An Authentication System for DDoS Attack Detection and Prevention on Cloud Platform

Abhijeetsingh S. Thakur, Dr. Mrs. S. S. Sherekar, Dr. V. M. Thakare

Abstract-**Cloud Computing is an information technology paradigm that enables ubiquitous access to shared pools of configurable system resources and higher level services that can be rapidly provisioned with minimal management effort over the internet. This paper focused on analysis of five different techniques and systems such as CS_DDoS system, DoS attack detection system that uses multivariate correlation analysis, dynamic resource allocation strategy to counter DDoS, FireCol Algorithm and detection using Software – Defined Networking etc. But there are some problems in each method. The problems to overcome are given in analysis and discussion. To overcome these problems, this paper proposes a new DDoS attack detection system model, so as to reduce the rate of DDoS attacks and prevent them. This system also reduces the delay caused while checking and receiving of packets.**

Keywords: Cloud, Cloud Computing, Distributed Denial of Service Attacks, Software - Defined Networking, Dynamic Resource Allocation Strategy.

I. INTRODUCTION

In the recent past, the Information Technology (IT) industry has witnessed a significant growth of cloud computing in hosting and delivering various data-intensive services. Cloud is becoming a dominant computing platform.Researchers have demonstrated that the essential issue of DDoS attack and defence is resource competition between defenders and attackers. This paper focused on five different techniques and systems such as CS_DDoS system [1]; DoS attack detection system that uses multivariate correlation analysis [2], dynamic resource allocation strategy to counter DDoS [3], FireCol Algorithm [4] and detection using Software – Defined Networking [5]. These techniques are used for the detection and prevention of DDoS Attacks. The techniques thus ensure to reduce the attacks to some extent and detect them whenever possible. But there are some problems in this technique.

II. BACKGROUND

Although the number of cloud projects has dramatically increased over the last few years, ensuring the availability and security of project data, services, and resources is still a crucial and challenging research issue. Distributed denial of service (DDoS) attack is the second most prevalent cyber-crime attacks after information theft. Distributed denial of service (DDoS) TCP flood attacks are DoS attacks in which attackers flood a victim machine with packets in order to exhaust its resources or consume bandwidth. The schemes and techniques used for detection and prevention are: CS_DDoS system is proposed that offers a solution to securing stored records by classifying the incoming packets and making a decision based on the classification results [1]. The proposed FireCol system address the problem of DDoS attacks and presents the theoretical foundation, architecture, and algorithms of FireCol [2]. A dynamic resource allocation strategy to counter DDoS attacks against individual cloud customers is proposed. When a DDoS attack occurs, it is employed that the idle resources of the cloud to clone sufficient intrusion prevention servers for the victim in order to quickly filter out attack packets and guarantee the quality of the service for benign users simultaneously[3]. A DoS attack detection system is proposed that uses multivariate correlation. 2 analysis (MCA) for accurate network traffic characterization by extracting the geometrical correlations between network traffic features [4]. The new trends and characteristics of DDoS attacks in cloud computing are discussed, and a comprehensive survey of defence mechanisms against DDoS attacks using SDN is provided [5]. The paper is organized as follows: Section 1 Introduction. Section 2 discusses Background. Section 3 discusses previous work. Section 4 discusses existing methodologies. Section 5 discusses attributes and parameters and how these are affected on mobility models. Section 6 proposed method. Section 7 shows outcome and possible results. Finally Section 8 Conclude this analytical paper.

III. PREVIOUS WORK DONE

Currently, cloud computing is the target business environment for many enterprises and government organizations. However, despite the huge potential gains that can be achieved, security represents a fundamental issue, which prevents them massive cloud adoption in mission – critical Information Technology sectors. Aqeel Sahi et al. (2017) [1] have proposed an efficient DDoS Flood Attack Detection and Prevention System in a Cloud Environment. This system was proposed in order to detect and prevent DDoS attacks in a cloud environment to some extent. Jérôme François et al. (2012) [2] has proposed system called FireCol for the detection of flooding DDoS attacks. The authors address the problem of DDoS attacks and present the theoretical foundation, architecture, and algorithms of FireCol.

Shui Yu et al. (2014) [3] has proposed a system that presents a dynamic resource allocation strategy to counter DDoS attacks against individual cloud customers. A mathematical model is established to approximate the needs of the resource investment based on queuing theory. Z. Tan et al. (2014) [4] proposed a DoS attack detection system that uses multivariate correlation analysis (MCA) for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. Q. Yan et al. (2016) [5] has proposed new trends and characteristics of DDoS attacks in cloud computing are discussed and provided a comprehensive survey of defense mechanisms against DDoS attacks using SDN. In addition, studies about launching DDoS attacks on SDN, as well as the methods against DDoS attacks in SDN are reviewed.

IV. EXISTING METHODOLOGIES

Many techniques and schemes have been implemented over the last several decades. There are different methodologies that are implemented i.e CS_DDoS system; DoS attack detection system that uses multivariate correlation analysis, dynamic resource allocation strategy to counter DDoS, FireCol Algorithm and detection using Software – Defined Networking.

4.1 CS_DDoS system: A CS_DDoS system has been proposed which can prevent DDoS TCP flood attacks. Firstly, it was assumed that the IP addresses of the attackers are not spoofed. This proposed system includes two sub-systems: 1. The detection sub-system.During the detection phase, the detection sub– system collects the incoming packets within a time frame, for example 60 seconds. The collected packets are subjected to a blacklist check to test whether their sources are blacklisted as attackers of the cloud system. 2. The prevention sub-system. When the packets reach the prevention system, they are considered to be attacking packets by the detection subsystem. The prevention sub-system first alerts the system administrator of the attacks. Then, the prevention sub-system will add the attacking source address to the attacker blacklist used by the detection sub-system, if it is not already on the list. Finally, the attacking packet will be dropped. The results show that using LS-SVM the CS_DDoS system can identify the attacks accurately [1].

4.2 FireCol System: FireCol is a new proposed collaborative system that detects flooding DDoS attacks as far as possible from the victim host and as close as possible to the attack source(s) at the Internet service provider (ISP) level. FireCol relies on a distributed architecture composed of multiple IPSs 3 forming overlay networks of protection rings around subscribed customers. FireCol is designed in a way that makes it a service to which customers can subscribe. Participating IPSs along the path to a subscribed customer collaborate (vertical communication) by computing and exchanging belief scores on potential attacks. The system works on the principle of collaborating routers and due to which there is time delay for the detection of attacks [2].

4.3 Dynamic Resource Allocation Strategy: A mechanism is proposed to dynamically allocate extra resources to an individual cloud hosted server when it is under DDoS attack. First of all, the features of a cloud hosted virtual server in a non-attack scenario are examined. The IPS is used to protect the specific server of the hosted service. All packets of benign users go through the queue, pass the IPS and are served by the server. From results it is possible to beat DDoS Attacks [3].

4.4 DoS attack detection system that uses multivariate correlation analysis: The whole detection process consists of three major steps. The sample-by-sample detection mechanism is involved in the whole detection phase. In Step 1, basic features are generated from ingress network traffic to the internal network where protected servers reside in and are used to form traffic records for a well-defined time interval. In Step 2 is multivariate correlation analysis, in which the "triangle area map generation" module is applied to extract the correlations between two distinct features within each traffic record coming from the first step or the traffic record normalized by the "feature normalization" module in this step. In Step 3, the anomaly based detection mechanism is adopted in decision making. It facilitates the detection of any DoS attacks without requiring any attack relevant knowledge. The proposed detection system achieves encouraging performance in most of the cases except Land attack [4].

4.5 Detection using Software Defined Networking: SDN itself may be a target of DDoS attacks. Since SDN I s vertically split into three main functional layers, including infrastructure layer, control layer, and application layer, potential malicious DDoS attacks can be launched on these three layers of SDN's architecture. Based on the possible targets, the DDoS attacks launching on SDN are classified into three categories: application layer DDoS attacks, control layer DDoS attacks, and infrastructure layer DDoS attacks [5].

V.ANALYSIS AND DISCUSSION

The performance of the CS_DDoS method is evaluated using the four classifiers of the LS-SVM, naive Bayes, k- earest, and multilayer perceptron. The results show that using LS-SVM the CS_DDoS system can identify the attacks accurately. The system has an accuracy of about 97 percent with a Kappa coefficient of about 0.89 when under single attack [1]. The objective of the experiments is to evaluate the accuracy of FireCol in different configurations. Furthermore, the robustness of FireCol is evaluated in abnormal situations such as the existence of non-cooperative routers or configuration errors. Firecol proves to be effective in simulation based approach [2]. The performance of the proposed dynamic resource allocation method is evaluated for DDoS mitigation in a cloud from various perspectives. It is evaluated that it is possible to beat DDoS Attacks [3]. The proposed detection system achieves encouraging performance in most of the cases except Land attack [4]. A mechanism named Virtual source Address Validation Edge (VAVE) is proposed to improve the SAVI solution. VAVE employs OpenFlow protocol to solve source address validation problem with a global view. OpenFlow devices are used to form a protective perimeter [5].

Proposed scheme and techniques	Advantages	Disadvantages
CS_DDoS system	The proposed approach can efficiently improve the security of records, reduce bandwidth consumption and mitigate the exhaustion of resources.	This cloud project is vulnerable to certain other types of attacks.
FireCol System	FireCol also helps in detecting other flooding scenarios, such as flash crowds, and for botnet-based DDoS attacks.	This system is vulnerable to certain other types of attacks.
Dynamic Resource Allocation Strategy.	The system is able to beat DDoS attacks.	This system is vulnerable to certain other types of attacks.
DoS attack detection system that uses multivariate correlation analysis .	The system is able to distinguish both known and unknown DoS attacks from legitimate network traffic.	The detection system suffers serious degeneration in the cases of the Teardrop and Neptune attacks.
Detection using Software Defined Networking	1) Separation of the control plane from the data plane. 2) A logical centralized controller and view of the network.	Performance degrades as the current controllers cannot handle a big number of flows.

TABLE 1: Comparisons between different schemes.

VI. PROPOSED METHODOLOGY

Although the number of cloud projects has dramatically increased over the last few years, ensuring the availability and security of project data, services, and resources is still a crucial and challenging research issue. Distributed denials of service (DDoS) attacks are the second most prevalent cyber-crime attacks after information theft. DDoS TCP flood attacks can exhaust the cloud's resources, consume most of its bandwidth, and damage an entire cloud project within a short period of time. In this paper, a DDoS attack prevention system is proposed so as to reduce the risk for DDoS attacks and prevent them. The model consists of Clients, Handler, Agent and other fields for the defense mechanism of the attacks. The client is where the attacker communicates with the rest of the DDoS attack system. The handlers are software packages located throughout the Internet that the attacker's client uses to communicate with the agents. The agent software exists in compromised systems that will eventually carry out the attack.The packets are received sent from the clients. The incoming packets may contain some vulnerability or the harmful packets form the attackers. The incoming packets are checked for vulnerability and then forwarded accordingly. If the packets contain no vulnerability, the packets are forwarded to the packet destination and then stored for future use. If the packet contains some vulnerability the packets are forwarded to the handler. Afterwards, the packets are transferred to the agent where the agent will try to reduce the vulnerabilities involved in the packet. If the vulnerabilities are reduced or removed the 5 packet is again checked and then forwarded to packet destination. If the packets again contain some vulnerability the packets are forwarded to the victim. This system reduces the rate of DDoS attacks and also prevents them to some extent. Basic steps of algorithm:

Step 1: Packet source receives the incoming packets.

Step 2: The incoming packets are detected and checked for any vulnerabilities.

Step 3: If there are no vulnerabilities in the packet the packets are forwarded to the packet destination. The packets are then stored for future use.

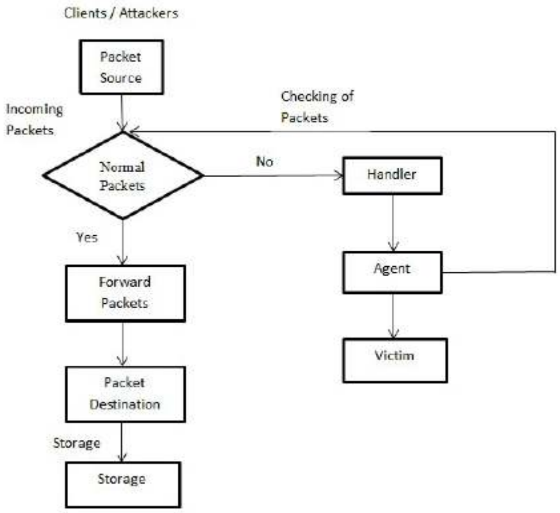
Step 4: If there are any vulnerabilities in the packet, the packets are transferred to the handler for further processing.

Step 5: After processing the packets are forwarded to the agent where the vulnerabilities are removed.

Step 6: The packets are again transferred for checking for vulnerabilities.

Step 7: If there are no vulnerabilities, Step 3 is repeated

Else the packets are sent back to Victim. Diagrammatic representation of proposed method is shown as follows:



VII. OUTCOME AND POSSIBLE RESULTS

DDoS attacks make a networked system or service unavailable to legitimate users. These attacks are an annoyance at a minimum, or can be seriously damaging if a critical system is a primary victim. This system is proposed to prevent the DDoS attack. This System also reduces the delay occurred while the packets are being checked for vulnerabilities.

VIII. CONCLUSION

This paper focused on five different techniques and systems such as CS_DDoS system, DoS attackdetection system that uses multivariate correlation analysis, dynamic resource allocation strategy to counter DDoS, FireCol Algorithm and detection using Software – Defined Networking. But there are some problems in each method so to overcome the problems that are given in analysis and discussion, a new DDoS attack detection system model is proposed so as to reduce the rate of DDos attacks and prevent them. This system also reduces the delay caused while checking and receiving of packets.

IX. FUTURE SCOPE

From observations of the proposed method the future work will include the implementation of the prevention model and to prevent DDoS attacks from occurring in a cloud environment.

REFERENCES

1. Aqeel Sahi, David Lai, Yan Li, and Mohammed Diykh, "An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment", ACCESS.2017.2688460.
2. Jérôme François, IssamAib, and Raouf Boutaba, "FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 20, NO. 6, DECEMBER 2012
3. Shui Yu, IEEE, Yonghong Tian, Song Guo, and Dapeng Oliver Wu, "Can We Beat DDoS Attacks in Clouds?", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 9, SEPTEMBER 2014.
4. Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Priyadarsi Nanda, and Ren Ping Liu, "A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014.
5. Qiao Yan, F. Richard Yu, Qingxiang Gong, and JianqiangLi, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 18, NO.1, FIRSTQUARTER 2016.