SECURITY SOLUTION FOR SDN USING HOST-BASED IDSs OVER DDoS ATTACK

M. JANAT VINNARASI
M.Phil Research Scholar,
janetvino@gmail.com
Bishop Appasamy College of Arts and Science, Coimbatore
Bharathiar University, Coimbatore, Tamil Nadu, India.

Dr. N. SUDHA
Associate Professor, Department of Computer Science,
Bishop Appasamy College of Arts and Science, Coimbatore
Bharathiar University, Coimbatore, Tamil Nadu, India.

Abstract: Many security issues were providing problematic thing for the data user. Amid various security issues SDN faces big obstacles threats were at the data plane and the application plane. These were controlled by the network provider or operator and also ASPs (Application Service Providers) was suggested by many researchers. Hence, superior attention is essential for the SDN control plane security attacks, particularly the Denial of Service (DoS) attack. Similarly, there are numerous non-recognizable attacks that have been provided against the Cloud environment that were faced by the cloud user. One such vulnerable attack is the Distributed DoS (DDoS) attack. DDoS attacks can occur when numerous compromised systems overflow the bandwidth to a targeted system with spoofed source IP addresses. The purpose of DDoS attack is to produce the network and application resources unreachable to the authorized users for some period of time. To overcome the DoS attack in SDC, we proposed the host-based IDSs (HBIDS), it having the capacity to monitor local events of a host, can notice attacks that cannot be realized by a NIDS. The host-based IDSs can do analyze the encrypted information and also used Signature based detection approach.

Keywords: SDN, Security issues, DDoS Attack and Host-based IDS
I. INTRODUCTION

Software-defined networking (SDN) architecture provides to the networks in easy and flexible manner. SDNs network is fully different from the traditional networks, here the key principle of interruption network policies totally from network operations. SDN worldview presents a concentrated and programmable method for planning systems and was intended to confront the inadequacies of customary systems, for example, manual design and upkeep of each gadget in the system, high inertia in way recuperation because of appropriated approach, and so on [1]. The SDN aims to improve the progress of network control, for that it allowing enterprises and service providers to answer quickly to varying business necessities. An important representative of the SDN architecture is the physical partition of the control plane from the forwarding plane. A sensibly centralized control function preserves the state of the network and delivers directions to the data plane. The data plane of network devices has sent the data packets based on the control instructions. Though this architectural move has increased significant attention from both the hypothetical and network trade, the idea of partition control and data plane functionality has been about for much lengthier [2]. SDN is one of the greatest inventive network technologies, makes security discovery and prevention more alert and dynamical in answering malicious actions. While security issues in SDN that were at the data plane and the application plane and it is manageable by the network operator and the Application Service Providers (ASPs) and it is programmable through APIs (Application Programming Interfaces). Actually, well-defined APIs among the planes are the pointer of a good SDN as they are divided the data plane and application plane. OpenFlow is one example of such API. While this process the security attack will happens in many networks. Hence DoS (Denial of Service) attack is one of the main security issues in SDN and also many attacks was not identified in Cloud environment. Cloud computing refers the use of computing resources like hardware and software which can be delivered as a service over a network. It is a solution for providing on-demand access to computing infrastructure. End users can visit cloud-based applications by web browser, lightweight desktop, mobile devices at a remote area while client’s information, data and computing resources are stored in cloud. It has been broadly deployed today that the requesting asset provisioning abilities [3]. Hence, security has been one of the top issues in cloud network while cloud resource misuse and malicious insiders are considered as top issues. With recent progress in software-defined networking (SDN), SDN-based cloud brings us new opportunities to crush DDoS attacks in cloud computing environments.

Distributed Denial of Services (DDoS) attacks is one of well-known and dangerous threats to the present system which consistently exists and advances based with the improvement of the network itself. DDoS make an online service become inaccessible by sending a mind-boggling number and size of fake packets from different sources is one of characteristic for DDoS attacks. Early DoS attack focused on the single victim with only source attacker. After some time, it changed to single or multiple victims against single or multiple sources. Security isn’t the main concentration in the design and improvement of the internet/network today [4]. Most research and flow focus around the best approach to sending information from source to destination in successful manner despite the fact that the protocol absence of security worked to isolate the malicious purpose. For e.g., TCP protocol won’t venture in and stop the source to send a malicious purpose that can hurt the destination have the traffic does not exist for this protocol [5, 6]. This security issues can be misused for DDoS attacks. Indeed, even now the DDoS attack is easy but difficult to execute even can be propelled with a large network against a huge system which called "asymmetric attack". Current system has entered the Software Defined Networking era which offers unified control and programmability network by decoupling the system control and data plane that expedite us a dynamic, cost-effective, sensible and agile stage. On the drawback, this centralized area can bring new security difficulties, for example, DDoS attacks on the central controller which could concession the whole network. This paper is organized as follows. Section 1 shows the introduction of SDN and DDoS mechanisms, section 2 describes the review of literature or related work about this concept by various existing authors work, section 3 describes about existing work and problem statement, section 4 describe about proposed method, section 5 shows the result of our system, section 6 contains the conclusion of this paper.

II. LITERATURE REVIEW

Jeanette Smith-Perrone et al [7] investigate the Distributed refusal of-administration (DDoS) and the digital danger scene is developing quicker than customary IPS/IDS arrangements can oversee utilizing known attack marks. The size, degree and varieties of the attacks would now be able to overpower huge venture conditions and reduce asset accessibility for internet

©IJETIE 2019
business, cloud, facilitating and transporter stages. This paper gives a review of the issue of Distributed Denial of Service (DDoS) attack, current alleviation process and proposed computerization for recognizable proof and exact moderation. In this paper, we present an accessible instrument for anticipating DDoS attacks without human intercession to relieve 0-day attacks. This paper gives a comprehension of the DDoS issue confronting cloud, SDN, and huge venture systems.

Tasnim Tamanna et al [8], find the Software Defined Networking has become a drone word to service and cloud providers since when they feel the need to make the network programmable. As the devices in data center and applications continue to rise in number, the need for bandwidth, storage and computing power grows substantially. This infrastructure needs to be managed, maintained, updated, powered and cooled. As a result, the traditional data center model is becoming too costly and complex to sustain. Also, security threats are growing significantly. Distributed Denial Service of Attacks (DDoS) is one of those vital security threats. With the progression of Software Defined Networking (SDN), protection mechanisms against DDoS attack has unlocked a new door to cloud computing environment. Based over SDN, new infrastructure of cloud computing has brought novel possibilities to defense against DDoS attacks. In this paper, we are going to discuss on some of the valuable features of SDN and show we can make full use of SDN's assets and advantages to make cloud highly competent and secured against all threats. The research results in this paper can be expanded to prepare a new architecture of SDN enabled secured IoT based cloud environment.

Kriti Bhushan et al [9], find the last one decade, cloud computing has evolved as a new and promising computational platform that provides cost effective and scalable computing facility. The merger of SDN technology with the cloud computing environment simplifies the cloud's networking complexities and significantly improves the manageability, programmability, dynamism, and scalability of the cloud. In the SDN-based cloud, the fundamental highlights of SDN, including worldwide perspective all in all system, software-based traffic investigation, unified authority over the system, and so on enormously improves the DDoS attack recognition and alleviation capacities of the cloud. In this paper, we initially examine about different fundamental highlights of SDN that makes it appropriate networking innovation for cloud figuring. Besides, we propose a way to deal with recognize DDoS attacks in SDN-based cloud by using the highlights of SDN. The proposed approach can detect the DDoS attacks with very low communicational and computational overhead. Our claims are well supported by the extensive simulation-based experiments.

Qiao Yan et al [10], study the Distributed Denial of Service (DDoS) attacks in cloud registering conditions are becoming because of the fundamental attributes of cloud figuring. In any case, there is an opposing connection among SDN and DDoS attacks. On one hand, the capacities of SDN, including software-based traffic investigation, brought together control, worldwide perspective on the system, dynamic refreshing of sending rules, make it simpler to identify and respond to DDoS attacks. Then again, the security of SDN itself stays to be tended to, and potential DDoS vulnerabilities exist crosswise over SDN stages. In this paper, creator talk about the new patterns and attributes of DDoS attacks in cloud processing, and give an extensive overview of protection components against DDoS attacks utilizing SDN. Apparently, the opposing connection among SDN and DDoS attacks has not been all around tended to in past works. This work can see how to utilize SDN's favorable circumstances to vanquish DDoS attacks in cloud processing conditions and how to anticipate SDN itself from turning into a casualty of DDoS attacks, which are significant for the smooth development of SDN-based cloud without the diversion of DDoS attacks.

Houda Guesmi et al [11], from their view of Distributed Denial of Service (DDoS) attacks represent major risks for the current cloud computing architecture. The rate of DDoS attacks in cloud is growing because of the essential characteristics of cloud computing. In this paper, we propose to use Software Defined Network (SDN) architecture and Fast Entropy approach in order to secure cloud computing environment from DDoS attacks in real time. Thus, we exploited the centralized control and programmable characteristics of SDN architecture to supervise cloud traffics. The provided architecture collects and analyzes flow tables from switches. It also detects DDoS attacks by the controller using Fast Entropy algorithms. Through the performed experimental tests, we evaluated the performance of our solution in defending Cloud computing infrastructure against Distributed Denial of Service attacks.

### III. PROBLEM STATEMENT

Software Defined designs is that of the changes inabilities to separate between authentic stream and unauthentic stream. This defect takes into consideration attackers to perform success DoS attacks at the Data plane level by filling the switches stream buffer with false demands. While it would be able to focus on
an individual information path and attempt to stop its accessibility, all things considered, the controller would be focused on, adequately making and spreading a system-wide lapse by in accessibility. The possibility of this can be conceivably crushing, especially production settings where service seeing high utilization will be unusable to customers and representatives [12]. It finds an effective way to decompose the general problem into smaller problems over paths to solve packet forwarding. Packet forwarding is one of the core functions of networking that can be defined by two kinds of rules. One is a routing policy to define how the packets can traverse in a network from a 220 source to a destination; and the other one is an endpoint policy, such as packet monitoring, access control, etc. The major challenging task for SDN switches is to define an access control mechanism that uses MAC filtering rules.

IV. PROPOSED METHOD

In SDN, security issues have been viewed as the primary obstacle in recent investigations. In SDN, the control plane is decoupled from the information plane and network device are constrained by the brought together controller. Hence, special consideration is required for the SDN control plane security attacks, particularly the Denial of Service (DoS) attack. In the battle to verify our stored information and the system, IDS can demonstrate to be an invaluable tool, where its aim is to perform early recognition of malicious action. Thus, by using IDS, one can identify an attack and notify appropriate user immediately. Signature based detection is performed by comparing the information collected from a network or system against a database of signatures. A signature is a predefined set of patterns or rules that correspond to a known attack. This technique is also recognized as misuse detection. To overcome the DoS attack in SDC, we propose the host-based IDSs. it having the ability to monitor local events of a host, can detect attacks that cannot be seen by a NIDS. The host-based IDSs do can analyze the encrypted information and also used Signature based detection approach.

Fig 1: Proposed Architecture

a. Data Gathering

Generally, in order to fully examine an IDS a suitable dataset is necessary. The key point is to accurately separate the normal data from the abnormal (attack) data. To achieve this goal, in the data gathering phase, the web applications and web server should be provided by a fully protected condition to ensure that we can gather the pure normal user behaviors. On the other hand, in order to prove the capability of the system in detecting various attacks, the attack data should cover large range of today’s DDoS attacks. It should be noted that there are other methods for interacting with web application such as HEAD and PUT, which are ignored because of their low importance. Second, the boundaries of sessions are not clearly defined in common log files [13]. As a result, extracting web sessions from these log files is not a straightforward process. Despite the fact that there are a few heuristics, for example, time out scheme that can lead us to recognize web sessions, these techniques are not extremely exact practically speaking. It takes the information from the cloud and for this situation the information of the cloud owner was sent to the intruders.

b. Analysing DDoS Attack

Various kinds of conventional DDoS attacks can be arisen in an SDN domain, yet it is a variation using manufactured stream
passages which can be outfitted by an attacker so as to focus on a controller and request its accessibility. By flooding the controller with solicitations for a stream choice, the controllers figure assets could progress toward becoming overpowered, and the controller would be rendered incapable to manage any authentic requests it gets. By focusing on the centralised point of control (for example the controller) it renders the whole network to a great extent unusable [14, 15]. While information path as of now in the system might almost certainly work incidentally with a brought down controller, once the hard break of standards in their table has terminated, they will be required to request with the controller once more, which will be not able arrangement with solicitations. In the event that an attacker(s) can be persevering with their flooding, this will in the long run reason the inaccessibility of all network functionality.

c. Monitoring Attacks using Host based IDS

A host-based intrusion detection system (HIDS) that monitors and evaluates the internals of a calculating system as well as the network packets on its network boundaries. The objective of attackers is frameworks in corporate system having classified data. HIDS identifies which program gets to what assets and finds that, for instance, a word-processor has all of a sudden begun changing the framework secret word database. HIDS additionally recognizes data present in framework and check data is unblemished for example not changed by gatecrashers.

Host based IDS (HIDS) screens explicit host machines, organize based IDS (NIDS) distinguishes interruptions on key system focuses and disseminated IDS (DIDS) works both on host just as system. IDSs produce cautions for the directors which depend on obvious positives or genuine alerts when really interruption happens and false positive or false alerts if there should be an occurrence of an off-base discovery by the framework. IDSs can distinguish interruption designs by fundamentally examining the system bundles, applying marks (pre-defined principles) and creating cautions for framework heads [16]. IDS utilize two technique for identification for example irregularity recognition, that deals with client standards of conduct and suspicious conduct. Other strategy is abuse recognition that can identify through prestigious attack designs and coordinating a lot of defined principles or attack against framework vulnerabilities through port filtering. This host-based security application examinations traffic coursing through the system interfaces of the observed (end-point) framework. As a result of the working of Virtual Machines in most regular cloud stages, there ought not be any similarity issues. A HIDS or HIPS can screen a virtual NIC equivalent to a physical NIC [17]. The OS should really not show any modification among virtual and physical devices to the requests that are connected.

The proposed HIDS algorithm has two main modules namely, REQUEST-HANDLER() and RESPONSE-HANDLER()

Algorithm 1: REQUEST-HANDLER()

Input: RP - request packet, t - time at which RP was received.

Output: Updated Request-sent table, Status

1: if (RP == mal_found) then
2: Status= mal_found
3: else if (RP is Unicast) then
4: Status=Unicast
5: else
6: if (RPIPS == RPIPD) then
7: Status=Gratuitous Packet
8: VERIFY IP-MAC(RP, τ)
9: else

![HIDs Architecture](image-url)
process running on the host and several VMs run over it. A type II environment, on the other hand, implies that the VMM runs as a software on the host machine. Normal host processes as well as VMM (over which the VM) run on the host machine. So, we can monitor the intruder’s activity easily and can protect the data from them.

V. EXPERIMENTAL RESULT

In this section, we discuss our approach to evaluate the effectiveness of our proposed work. In our evaluation, we emulate a scenario where a malicious host under control of an attacker is present in an SDN network. In our experiment, we conduct a set of DDoS attacks towards a cloud data. The attacker targets the cloud data. We use two requests for our proposed work that were shown below.

The REQUEST-HANDLER() generates a RQP event on receipt of the request packet sent by m having IP(v)-MAC(rp). IDS send the investigation request for the confirmation and the PRQP instance is produced. And the transmission was established by the swarms. V is unaffected and it will be the answer by the ARP response packet which consume IP(v)-MAC(v), hence MAC is dissimilar than the one in the request packet presence verified. Here the attackers will be responsible to prove IP(v)-MAC(rp). From this attacker will be detected by IDS, hence there respond must be at least one to the PRQP whose MAC is dissimilar from the request packet being established. So, IP (v)-MAC(k) is properly identified to be deceived.

The RESPONSE-HANDLER() will check for needless parcel which will be discovered false as source IP and destination IP’s are not same. At that point it will compare the IP(v)-MAC(v) pair with that of IDS, yet no match will be found. At that point it will check solicitation sent table for a match with IP(v), won't discover a match. Next on correlation with verification restricting table, likewise no match will be discovered (expecting it was not confirmed before). This will bring about calling of VERIFY IP-MAC(RSP,τ) which at that point will confirm if IP(v) is in verification table. Since it won't discover any match, a test will be sent to IP(v)and record IP(v), MAC(v) in confirmation table and call the SPOOF-DETECTOR(RP, τ). The SPOOF-DETECTOR will hang tight for Treq time interim and after that confirm IP(v) with IP of PRSP, will discover a match, think about the MAC(v), will discover a counterpart for the comparing MAC address, coming about into the assertion of the parcel be Genuine.

Algorithm 2: RESPONSE HANDLER ()
Input: RS - ARP response packet, t - time at which RSP was received RSMACs – Response MAC Send, RSMACD - Response MAC Detect
Output: Updated Response-received table, Status
1: if (RS == mal_found) then
2: Status= mal_found
3: else
4: Add RSIPS, RSMACs and τ to Response-received table
5: if (RSIPS == RIPIPDP) then
6: Status= Gratuitous
7: VERIFY IP-MAC(RSP, τ)
8: else if ((RSIPD == IP(HIDS) && RSMACD == MAC(HIDS)) && (RSIPS == VRFTIPS[k])(for some k, 1≤ k≤ VRFTMAX )) then
9: EXIT
10: else if (RSMACs == AUTHMACS[ j]) then
11: Status=Genuine
12: Else
13: Status=Spoofed
14: end if
15: else
16: VERIFY IP-MAC(RS, τ)
17: end if
18: end if
19: end if

HIDS techniques, with respect to cloud generally, can be divided into three main deployment-based classifications. HIDS, inside the VM for monitoring, can be deployed in the host OS (where it can monitor either the host OS or the guest OS via communication through the VMM) or in a separate guest OS. Virtual Machine Monitor (VMM) is a software package that allows the formation, management and supremacy of virtual machines (VM) and achieves the process of a virtualized situation on top of a physical host machine. The first scenario, in which the IDS would be completely under the control of the customer, has the drawback of low attack resistance. It has been overwhelmingly rejected in the literature and hence marked unsuitable for the virtual cloud. In this proposed work it describes as VMIs suited for type I or type II environment—where a type I environment implies that the VMM is the only
The experimental environment to perform the DDoS attacks in the simulated SDN and cloud computing environments. To measure the performance of IDs, we define the detection rate (DR) and false positive rate (FPR) as follows:

\[ DR = \frac{TP}{TP + FN}, \quad FPR = \frac{FP}{TN + FP} \]
TP- True Positive, FP- False Positive, TN- True Negative, FN- False Negative.

VI. CONCLUSIONS

With SDN technology user can realize the flexibility, manageability, dynamicity, programmability, and intelligence to present network manner by using single lookout, preparation and saving cost. Many features that may contain valuable information could be extracted or it can be a focus on one specific type of attack. Mainly this paper deals with the DDoS Attack in the SDN for the Cloud data. In this paper, we have presented an HIDS for detecting the DDoS attack for monitoring the intruder’s activity. In this Host based IDS, the host machine would allow the administrator to monitor the attacker and activity of the attackers and provide an alert to the owner of the data in cloud and our proposed system is provide improving efficiency of overall performance of the existing IDS work and the result shown in experimental section.

REFERENCES

[7]. Jeanetteet al, “Securing cloud, SDN and large data network environments from emerging DDoS attacks” IEEE, Jan. 2017
[8]. Tasnim Tamanna et al, “SDN, A research on SDN assets and tools to defence DDoS attack in cloud computing environment”. 2017, IEEE