IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 21-24

Designing the Authentication System for DDoS Attack Detection and Prevention on Cloud Platform.

Abhijeetsingh S. Thakur[1], Dr. Mrs. S. S. Sherekar[2], Dr. V. M. Thakare[3]
Student in Department of Computer Science S.G.B.A.U., Amravati, Professor in Department of Computer Science, S.G.B.A.U., Amravati, Head of Department of Computer Science, S.G.B.A.U., Amravati.

Abstract: *Cloud Computing provides easy access to the end users i.e. users can access the services easily from wherever they want to without the concern about the storage, management, and cost and so on. As the numbers of users per day are increasing, threats for protecting the data residing in the Cloud is also increasing. This paper is focused on analysis of five different techniques and systems such as SD-IoT Framework, Low Rate Strategy, Three Tier Network Architecture, Network Simulation Strategy and Survey of Defense Mechanisms etc. But there are some problems that are present 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.*

Keywords: *Cloud Computing, Distributed Denial of Service attack, Security, Defense, SDN.*

I. Introduction

A computing paradigm with virtual network of remote servers allowing users to store, process and access data, providing on-demand computational services with features like elasticity, scalability, security and redundancy is **Cloud computing**. 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 allows the users to easily access the cloud services from wherever they want to. This paper focused on five different techniques and systems such as SD-IoT Framework [1], Low Rate Strategy [2], Three Tier Network Architecture [3], Network Simulation Strategy [4] and Survey of Defense Mechanisms [5]. These techniques are used for the detection and prevention of DDoS Attacks. The techniques are helpful to detect and prevent the DDoS Attacks. But there are some problems in this technique.

This paper presents a DDoS Attack Detection and Prevention technique which helps to solve the problems of DDoS attacks. This methods works on the principle of threshold value. During a DDoS attack the packets are transferred continuously from the client to the server/cloud for the system to crash. A threshold value is set which is responsible for the detection and prevention of DDoS attacks. The number of packets upon crossing the given specified threshold value results in DDoS attack Detection. After the DDoS attack is detected the client is blocked from sending the packets onto the server. This proposed method works efficiently in order to detect and prevent DDoS attacks. The DDoS attacks are prevented in this method as well as the IP address of the Client is blocked so as to avoid further problems.

II. Background

Cloud computing has emerged as a hotspot in both academics and industry due to its essential characteristics, such as an on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Currently, security issues have been regarded as the dominant barrier in development of cloud computing. The schemes and techniques used for detection and prevention are:

SD – IOT Framework proposed an algorithm for the detection and mitigation of the DDoS attacks using the proposed SD-IoT framework, and in the proposed algorithm, the cosine similarity of the vectors of packet-in message rate at the boundary SD-IoT switch ports is used to determine whether DDoS attacks occur in the IoT. [1]. The proposed Low Rate Strategy presents some strategies exploiting the cloud flexibility in order to increase in a fraudulent way the overall energy consumption and analyze their impact within large-scale cloud infrastructures [2]. Three Tier Network Architecture proposes use of multi-tiered network design based on Hybrid cloud solution comprising of an On-premise solution as well as a public cloud infrastructure capable of handling hurricane sized DDoS storms [3]. This paper includes a network simulation to study the feasibility of such an attack motivated by our experiences of such a security incident in a real data center [4]. The scope of the DDoS flooding attack problem and attempts to combat it are explored in this paper [5].

The paper is organized as follows: **Section I** Introduction. **Section II** discusses Background. **Section III** discusses previous work. **Section IV** discusses existing methodologies. **Section V** discusses attributes and parameters and how these are affected on mobility models. **Section VI** proposed method and outcome of result. Finally **Section VII** conclude this analytical paper.

III. Previous Work Done

Currently, cloud computing is the highly used environment for many enterprises and government organizations. However, despite the huge potential gains that can be achieved, there are many security threats which are responsible for the breakdown of services of cloud .

Da Yin et al. (2018) [1] has projected an algorithm for detection and mitigation of DDoS attacks using the proposed SD-IoT framework, and in the proposed algorithm, the cosine similarity of the vectors of the packet-in message rate at the boundary of SD-IoT switch ports is used to determine whether the DDoS attack occurs in the IoT.

Massimo Ficco et al. (2017) [2] has presented some strategies exploiting the cloud flexibility in order to increase in a fraudulent way the overall energy consumption and analyze their impact within large-scale cloud infrastructures.

Akashdeep Bhardwaj et al. (2016) [3] proposes the use of multi-tiered network designs based on the Hybrid cloud solution comprising of an On-premise solution as well as a public cloud infrastructure capable of handling hurricane sized DDoS storms.

Zahid Anwar et al. (2014) [4] included a network simulation to study the feasibility of such an attack motivated your experiences of such a security incident in a real data center.

Saman Taghavi Zargar et al. (2013) [5] has explored the scope of the DDoS flooding attack problem and attempts to combat it.

IV. Existing Methodologies

Many techniques and schemes have been implemented over the last several decades. There are different methodologies that are implemented i.e as SD-IoT Framework, Low Rate Strategy, Three Tier Network Architecture, Network Simulation Strategy and Survey of Defense Mechanisms.

SD-IOT Framework: In this paper, the authors first presented a general framework for software-defined Internet of Things (SD-IoT) based on the SDx paradigm. The proposed framework consistd of a controller pool which contains the SD-IoT controllers, SD-IoT switches integrated with an IoT gateway, and IoT devices. The authors then proposed an algorithm for detecting and mitigating DDoS attacks using the proposed SD-IoT framework, and in the proposed algorithm, the cosine similarity of the vectors of the packet-in message rate at the boundary on SD-IoT switch ports is used to determine whether DDoS attack occurs in the IoT. Finally, experimental results show that the proposed algorithm has good performance, and the proposed framework adapts to strengthen the security of the IoT with heterogeneous and vulnerable devices [1].

Low Rate Strategy: The proposed work presents a detailed analysis of new sophisticated menaces, by focusing on those that are specifically tailored to originate the worst-case energy demands by leveraging properly crafted low-rate traffic patterns in order to ensure the stealth operations. The authors presented some strategies exploiting the cloud flexibility in order to increase in a fraudulent way the overall energy consumption and analyze their impact within large-scale cloud infrastructures. This should help the cloud providers in understanding the weaknesses and highlighting their root causes, as well as in providing some hints on how they can counter the subtle security issues [2].

Three Tier Network Architecture: This paper proposes use of multi-tiered network design based on Hybrid cloud solution comprising of an On-premise solution as well as a public cloud infrastructure capable of handling hurricane sized DDoS storms. By providing the increased layers of the network and web application security in the form of separate tiers, it is possible to protect the integrity, availability and performance of critical web applications, resulting in improved brand and customer confidence and reduced business risk from under-provisioning security devices [3].

Network Simulation Strategy: Recently, Cloud providers have experienced outages due to HVAC malfunctions. The contributions include a network simulation to study the feasibility of such an attack motivated by the past experiences of such a security incident in a real data center. It demonstrates how a network simulator can study the interplay of communication and thermal properties of a network and help prevent the Cloud provider’s worst nightmare: meltdown of the data center as a result of a DDoS attack [4].

Survey of Defense Mechanisms: The authorsexplored the scope of the DDoS flooding attack problem and attempts to combat it. The authors categorized the DDoS flooding attacks and classified the existing countermeasures supported wherever and when they prevent, detect, and respond to the DDoS flooding attacks. Moreover, the authors highlighted the need for a comprehensive distributed and collaborative defense approach [5].

V. Analysis And Discussion

A detailed appraisal of the major requirements of efficient DDoS mitigation solutions and the factors governing these requirements is provided. A general framework for SD-IoT composed of an SD-IoT controller pool with controllers, SD-IoT switches integrated with the IoT gateway, and terminal IoT devices is proposed. The simulation results show that the proposed algorithm can find the IoT device from which a DDoS attack is launched within a shorter time period, quickly handle and mitigate the DDoS attack, and ultimately improve the unveiled glaring vulnerabilities [1]. This work has presented a new generation of menaces, which exploit the cloud flexibility in order to inflict additional operational costs to cloud service providers. These techniques must be able to effectively recognize and isolate malicious service requests from the legitimate traffic, by using a comprehensive security solution that considers energy-related aspects as a fundamental part of its monitoring focus [2]. By providing the increased layers of network and web application security in form of separate tiers, it is possible to protect the integrity, availability and the performance of critical web applications, resulting in improved brand and customer confidence and reduced business risk from under-provisioning security devices [3]. This includes a network simulation to study the feasibility of such an attack motivated by our experiences of such a security incident in a real data center. It demonstrates how the network simulator could study the interplay of communication and thermal properties of a network and facilitate prevent the Cloud provider’s worst nightmare: meltdown of the data center as a result of a DDoS attack [5].

Table 1 : Comparisons between different schemes.

Proposed scheme and techniques	**Advantages**	**Disadvantages**
SD – IOT Framework	The proposed algorithm has good performance, and the proposed framework adapts to strengthen the security of the IoT with heterogeneous and vulnerable devices.	The Proposed System is difficult to Implement.
Low Rate Strategy	These strategies helps to counter DDoS Attacks.	The accuracy of the system is not known.
Three Tier Network Architecture	It is possible to protect the integrity, availability and performance of critical web applications.	The cost associated with the system implementation is higher.
Network Simulation Strategy	This paper demonstrates how a network simulator can study the interplay of the communication and thermal properties of a network and help prevent the Meltdown of data centre.	It is not practical to place the HVAC (a mechanical system) on UPS(s) because of its dynamics network
Survey of Defense Mechanisms	The scope of the DDoS flooding attack problem and attempts to combat it is explored	This system has not been implemented yet.

VI. Proposed Methodology

The use of cloud projects has been increasing day by day. It is easier for the users to use cloud for their day to day use. Thus everyone is using it as a daily purpose. But it is also easy for the attackers to disrupt the service of the cloud as it is available to everyone for using it. The attackers can flood the cloud and stop the service provided by it. So it is an important task to detect the attacks and prevent them. In this proposed method an open source tool named “Wireshark” is used. Wireshark is a free and open-source packet analyzer. It is used as a network troubleshooting tool, analysis, software and communications protocol development, and education. This tool captures the packet and analyses it and by the pattern detection of the packets. This tool is responsible for the analysis of the packets and detecting the attacks.

Basic steps of algorithm:

Step 1: Packet source receives the incoming packets.

Step 2: The packets are analyzed through the Wireshark tool.

Step 3: During the DDoS attack, many number of packets are transferred in the cloud. If the numbers of packets are in limit the packets are stored.

Step 4: If the number of packets passes the threshold value the DDoS attack is detected and then prevents it. It discards the packets and the attack is prevented.

Step 5: If the packets are normal then the packets are stored and if it passes the threshold value the packets are sent to the Handler where they are discarded.

Diagrammatic representation of proposed method is shown as follows:

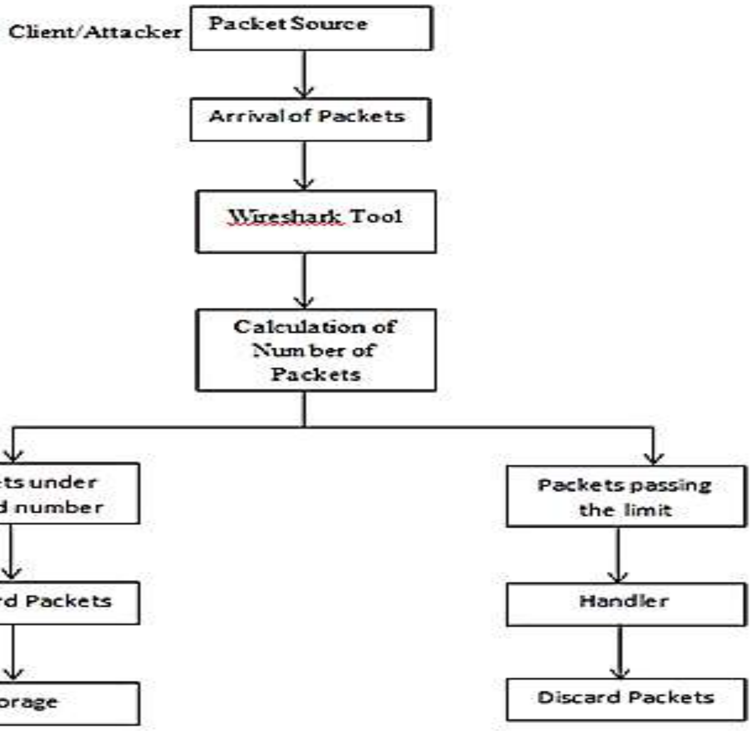

Figure: *Data flow diagram of detection system*

VII. Outcome And Possible Results

DDoS attacks causes the breakage of the services provided by the cloud. This attacks can result into the damage to the user data. This proposed system is proposed to stop this DDoS attacks. This system promises to stop the DDoS attacks and continue the services provided by the cloud. The proposed system also blocks the IP address of the Client / Attacker from further causing the disturbances in the system.

VIII. Conclusion

This paper is focused on analysis of five different techniques and systems such as SD-IoT Framework, Low Rate Strategy, Three Tier Network Architecture, Network Simulation Strategy and Survey of Defense Mechanisms 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 proposed system not only detects DDoS attacks but also blocks the Client’s IP from causing further problems.

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. The Future work will also include the improvement of the system thus making the system better.

References

[1]. Da Min, Lianming Zhang, Kun Yang, “A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework”, IEEE Access, April 2018.

[2]. Massimo Ficco and FrancescoPalmieri, “Introducing Fraudulent Energy Consumption in Cloud Infrastructures: A New Generation of Denial-of-Service Attacks”, IEEE, June 2017.

[3]. Akashdeep Bhardwaj, GVB Subrahmanyam, Vinay Avasthi, Hanumat Sastry, “Three Tier Network Architecture to Mitigate DDoS Attacks on Hybrid Cloud Environments”, ACM, March, 2016.

[4]. Zahid Anwar and Asad Waqar Malik, “Can a DDoS Attack Meltdown My Data Center? A Simulation Study July 2014.

[5]. Saman Taghavi Zargar, James Joshi, David Tipper, “A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks”, IEEE COMMUNICATIONS SURVEYS & TUTORIALS 2013.