store and provide image services.
2. SDN: - It decouples the control plane and the data plane which relies on open flow. With this controller come to know about network and provide flow based table. Due to this services and resources are provided to clients.
3. IDS/IPS: - IDS is a mechanism to provide information of attack but it cannot stop the attack. IPS with the help of IDS and firewall able to detect and stop the attack. Since IPS is connected in series so because of its limited capacity network congestion occurs.

Traditional IPS uses firewall to prevent attack, now SDN uses IPS with controller. So, traditional firewall is expensive compared to SDN. Due to issues like low throughput, low efficiency and high packet loss rate IPS get combined with SDN to provides security to cloud computing. In this paper author, has made cloud platform IPS based on SDN which contains following steps: -

1. The General Scheme Design: - It is consisting of three modules. First is SDN which provides virtual network. Second is open stack which is capable of virtual resource management. Third is interaction which provides the function that prevents intrusion.
2. The design of the interaction module: -This function contains five modules. First when data packets reach switch, it is forwarded to the controller. Second controller distributes the flow table I terms of security. Third packets again reach to the switch is redirected to the flow table. Fourth when the intrusion is detected it is send to the controller’s sink. Fifth message is sent to the security policy and it is distributed the flow table.
3. Comparison of the cloud platform IPS based on SDN and Traditional IPS: - when we compare traditional IPS with IPS with SDN then second is more efficient in terms of test, forwarding single failure, flexibility.

The author has also given scheme verification-

1. Construct of the scheme: - Ryu is made by combining Open stack cloud frame stack with SDN controller to verify scheme.
2. Practicability of the scheme: - This scheme consists of five steps. First construction of 2 virtual machines in open stack. Second new rules are defined. Third new rules are applied. Fourth configuration of security policy. Fifth prevention of intrusion.
3. Evaluation of the system: - The efficiency reaches up to 85%. So, resource utilisation and forwarding rates of IPS based SDN are higher than traditional intrusion prevention system.

This paper concludes that IDS and IPS are both cloud security mechanisms which is based on SDN compared to traditional IPS. [10].

In this author proposed voting done by mobiles. With increase in demand of mobiles there increases the risk of security. Voting by mobile is called M-Voting subset of e-voting. This can be done with the help of cloud computing so intrusion detection system is compulsory to install where database is taken as MySQL. In this paper three detection methods of IDPS are used-

1. Signature detection method: - It is also known as misuse detection method requires large malware signatures database because it is a file dictionary of malware signature.
2. Anomaly based detection: - It is also known as behaviour detection method which analyses the run time behaviour of mobile application and compares it with profiles behaviour to detect attack.
3. Hybrid detection method: - it is a combination of above two method which is used in this paper.

Two classifications of IDS are-

1. An active Intrusion Detection Systems: - It is also known as Intrusion Detection and Prevention system to

block attacks without any intervention of human automatically. It is a real-time response towards attack.

2. A passive Intrusion Detection Systems: - This system cannot able to take any action against attack but only alert an operator about intrusions.

M-voting provide privacy, secrecy and availability to the voter. So, the proposed project provides confidentiality and integrity to voting process. [11]

III. PROBLEM STATEMENT & POSSIBLE SOLUTIONS

The problem statement is to detect and prevent DDoS attacks on the network to provide services to the users. Though there are lots of solution to tackle ddos attacks but still large number of sophisticated tools are coming in the market to implement attacks. So, defence system must be updated time to time to handle the new upcoming attacks.

So, to get a unique and general solutions to overcome this problem, this paper tries to make a system to detect and prevent ddos attacks. Here system is collecting data online and attack is identified per requests send to get a service. By blocking an IP address, we can stop attackers to send fake requests. So, that the legitimate users can get the services required. This is done by the help of association rule mining.

IV. CONCLUSION

The efficiency and accuracy of the network depends on the security of the system. IDS and IPS is the main key of cloud computing security. Association rule mining plays an important role in network security. In this association rule mining is used to detect and prevent ddos attacks to increase the efficiency of network and provides the services to the users.

REFERENCES

[1] Mohd. Azahari Mohd Yusof, Fakariah Hani ali, and Mohd. Yusof Darus. Detection and Defense Algorithms of Different types of DDoS Attack. International Journal of Engineering and Technology, October 2017.

[2] Sunny Behal. Characterization and comparison of DDoS attack tools and traffic generators. International Journal of network security, April 2017.

[3] Zhu Limiao, Haung Hua and Zheng Hao. Research on Intrusion Detection System Model based on data mining. Fourth International Conference on Multimedia Information Networking and security, 2012.

[4]Desheng Fu, Shu Zhou, Phing Guo. The design and implementation of a distributed network intrusion detection system based on data mining. World Congress on software engineering.

[5] Surbhi K. Solanki, Jalpa T. Patel. A survey on association rule mining. Fifth International Conference on Advanced computing & communication technologies.

[6]Nivedha and M. Naveen Nanda, Two layer cloud security set architecture on hypervisor. Second International Conference on Advances in Electronics, Computer and Cmmunications , 2018.

[7]Kemal Hajdarevic, Survey on machine learning algorithms as cloud services for CIDPS, 25th telecommunications forum TELFOR, Serbia, 2017.

[8]V. Priyadharshini and Dr. K.Kuppusamy, Prevention of DDOS attacks using New Cracking Algorithm, International Journal of Enginnering Research and Application, may-june 2012.

[9]Jigang ZHENG and Jingmei ZHANG, Association rule mining in DoS attack detection and defense in the application of network, 5th International Conference on Education, Management, Information and Medicine, 2015.

[10] Yaping Chi, Tingting Jiang, Xiao Li and Cong Gao, Design and implementation of cloud platform intrusion prevention system based on SDN, Department of communication engineering Beijing electronic science and technology institute, 2017.

[11] Dina Moloja and Noluntu Mpekoa, Securing M-voting using cloud Intrusion Detection and Prevention system: A New Dawn, IST, International Information Management Corporation Africa, 2017.

AUTHORS PROFILE

Anjulee Gupta received her BSc(Hons) in Computer Science from Ranchi University, Jharkhand in 2001 and received master degree of computer application from IGNOU in 2005.

She is currently pursuing M.Tech degree in Computer Technology and Application. She has 13 years of teaching experience in different CBSE school. Her current research interest includes detection and prevention of ddos attacks in a network.