Software-Defined Networking (SDN) based cloud without dementia of Distributed Denial of Service attack (DDoS)

Akash Bandi[1], Prajakta Donde[2], Kanchan Bhagwat[3], Swapnil Umap[4],

S A Agrawal[5]

[1234]*Student, Dept of Computer, MMIT, Maharashtra, India*

[5]*Professor, Dept of Computer, MMIT, Maharashtra, India*

Abstract

Networking and security consists of the policies and practices adopted to prevent and monitor unauthorized access, denial of a services and network-accessible resources .Distributed Denial-of-Service (DDoS) is an attack where two or more attack source make machine unavailable to user such as to interrupt the service of connected internet .DDoS attack on cloud had been double folded in last decade. DDoS attacks on cloud computing have increased a lot due to its crucial characteristics .Software Defined Networks(SDN) based cloud leads us to new opportunities to defend DDoS attacks on cloud. It is easy to detect and react to DDoS attack using SDN, because of its various potentials such as software based traffic analysis, central control, global view control and dynamic updating of forwarding rules .In this system, the traffic analysis will be conducted by Networked based mechanism using SDN .In which six tuples will be monitored so as to distinguish between intruders and legitimate traffic. We will also prevent SDN from becoming a victim to DDoS attacks.

***Key Words*:** *Software Defined Network (SDN) , Distributed Denial of Services(DDoS), Cloud Computing Web Crawler(WC) , Information extraction(IE), Named Defined Network(NDN)*

1. INTRODUCTION

Now a days, use of cloud is growing all over the world. Cloud computing is a type of Internet-based computing that contributes shared computer processing resources and data to computers and other devices when requisite. Cloud provide users with various capabilities to store and process their data in third-party that may be located far from the user–ranging in distance from across the world. Due to increase of the sharing of data from one user/group to other user/group through network there is also possibility of increasing in attacks on the data accessed by the intruders on clouds. Due to this, users are facing some problems in terms of different network attacks such as DDoS, X-DoS,H-DoS etc. *Denial of Service* (DoS) attacks and *Distributed Denial of Service* (DDoS) flooding attacks are the main methods to destroy availability of cloud computing. DoS attacks or DDoS attacks are an attempt to make a machine or network resource unavailable to its intended users. DDoS attacks are sent by two or more persons, or bots, while DoS attacks are sent by one person or system. The rate of DDoS attack in past decade have been double folded. Hence to defeat this DDoS and maintain the traffic SDN had been introduced. SDN is currently attracting significant attention from both academia and industry. So by calculating the tuples we are going to defeat the DDoS attack and control the traffic.

2. RELATED WORK

The access point which is an Open Flow-enabled switch and is controlled by an Open Flow controller, detects mobile malware through real time [2]. VAVE that employs Open Flow protocol to solve source address validation problem with a global view is proposed to improve the SAVI
solution.[1]. An agent based framework, AgNOS for the building of cooperative SDNs that extend their domains beyond enterprise networks is presented, which is built on top of the abstractions provided by SDN [3]. It theoretically analyzes the quantitative relation among the probability that a flow is successfully imprinted back various ASlevel hop number, independently sampling probability, and the packet number that the attacking flow comprises [5]. It comprises receiving a DDoS attack indication performed against at least one destination server; programming each network element in
SDN to forward a packet based on a diversion value designated in a packet diversion field, upon reception of the DDoS at indication [4].

3. SYSTEM ARCHITECTURE

In this system we are developing a banking application which will be able of detecting and defending DDoS attack using SDN.
The system architecture is divided into three modules given as follows:-
1. CLIENT:-
Banking Application.

User can do online transactions-.Bill Payments (electricity bill, income tax, mobile recharge), Fund transfer. Application will be host on cloud which have implemented SDN. Our system will prevent following DDoS types of attacks: SQL injection, Brute force attack,URL injection and Cross site Scripting attack. Personal information of customer gets stored into the database in the encrypted format.
Dynamic password, PIN generation and sending it to user on his mail. After every transaction User will get notification by message. User can see his account details and Mini statement.
2. SERVER:-
Approve or reject application on the basis of tuples. Checking the validity of tuple. If yes, search customer by account number or customer name. Check the logs of attacks.

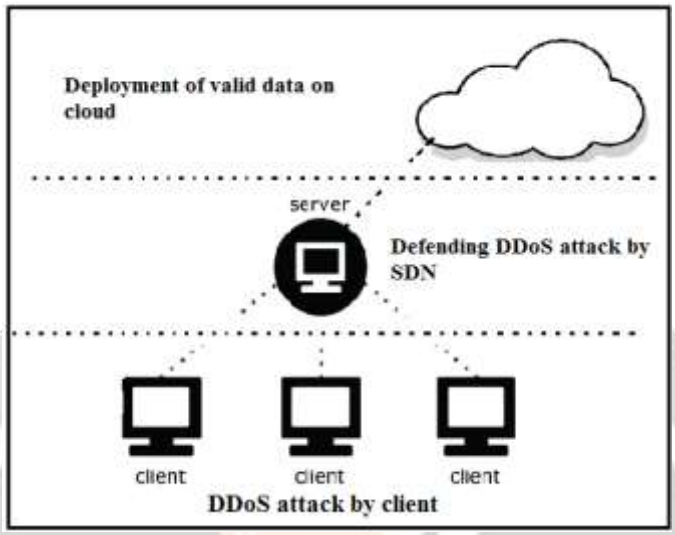

fig 1: System Architecture

3. CLOUD:-

Creating cloud instance of OS. Authentiation of all credentials which will be provided from cloud service provider. Accessing the instance that we have created.After you have installed XL Deploy, log in to XL Deploy and follow these instructions to: Connect XL Deploy to your IBM WebSphere Application Server (WAS) Network Deployment (ND) or Base installation.
Create an environment where you can deploy applications.Installation of softwares (Database, Tomcat).Import a Project application into XL Deploy.Deploy the Project application to the environment that you created.Acceses the data using web services.

4. MATHEMATICAL MODEL

- S={X,F,T,R,Y}
- S (system) =Proposed system.
- X(input to system)=Input Query
- F(main algorithm)=Contains process T
- SOM method is used to calculate 4 tuples by the following equation $Wv(s+1) = Wv(s) + \theta(u,v,s) \cdot \alpha(s) \cdot (D(t) - Wv(s))$
- D(t) = target input data vector $\theta(u,v,s)$ = restraint due to distance from BMU,usually called the neighbourhood function
- Wv = current weight vector of nodeT(types of tuples)Where T = {t1,t2,t3,t4}(t1 = average of packets perflow,t2 = average of bytes perflow,t3 =
  Average of duration per flow, t4 = percentage pair flow)
- R=Set threshold value by average of daily transaction.
- If R>T then legitimate URL.
- If R< then intruders URL.

5. ALGORITHM TO BE USED:

Network-Based Mechanisms Using SDN: A lightweight
Method for DDoS attacks detection based on traffic flow
features is presented in which the extraction of such information is made with a very low overhead compared to traditional approaches. The method is divided into three modules
1) The Flow Collector module is responsible for periodically Requesting flow entries from all Flow Tables of OF
Switches.
2) The Feature Extractor module receives the collected Flows, extracts features that are important to DDoS flooding 0Attack detection. These important features include:
Average of Packets per flow (APf), Average of Bytes per flow (ABf), Average of Duration per flow (ADf), And percentage pair flow (APf). The Feature Extractor0 module gathers them in tuples to be passed to
The classifier.
3) The Classifier module analyzes whether or not a given Tuple corresponds to a DDoS flooding attack or to legitimate
Traffic. Self-Organizing Maps (SOMs) are used as the classification method.

6. CONCLUSIONS

We can conclude inferring that the proposed system is practically feasible model and gives a much improved result with better performance.

7. ADVANTAGES

1. Strong security against malicious attacks.
2. Control traffic.
3. Mitigation of DDoS is achieved.

8. ACKNOWLEDGEMENT

We express our sincere thanks to Head of Department of Computer Engineering for her kind co-operation. We express our sincere thanks to Prof. S. A. Agrawal.

9. REFERENCES

1. G. Yao, J. Bi, and P. Xiao, Source address validation solution with openflow/ NOx architecture, in Proc. 19th IEEE ICNP, 2011.

2. R. Jin and B. Wang, Malware detection for mobile devices using software defined Networking, in Proc. IEEE 2nd GREE Workshop, 2013.

3. A. Passito, E. Mota, R. Bennesby, and P. Fonseca, AgNOS: A framework For autonomous control of software-defined networks, in Proc. 28th IEEE Int. Conf. AINA, 2014.

4. H. Tian and J. Bi, An incrementally deployable flow-based scheme for IP Trace back, IEEE Commun. Lett. vol. 16, no. 7, pp. 11401143,Jul. 2012.

5. A. Chesla and E. Doron, Techniques for traffic diversion in software defined Networks for mitigating denial of service attacks, U.S. Patent App. 13/913916, Jun. 10, 2013.