Towards Securing Cloud Computing from DDOS Attacks

Ishtiaq Ahmed[1], Sheeraz Ahmed[2]
Department of Computer Science
Iqra National University
Peshawar, Pakistan

Asif Nawaz[3]
Faculty of Engineering
Higher College of Technology
Dubai, UAE

Sadeeq Jan[4]
Department of CS and IT
National Center for Cyber Security
UET Peshawar, Pakistan

Zeeshan Najam[5]
Department of Electrical Engineering
MNS Uni of Engg and Technology
Multan, Pakistan

Muneeb Saadat[6], Rehan Ali Khan[7]
Department of Electrical Engineering
University of Science and Technology
Bannu, Pakistan

Khalid Zaman[8]
Department of Computer Science
Near East University North Cyprus
Mersin 10, Turkey

***Abstract*—Cloud computing (CC) is an advanced technology that provides data sharing and access to computing resources. The cloud deployment model represents the exact type of cloud environment based on ownership, size, and accessibility rights, and also describes the purpose and nature of the cloud. Since all processes today are computerized, consumers need a lot amount of data and cache size. The security of the cloud is ensured in many levels, but the scope of intrusions makes it necessary to understand the factors that affect cloud security. CC-certified users rely on third parties for their other important security issues in third-party computing clouds. A DDoS attack is an attack-type in which it is not necessary to send a large number of packets to the server, which makes it impossible for legitimate users to access them. In this research work, a DDoS attack was launched and a tool for launching a DDoS attack was discussed. In this research, DDoS attacks were rejected using three different SNORT rules. In this research, rules predefined for detecting DDoS attacks on SNORT profiles detect and prevent DDoS attacks, but because they block certain legitimate requests and generate false alarms, this should be the subject of future research.**

Keywords—Cloud computing; denial of service; SNORT rules; network; energy consumption

I. INTRODUCTION

Cloud computing, a popular topic in the past few years involves various technologies and provides scalable IT related services over the Internet. Cloud computing is the use of various services, such as software development platforms, servers, storage and software, over the internet, often referred to as the "cloud." Emergence of cloud computing technologies has changed the way we store, retrieve, and archive our data. With the promise of unlimited, reliable and always-available storage, a lot of private and confidential data are now stored on different cloud platforms.

Cloud computing is a concept used primarily in computer science, but in the last decade, the term "cloud computing" has always been used in the field of library and information science, as well as in other areas like Business, Industry, Medical Science and Corporate sector, etc. is also being done the application of cloud computing.

On the Internet, cloud computing (CC) is an advanced technology that provides data sharing and access to computing resources. CC is an Internet-based environment that provides services such as storage, applications, and servers [1,2]. CC is a very easy and fun method for today's consumers to use the Internet and do professional with CC. Since it is about providing remote resource resources to alleviate consumer problems, they need to use only those resources. They do not have to pay for local services such as infrastructure or storage. This atmosphere can be seen as a novel sculptural archetypal that offers greater flexibility and lower cost availability as shown in Fig. 1. Data and resources are available anytime, anywhere and accessible on the Internet. CC permits you to launch your own applications, software, and hosts on a virtual server, which can be restored when required. For example, Google App Engine, societal networks, Google Docs, AWS, etc.

CC provides a number of steps, including utilities and grid computing. Grid computing is a large-scale, decentralized calculation that provides a direct way to access a variety of useful resources [3,4]. To manage the resources of its users, service providers have been enabled through utility computing [5]. In 1960, ARPA (Advanced Research Institute) in the United States began to realize the connectivity of integrated devices [6]. They are concerned about integrated devices because ARPA agents have different branch sizes and participate in different functions of branch search. ARPA funds its employees so they can find new ideas. Therefore, the agency must connect with the distribution agencies and share their personal efforts with everyone to achieve the best results. To this end, the IRPA's IRAPNET is proposed and four different branches have been established: Stanford Research Institute (SR), the University of California, Santa Barbara, and the University of Utah. These devices do not affect each other. The ARPA [7,8,9] proposed the current IMP protocol (the current message processor) for this purpose. IMP is designed to make communiqué conceivable and act corresponding a gateway. The ARPA connects its four twigs together, with branches from apiece host, and apiece branch connects with another branch of the IMP.

Since cloud technology offers a lot of benefits to consumers, these benefits must be classified with respect to the user's needs. The cloud deployment model represents the exact type of cloud environment based on ownership, size, and accessibility rights, and also describes the purpose and nature of the cloud [10].

A. *Security in CC*

Data safety transmitted to the Internet in the Cloud Configuration field is actually clouded computing security. Since all processes today are computerized, consumers need a lot amount of data and cache size. In CC, users must request that their data be stored and retrieved [11,12]. In this environment more storage capacity and services are accessed in many places. For cloud breadwinners, safety is an ever-present tricky, and security is a huge challenge regardless of Internet access. Because as soon as a real user receives their information from one place, the interloper can entree the information from alternative site, which may prevent the original user from approaching.

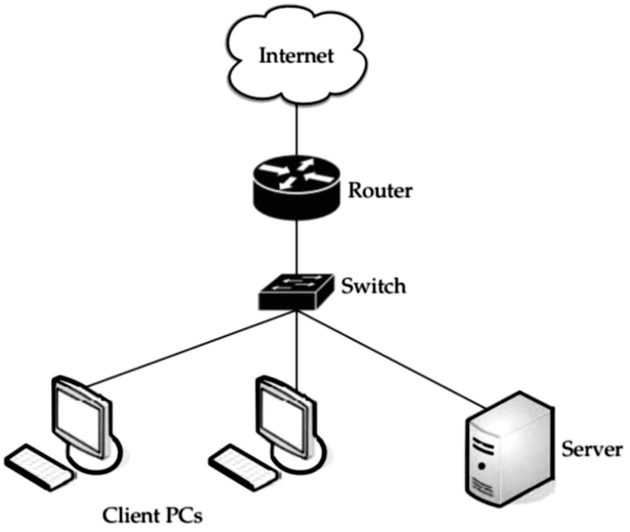


Fig. 1. Internet Depicted as Cloud in a Network.

B. *DDoS Attacks in CC*

DDoS attacks can disable cloud services at any time. The amount of DDoS ravages increased by 51% in 2013, but companies using DDoS security services can prevent these attacks. Denial of service attack usually creates a working server, system, or network that can advertise the target asset and prevent real clients from using the resource. The target of DOS Attack is the same as the target of DoS Attack. However, these attacks are a distributed form of DoS attacks, meaning they come from many locations and target a single victim [13,14,15].

The benefit of denying the distribution of service attacks is when attacks become accessible, expandable, flexible, and accessible from somewhere, because denial of service attacks is due to dissimilar sites [16]. Several hosts are involved in the ravage. In fact, they are named managers and representatives. An attacker prepares the first two or more managers and, with the help of these managers, manages the agent so that the service refuses to split the attack.

DDoS attacks are increasing speedily, causing great harm to large businesses and economic loss to global businesses and websites [17]. Although the Department of Defense condemns funding for targeted attacks, the economic withdrawal is often not the cause of such attacks. In each case, the attacker claims to destroy the company or sole attacker; in other cases, the attacker only tries to hit the target, causing the most damage, or hitting too many targets. There is a loss. When identifying a partner in denial of service attack, the target of the attack may be displayed. DDOS attacks architecture is explained diagrammatically in Fig. 2.

Many DoS attacks are actually split, and attack traffic comes from different systems. Although DOS attacks generated by a single source are more likely to be downplayed, as defense networks can intercept traffic through malicious sources, attacks from different systems are difficult to identify and defend [18]. The attack is because it's difficult to distinguish malicious packets and actual traffic.

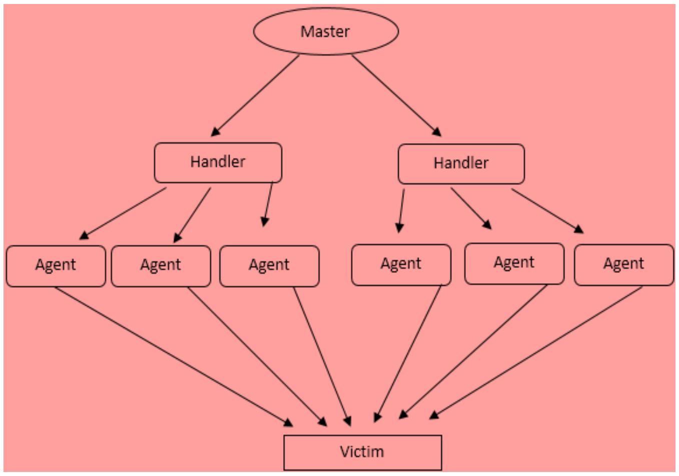


Fig. 2. DDoS Attacks Architecture.

II. Methodology

DDoS Spell is a massively synchronized ravage on the search network's resources or the availability of the service. By managing a large number of hostages outside the network, a large number of data packets are sent to the target node to attack the DDoS. Victims use high traffic bandwidth and do not permit it to reach the victim of another large package [19]. There are many security vulnerabilities due to CC availability and scalability. The existence of DDoS over the network greatly increases the loss of packets, and causes security issues on the network. To identify such kind of attack various techniques are used in the previous researches like entropy-based anomaly recognition, this technique.

In the proposed work we test two approaches for the recognition of DDoS ravage, SNORT and Mutual Egress Filtering Approach following are the topology and configurations for both approaches. In this research work, we test two approaches for the recognition of DDoS ravage, SNORT and Mutual Egress Filtering approach following are the topology and configurations for both approaches.

A. Network Topology

Network topology is in what way we create networks to simulate DDoS ravage and sense it in the cloud. Fig. 3 temporarily describes the topology.

The topology has been implemented in Gns3 and consists of four networks. For the invaders, two different networks started for the ravage. The attack bump with IP address 1.1.1.2 has been fitted as Virtual Machine in VMware [20]. Another attacker with our IP address of 10.0.0.2 is our hosting system. The test server and SNORT node are also installed in VMware. The test node checks if the server responds after starting a DDoS attack. Install the SNORT to sense DDoS ravage and keep between these servers and the revenue generating network.

Windows Server 2012 is fitted in VMware and includes Internet Information Services (IIS). IIS is contained within in the server window and consist of the default Web site. The default Windows Server 2012 site is easy to manage.

Same topology is used for Mutual Egress Filtering Approach but instead of SNORT an Access Control List is configured on egress router.

1) *Configuration of SNORT:* First, the router is organized with four edges and assigns IP address to each interface:

a) Fast Ethernet (0/0) and the IP address of the line is 10.0.0.1

b) Fast Ethernet (0/1) and the IP address of the line is 1.1.1.1.

c) Fast Ethernet (4/0) and the IP address of the line is 192.168.2.2.

d) Fast Ethernet (4/1) and the IP address of the line is 192.168.0.2.

Then, configure SNORT in VMware. SNORT performs according to the rules, and the rule no 1 has already loaded SNORT. The loaded instructions hold a file because these files are similarly in the established SNORT. We need to use rules to copy some of the downloaded folders and then go to into the installed directory of SNORT software and paste them there. In these files, there is a local named folder. Local can be edited by rule users. Notepad, Notepad++ or any folder editor in the file editor can modify rules or create your own rules according to your needs. We also changed the rules for detecting DDoS ravage in CC.

dropTCP any any> any 80 (\msg:"Reset outside window"; \ detection_filter:trackby_dst, count 30, seconds 1; \ new_action drop; timeout 50; sid:1000001;)".

This is our instruction for detecting DDoS ravage in CC and has been further to the local SNORT folder. Nodes that install SNORT also have two dissimilar boundaries: one that connects straight to the external network and one that connects to the internal server, and that is victim of the attacker. The IP addresses of the two edges are 192.168.0.3 and 2.0.0.1 and are linked over a network adapter. Install Windows Server 2012 and configure IIS (information on the Internet) on the server. Installing Windows Server 2012 is as meek as installing somewhat Windows OS. The IP address of the server is 2.0.0.2, and the hacker points to the address. The attacker's node has been configured as if it contained the LOIC letter, which is explained in Fig. 4.

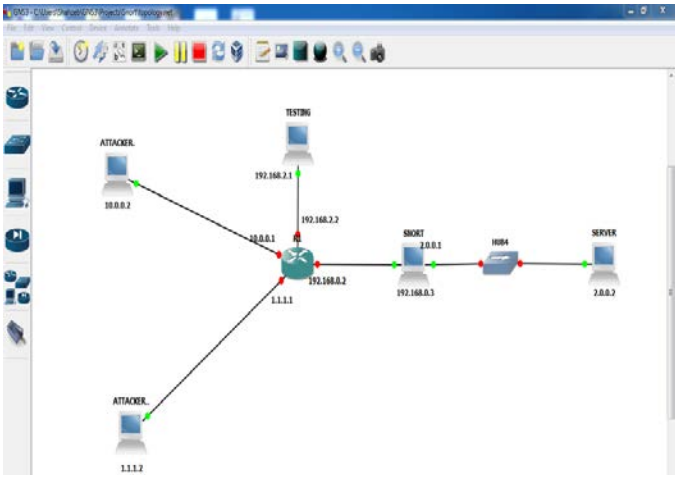
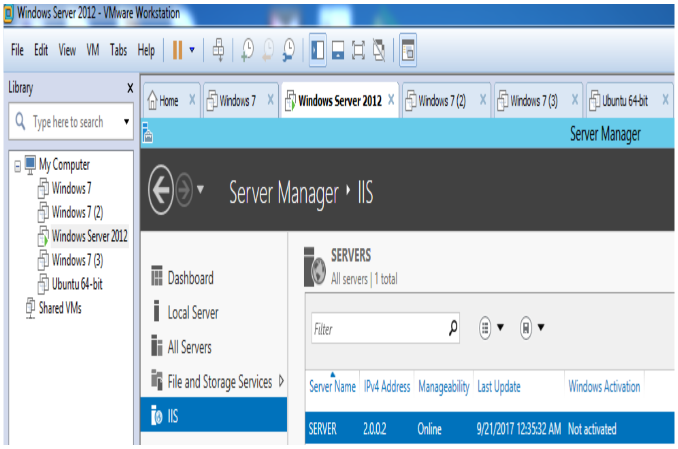


Fig. 3. Network Topology.



Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
SERVER	2.0.0.2	Online	9/21/2017 12:35:32 AM	Not activated

Fig. 4. VMware Platform.

B. Simulator Setup

To test the impact of DDoS ravage and detect them in the cloud using SNORT, the following tools were configured.

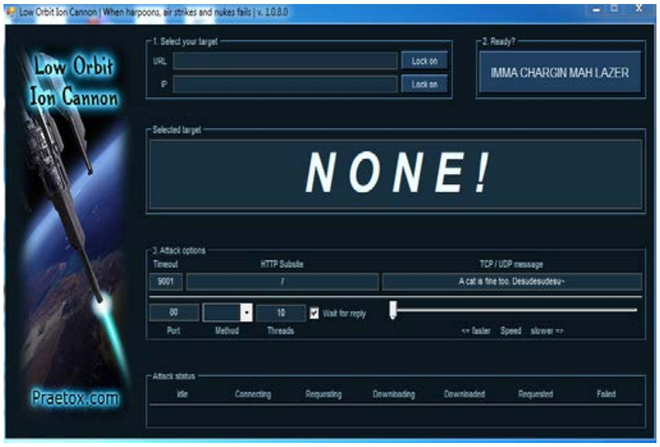
1) Graphical Network Simulator (GNS3): GNS3 is used to create network topologies and simulate various kinds of ravage. Fig. 3, variant devices are displayed, consists of routers, switches, firewalls, and computers. These all devices are used in an actual network location. GNS3 uses these devices virtually, providing us with an atmosphere to test and model various kinds of topologies. In order to use GNS3IOS, the actual CISCO device images are used, which are really the OS (operating systems) of the router [21]. Users can initial fetch these pictures to the router configuration in the GNS3 simulator. Lacking an IOS image, the router will not be able to perform its operations.

2) VMware: A database which permits employers to develop many virtual machines by using a solo workstation is VMware. On the VMware stage, you can improve multiple virtual machineries to one physical apparatus, and the virtual machine can run as per another. It provides excellent routine when you need to practice a different operating system or other server in your user's system. For example, you can install a server and a Windows operating system in VMware to test the network or launch extra applications. It is informal to connect in any OS (operating system.

3) LOIC (Low Orbit Ion Canon): LOIC is an uncluttered basis net anxiety test device used to refuse service attacks. LOIC (for Microsoft Windows and Mac OS X) is a flood-making instrument for creating a large number of network streams for use with network resources or applications. This amount of traffic can be a result of service failure or lack of visibility due to server or application downtime. Users can use LOIC to refuse service attacks and reload the server using native TCP or UDP TCP packets.

Fig. 5 shows three parameters that trigger the attack: the target, the preparation, and the attack parameters.

- When selecting a destination, there will be a URL and an IP address. Click the URL to specify the target service URL. The IP Tap is secondhand to enter the IP address of the target package [22].
- Underneath the "Attack" choice, there are port challenges, technologies and risks. The number of ports that connect to the port for the application are identified. This technique is castoff for TCP, UDP, and HTTP, and risk associations are castoff to determine the amount of fears that arise.
- Once all the necessities for the attack have been determined, the ready state is reached. In the "Complete" section, there is a button that you can click to launch an attack.


Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.8.0

Selected target: NONE!

Timeout: 9001
HTTP Subsite: /
TCP / UDP message: A cat is fine too. Desudesudesu~
Port: 80
Threads: 10
☑ Wait for reply

Fig. 5. LOIC A DDoS Attacking Tool.

C. Proposed Solution for DoS and DDoS Attacks

Various methods have been previously used to sense DoS and DDoS attacks in CC. In our effort, SNORT is used to sense DoS and DDoS. SNORT is software containing a list of instructions. It is also described in section, using these SNORT instructions to sense various kinds of attacks. Users can adjust these rules as needed. In a previous study [23], DoS and DDoS attacks were detected using SNORT according to the following rules:

- "dropTCP any any> any 80 (\msg:"Reset outside window"; \ detection_filter:trackby_src, count 30, seconds 1; \ new_action drop; timeout 50; sid:1000001;)".

This instruction triggers the SNORT device to sense a TCP appeal from any basis on port 80 (if more than 30 requests/sec) and cannot establish a connection with the IP address for 50 seconds.

In our effort, we made some variations to the rules, because the above rules only sense DoS attacks, which mean that this instruction can't sense DDoS attacks, since in the rules by_src, which means from any source An IP address, is detected every second for any IP address. The changes we made to detect DDoS attacks,

- "dropTCP any any> any 80 (\msg:"Reset outside window"; \ detection_filter: trackby_dst, count 30, seconds 1; \ new_action drop; timeout 50; sid:1000001;)".

In this instruction, we practice by_dst to sense the IP address close to its target and have found multiple IP addresses. Another solution to detect DoS and DDoS attack is combine both the rules and create another rule which will sense DoS and DDoS attacks from both sides either from source side or also from destination side. The rule is written as:

```
        if (by_src,count==30, seconds 1;\)
              {
        “droptcp                                   any
any>80(\detection_filter:new_actiondrop;timeout
50;sid1000001;)”.})
        }
        else
        {
        “dropTCP any any> any 80 (\msg:"Reset outside
window"; \ detection_filter:trackby_src, count 30, seconds 1; \
new_action drop; timeout 50; sid:1000001;)”.
        }
```

This law detects DoS and DDoS attacks from both ends, according to this rule SNORT monitors traffic which is coming from one source, and from multiple sources as well.

1) Design procedure: After identifying different approaches for sensing DDoS ravage in CC, the suitable approach is used to detect DDoS ravage. In the proposed effort we implement two different approaches that is SNORT as IDS and Mutual Egress Filtering Approach. After testing both the approaches we make a comparative analysis that which approach is better for preventing DDoS attack in Cloud Environment. Fig. 6 describes the design procedure of our proposed work.

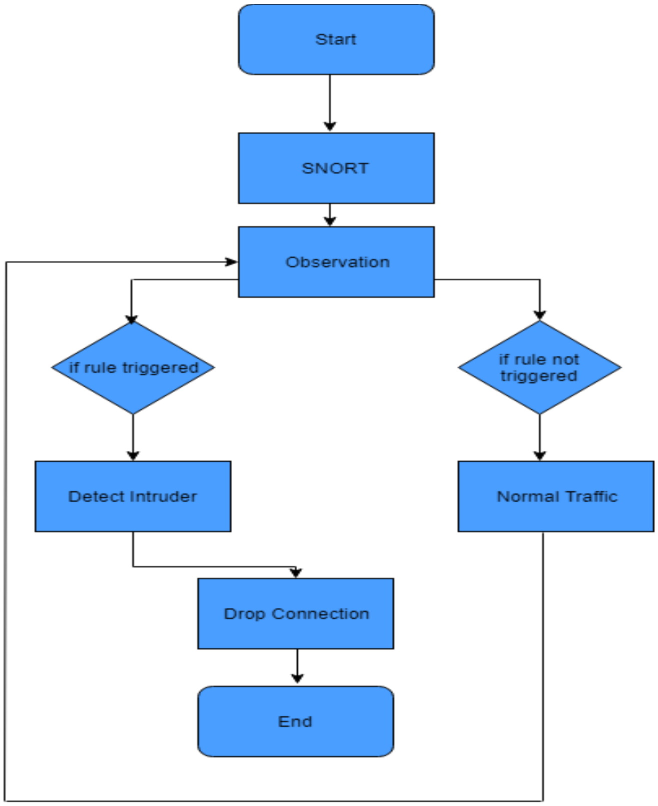


Fig. 6. Block Diagram for SNORT.

In the proposed work first we test IDS SNORT, for the detection of DDoS attack. Following are the major steps of our proposed solution.

- Start communication.
- SNORT implementation.
- Observation of data.
- Detection of DDoS attack.
- End of communication.

After creating the topology and setting up network configurations, communication is started. SNORT AN ID is implemented with predefined rules to observe the flow of data. In the proposed work we detect DDoS attack, for that a rule is written in the base file of SNORT, which is used for the recognition of DDoS attack. If the rule is triggered, then the flow of data is harmful. SNORT will aware the network administrator about the invasion and drop connection with the corresponding communicating party. If the rule is not triggered, that means that the flow of data is normal.

III. Simulation and Results

To use SNORT [18], the network topology and its format are configured. The DDoS ravage has been launched. It spoke fleetingly about its impact on cloud services; fixed between SNORT server and received network. The latest LOIC tool (Canon Ion Orbit) is also under discussion. This chapter contains various SNORT rules, simulation analysis, and implementation and comparison results.

To integrate shared DDoS features, a virtual background has been created. The virtual machine consists of a client and a cloud server. It is placed in different areas of the earth. SNORT is built in the center of external networks and servers. Locks can be used to test DOS attacks. This requires either the source IP address (board service) or the source URL, the port address (port numeral of the board bid), and the nature of the ravage under the target service. What kind of attack is TCP, UDP or HTTP form should apply. Once all these parameters have been defined, when you click this button, the Ready button will appear and the saturation of the selected service will begin. SNORT is used to detect attacks. SNORT contains config files. Here, the home network is defined as the net address of the server, and the exterior network is defined as something that isn’t a homebased network. We can protect our home network from DDoS attacks. An external network is a network from outside or from anywhere.

We employed SNORT with two dissimilar directions. The last is the earlier search rule, which detects DDoS attacks, but not both. It can sense only one ravager at a time. Another principle is that we have to make variations to sense many ravagers at the same time and we have to give better results than the previous search rules. After testing SNORT, we implemented a mutual sewerage filtering method that completely prevented the attacker from flooding the server.

A. Monitoring Server Performance when DDoS Attack has not been Launched

Fig. 7 displays reserve monitoring previously any contact with the server: The chart in figure overhead shows six CPU procedure at the beginning of the performance check. The processor uses three percent, and its load reaches six percent after a period of time, and through continuous monitoring, it causes the processor to use three or four percent. According to some permissible necessities, it reaches 8 percent and 9 percent but no further than 10 percent.

B. Monitoring Server Performance with DDoS Attack Launched

Afterward starting the DDoS ravage, if SNORT is not implemented and the TCP SYN ravage is launched from two dissimilar sites, then the server act is checked. Fig. 8 shows how DDoS attacks use server properties.

Initial, there is no server request and CPU load are low. When an attacker knockouts server, server responds to the ravagers request. As a TCPSYN ravage, its server is on relevant IP address (attacker's IP address) to establish a TCP connection and three-way connection between client and server during TCP linking. First, the user directs a SYN package, which means that user wishes to launch a TCP linking to the server and responds with the SYN response and a salutation package. The client sends an identity packet. After this process, "Establishes the original connection", but does not wait for a response from the attacker server, and continuously sends the SYN packet. As a consequence, the server becomes busy, so sincere users cannot respond, as shown in Fig. 8. CPU ravage reaches the top end of CPU but reaches time, time, hour, hour, hour.

C. When SNORT is Implemented using existing Rule

Monitor server routine when launching SNORT, launch attack and SNORT the same solution - detect and prevent attacks. Fig. 9 use the previous experiment [14], to illustrate how SNORT can prevent DDoS attacks.

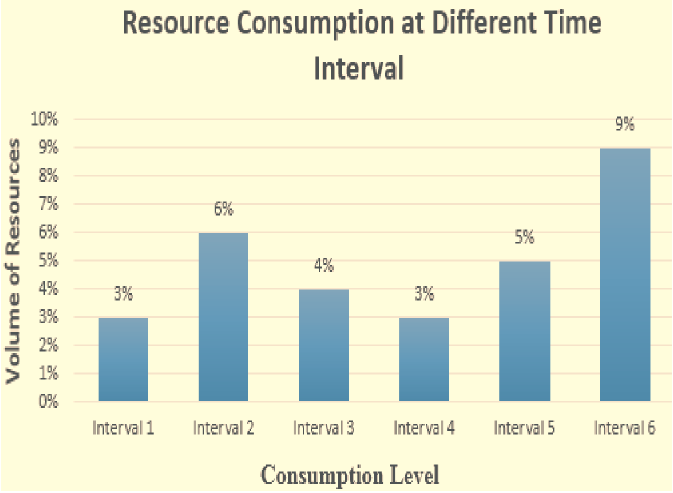


Fig. 7. Resource Monitoring before the Attack.

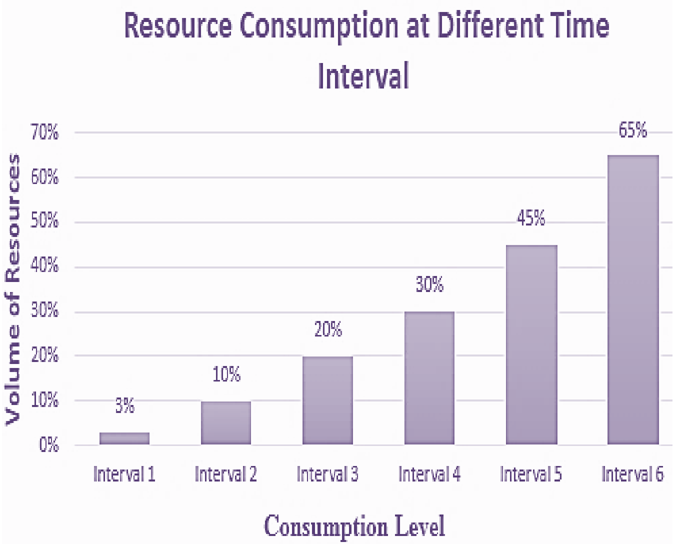


Fig. 8. Resources Monitoring after the Attack.

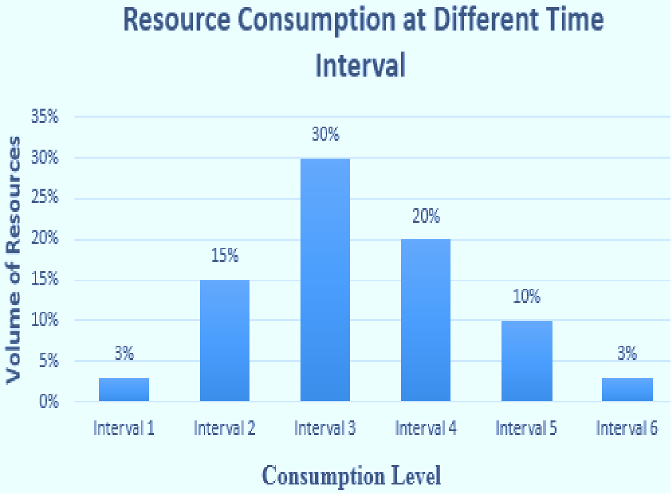


Fig. 9. Resource Monitoring when SNORT is Implemented with New Rule.

Fig. 9 shows that our proposed rules totally avoid DDoS attacks. In the above data (interval 1, interval 2, interval 3, interval 4, interval 5, and interval 6), the period interval for resource monitoring is different. As shown in the figure, when the ravage reaches the server, CPU tradition is constantly monitored at six different intervals. At interval 1, CPU usage is 3%. After a while, it will reach 15 reach and will gradually increase over the second and third intervals. To detect this ravage, SNORT is installed among the server and incoming network. When an attacker is hit by a server, resource consumption increases, but when the SNORT rule is started, it stops attacker. Resource feasting is reduced at intervals 4, 5, and 6, and CPU usage returns to its normal state.

D. Monitoring Server Performance when SNORT is Implemented with a Combined rule which is the Combination of First and Second Rule

After SNORT is executed by the blend rule, server act is constantly observed. Fig. 10 illustrates how to reduce server resource consumption from this point of view.

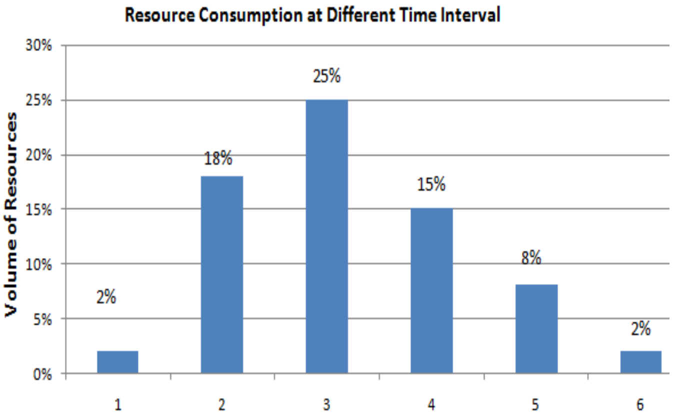


Fig. 10. Resource Monitoring when SNORT is Implemented with Combined Rule.

In the above image, we can look at different time intervals for monitoring resource consumption. At interval 1, the server resource is 2% on normal when the attack has not yet begun. When a flooded packet arrives at the server, the DDoS attack begins, increasing resource consumption between slots 2 and 3. After triggering the combined SNORT rule, resource consumption decreases when the condition is met and when the attack is immediately rejected. At intervals 4, 5 and 6, we can see that the server is normal.

E. Comparison of SNORT Rules

After testing SNORT Approaches, both are rules are giving better results in the detection of DDoS attack, SNORT works on rules to identify and prevent the attack. Fig. 11 shows the results and comparative analysis of SNORT rules.

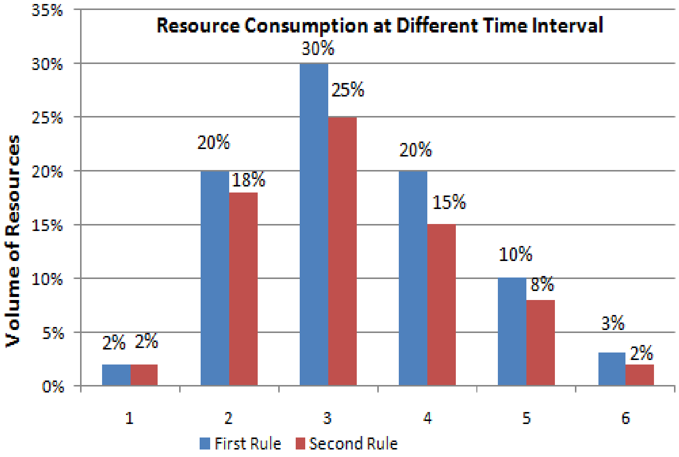


Fig. 11. Comparative Analysis of SNORT Rules.

In the above Fig. 11, first rule is our proposed rule and Second rule is the combination of both previous (existing) rule and proposed rule. When SNORT is implemented using the first principle and SNORT is implemented using the second principle. The blue chart shows the server performance when SNORT is implemented using the first rule, and when the coral map shows the server performance when SNORT is implemented using the second rule. These results are discussed in Fig. 10 and 11, but on the contrary, when we look at the ranges of 4 and 5 in the two figures, the first SNORT principle of SNORT will gradually reduce the impact of the DDoS attack. Yes, the second principle is to minimize the effect of denial of service and an immediate attack on DDoS. Both methods prevent predetermined rule-based attacks. SNORT is the best choice for the global network. For CC environments, SNORT works well as cloud users are spreading all over the world.

IV. CONCLUSION

The determination of the planned effort is to define the CC, its service model, safety problems, the address of the CC security issue, and the details of the DDoS attack and its influence on the cloud server. Computer security is a serious problem in modern clouds because it provides data storage, data exchange and other resources that are available anywhere in the world. The Internet is a public network that allows an attacker to access a cloud service without any access. CC-certified users rely on third parties for their other important security issues in third-party computing clouds. A DDoS attack is an attack-type in which it is not necessary to send a large number of packets to the server, which makes it impossible for legitimate users to access them. In this research work, a DDoS attack was launched and a tool for launching a DDoS attack was discussed. In this research, DDoS attacks were rejected using three different SNORT rules. Since SNORT uses rules after specifying rules in the SNORT base file, attacks are identified and blocked each time. In the proposed research, written rules for detecting DDoS attacks on SNORT profiles detect and prevent DDoS attacks, but because they block certain legitimate requests and generate false alarms, this should be the subject of future research.

REFERENCES

[1] Rajpurohit, Akshat, Akshat Jain, and Manish Sharma. "A Review on Cloud Computing and its Security Issues." (2018).

[2] Rakotondravony, Noëlle, Benjamin Taubmann, Waseem Mandarawi, Eva Weishäupl, Peng Xu, Bojan Kolosnjaji, Mykolai Protsenko, Hermann De Meer, and Hans P. Reiser. "Classifying malware attacks in IaaS cloud environments." Journal of Cloud Computing 6, no. 1 (2017): 26.

[3] Sridhar, S., and S. Smys. "A Survey on Cloud Security Issues and Challenges with Possible Measures." In International Conference on Inventive Research in Engineering and Technology, vol. 4. 2016.

[4] Mondal, Ranjan Kumar, and Debabrata Sarddar. "Utility Computing." International Journal of Grid and Distributed Computing 8, no. 4 (2015): 115-122.

[5] Nandi, Enakshmi, Ranjan Kumar Mondal, Payel Ray, Biswajit Biswas, Manas Kumar Sanyal, and Debabrata Sarddar. "Improved Cost-Effective Technique for Resource Allocation in Mobile Cloud Computing." In Progress in Computing, Analytics and Networking, pp. 551-558. Springer, Singapore, 2018.

[6] Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. "A brief history of the Internet." ACM SIGCOMM Computer Communication Review 39, no. 5 (2009): 22-31.

[7] Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. "A brief history of the Internet." ACM SIGCOMM Computer Communication Review 39, no. 5 (2009): 22-31.

[8] Jadeja, Yashpalsinh, and Kirit Modi. "Cloud computing-concepts, architecture and challenges." In 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), pp. 877-880. IEEE, 2012.

[9] Goran Novkovic “Cloud computing's characteristics and benefits include on-demand self-service, broad network access, and being very elastic and scalable” nov 2017.

[10] Kumar, Sanjay, Syed Akbar Abbas Jafri, NishitArun Nigam, Nakshatra Gupta, Gagan Gupta, and S. K. Singh. "A New User Identity Based Authentication, Using Security and Distributed for Cloud Computing." In IOP Conference Series: Materials Science and Engineering, vol. 748, no. 1, p. 012026. IOP Publishing Ltd., 2020.

[11] Widyastuti, Dwininta, and Irwansyah Irwansyah. "Benefits and challenges of cloud computing technology adoption in small and medium enterprises (SMEs)."Bandung Creative Movement (BCM) Journal 4, no. 1 (2018).

[12] Odun-Ayo, Isaac, Olasupo Ajayi, and Sanjay Misra. "Cloud computing security: Issues and developments." (2018): 175-181.

[13] MKumar, P. Ravi, P. Herbert Raj, and P. Jelciana. "Exploring data security issues and solutions in cloud computing." Procedia Computer Science 125 (2018): 691-697.

[14] Maes, Stephane H., Rajeev Bharadhwaj, Travis S. Tripp, Kevin Lee Wilson, Petr Fiedler, and John M. Green. "Cloud application deployment." U.S. Patent 9,923,952, issued March 20, 2018.

[15] Agrawal, Gunjan. "A Survey on the “Visiosn of Cloud Compuiting–Its Referential Architecture Characteristics and Applications”." Journal Current Science 20, no. 1 (2019).

[16] Vaishnnave, M. P., K. Suganya Devi, and P. Srinivasan. "A Survey on Cloud Computing and Hybrid Cloud." International Journal of Applied Engineering Research 14, no. 2 (2019): 429-434.

[17] Khurana, Sumit, and Anmol Gaurav Verma. "Comparison of cloud computing service models: SaaS, PaaS, IaaS." International Journal of Electronics & Communication Technology IJECT 4 (2013).

[18] Liao, Yongxin, Fernando Deschamps, Eduardo de Freitas Rocha Loures, and Luiz Felipe Pierin Ramos. "Past, present and future of Industry 4.0-a systematic literature review and research agenda proposal." International journal of production research 55, no. 12 (2017): 3609-3629.

[19] Imran Ashrafa a Department of Information Technology, University of The Punjab, Gujranwala Campus, Pakistan “An Overview of Service Models of Cloud Computing” Accepted 15 Aug 2014, Available online 27 Aug 2014, Vol.2 (July/Aug 2014 issue)

[20] Siddiqui, Shams Tabrez, Shadab Alam, Zaki Ahmad Khan, and Ashok Gupta. "Cloud-Based E-Learning: Using Cloud Computing Platform for an Effective E-Learning." In Smart Innovations in Communication and Computational Sciences, pp. 335-346. Springer, Singapore, 2019.

[21] Molnar, D. and Schechter, S. “Self hosting vs. cloud hosting: Accounting for the security imp act of ho sting in the cloud”, In Proceedings of the Ninth Workshop on the Economics of Information Security (WEIS), 2010.

[22] Akhawe, D., Barth, A., Lam, P. E., Mitchell, J.C. and Song, D. “Towards a formal foundation of web security”, CSF, pp. 290-304,2010.

[23] Youngmin, J. and Mokdong, C. “Adaptive security management model in cloud computing environment”, In the 12th International Conference on Advanced Communication Technology (ICACT), pp 1664-1669,2020.