www.ijaceeonline.com ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 9, September 2020, pp. 1–9

Analysis and Implementation DoS Spoofing Attacks in the Cloud Computing Environment

Huda Basim Hamid
PG Scholar, Computer Engineering department, Mosul University, Iraq
Email: h.basim9h@gmail.com

Turkan Ahmad Khaleel
Senior Lecturer, Computer Engineering Department, Mosul University, Iraq
Email: turkan@uomosul.edu.iq

Abstract: *Cloud computing has been widely mentioned due to its resonated with its benefits and services; while the security issues have reduced its adoption in a wide manner. These issues include data security, confidentiality, location, etc. Security is the first cloud challenges. Denial of Service attacks often using Internet Protocol (IP) spoofing to encapsulate its attack; which depends on depletion of resources allocated to the legitimate users. Resources may be bandwidth, availability, response speed, storage capacity, and others. Therefore; DoS is the most dangerous and most prominent attack on the cloud environment and the Internet. Simulation Programs often do not provide attacker tools; here, began the idea to configure an IP Spoofing attacker using the OPNET Modeler 14.5A simulation program (one of the most prominent simulation programs for distributed networks and systems). And then, some analysis was performed to detect this attack.*

Keyword: *Attack Tool; Cloud Computing; DoS Attack; IP Spoofing; Network Security;*

1. INTRODUCTION

Cloud is a technology that transfers the applications, processing, and storage space from traditional computers to servers via the internet, these transfers the programs of Information Technology (IT) to services instead of products. Its infrastructure relies on advanced data centers, which offer some programs as services to the customer and provide large storage space for them. The most basic cloud features are self-service on-demand, resource allocation, and flexible handling, etc. [1].

Although the cloud is widespread, technological challenges will loom in the future. The most important challenges begin with the site, infrastructure, management, and organization; and may not end with information's privacy and confidentiality, which is the most important and worrying factor [2].

The most important security issue in the cloud is Spoofing Attack; "Spoofing" means an ironic trick. So: in the IT world, it refers to fooling computer systems and users, usually by hiding the identity of the sender, while using another user's identity on the Internet [3]. This attack involves malicious intent by attackers who deliberately conceal their identity to access client information, or maybe the source of viruses or malicious software, or even floods the target with counterfeit packages and stops its response [4] [5]; this leads the subsequent physical and security damage and commercial reputation. This attack is often encapsulated by Denial of Service (DoS) or Distributed Denial of Service (DDOS), after gets an Internet Protocol (IP) of the legal user, and poses serious attacks to the Internet in general and the cloud in particular [3].

Simulation programs are those computer programs that represent or mimic the existing or intended real system, A Simulation is a very important tool because of the cost-saving (during the design stages), Study complex networks, observe changes that may occur, then study the system clearly with the various circumstances and variables and expected future results, which is reflected on the efficiency of work. Briefly, it is testing the network before actually experimenting on the ground. It is worth mentioning; this research depended on a program called "OPNET Modeler 14.5 A", which is a large and great simulation program for communication and distributed networks [6].

This paper is organized as the first section is for Introduction, while the second section discusses some background about the attacker and some attacks' type and literature review. The methodology of the simulation is in the third section, moreover, the results and its discussion are put in the fourth, finally, the fifth section is the conclusion and future works.

Cite this paper:

Huda Basim Hamid, Turkan Ahmad Khaleel, "Analysis and Implementation DoS Spoofing Attacks in the Cloud Computing Environment", International Journal of Advances in Computer and Electronics Engineering, Vol. 5, No. 9, pp. 1-9, September 2020.

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 9, September 2020, pp. 1–9

2. BACKGROUND

Spoofing: (in general) is an attempt to make someone believe something wrong, in networks; is a trick in which a message is sent from an anonymous source (often a malicious element) disguised as a known source at the receiver, it is the most common in communication mechanisms that lack a high level of security [7], as in Figure 1.

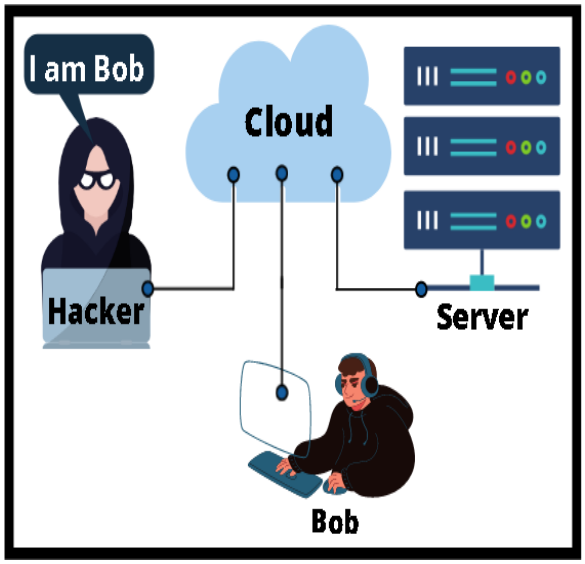

Figure 1 Spoofing

Spoofing is considered as non-harmful itself unless it caused a block or module the legal user or costumer's contents and/or data or use his credit card.

This type of attack always launch with another attack called "Denial of Service (DoS)"; In this type of attack, the attacker sends useless packets to the victim or use the resources desired by flooding a network [8], consumption the bandwidth, file space, or traffic, etc. [9], it causes the inability of the victim to respond, and became out of the work partially or completely; depending on the strength and magnitude of the attack and the number of attackers [4], Figure 2 shows the procedure of this attack.

DoS targets shared resources among users, so the Internet and cloud environments are favorable for this attack [10]; especially, the operating system notes the high workload on the service after a long period of work under this attack. Thus, to succeed in the attack, an attacker has hacked only one server (unnecessary all servers at cloud) to perform a complete loss of availability in the intended service [11]. Since the attack targets resources, an attempt to increasing these resources may mitigate the impact of the attack, but resources will be wasted and subsequent financial losses [2].

Do not forget to mention one of the most widespread attacks across the Internet, called Distributed Denial of Service (DDoS) as in Figure 3, It is a type of DoS with multiple attackers (up to several hundred or thousands), to sink the victim into requests that eventually lead the victim being out of service, in other words, targeting the availability of the system [8][12].

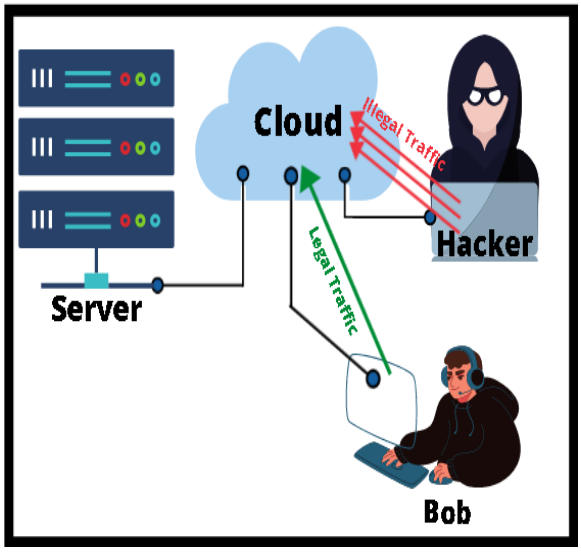

Figure 2 Denial of Service (DoS) Attack

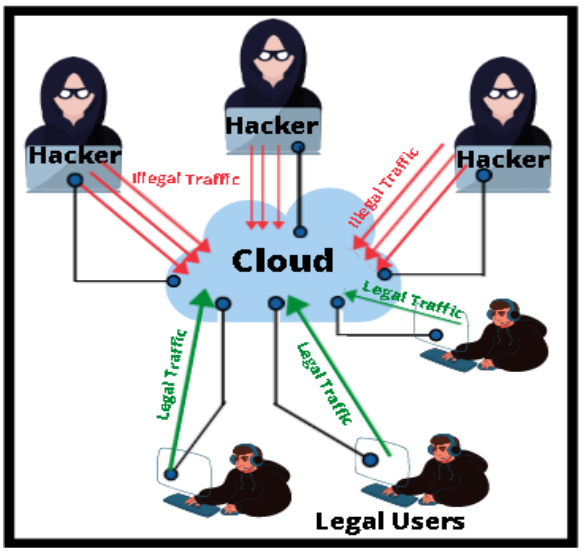

Figure 3 Distributed Denial of Service

Spoofing Attacks can be classified into three main categories depending on the nature of their launching and routing on behalf of victims (clients, data centers, or even servers). The main purpose of spoofing attacks is destroying or depleting resources [13]. Next, we briefly discuss these types of spoofing malicious attacks.

2.1.1 Hiding Attacks

Here the attacker tries to send a large number of packets simultaneously, by using fake addresses. This causes additional load at the recipient site, that needs more queuing, packet processing, delay, and so on Figure 4 shows an example of a hiding attack.

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 9, September 2020, pp. 1–9

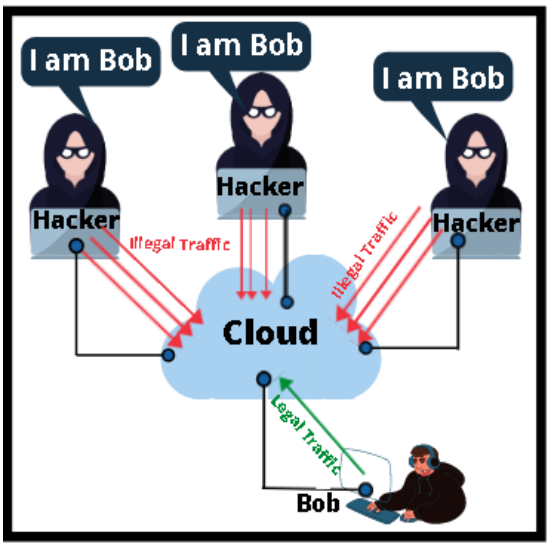

Figure 4 Hiding Attack

2.1.2 Reflection Attack

In this case, the attackers will send fraudulent packets using a fake IP server address. This causes unwanted responses that reach the target (legal user), thereby increasing the flooding rate, as in Figure 5.

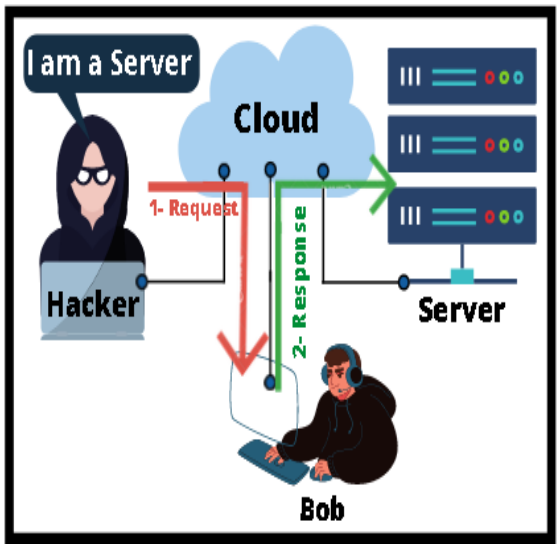

Figure 4 Reflection Attack

2.1.3 Impersonation Attack

The attackers here send an impersonation packet has an IP address of legitimate user, and they will behave as a legal user. The impersonation attacker sends requests firmly using the client's IP address and route them to the target completely like a legal user. On the other hand, the target replies the legitimate user's address, as Figure 6.

The main difference between the hiding attack and Impersonation Attack is the Attackers' goal of hiding attack is to flood the server with non-useful packages and reach it out of manner by exhausting the traffic, memory, queuing, and processing mechanisms; While, the Attack aims to make the legal user be confused with responses of servers that he did not ask it also pay for those requests anyway; therefore, the hiding attack affect the server in the cloud, but, Impersonation attack affect the client of a cloud.

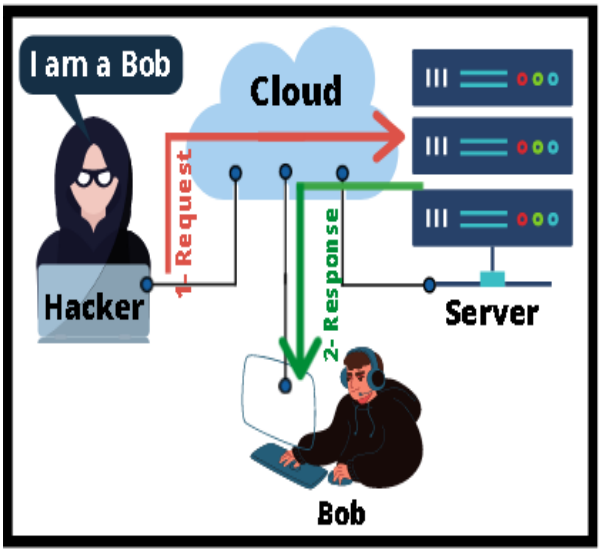

Figure 6 Impersonation Attack

2.2 Literature Review

Academic schools, Economic platforms, etc. highly related nowadays our life with cloud computing; therefore studying tries to scope the holes that affected these environments and penetration the clients ' information, to overcome somehow these vulnerabilities. Below some papers that discuss IP spoofing and the methods, they used to countermeasure it.

In reference [14], the authors used the Hop-Count Defense(HCF) Mechanism and created a table that matches the IP addresses with the Hop Count (which is constructed from TTL field of IP packet) and tests every incoming message that comes to the cloud, but they used static addresses to whole the field itself and it covers the preventing strategy.

P. Indu and et al. create an enhancement to the HCF method by adding TCP port numbers, in addition to the Basic HCF's method's contents (IP addresses and hop count values). the detection has been well noticed. as in reference [15], in 2017.

In [16], the authors adopted the Improved Hop Count Strategy, which requires to build the table called Add2HC that contains the IP address, TCP or UDP port number, and the latest device (immediately before the cloud) Physical address, furthermore the Hop Count values for each packet received in the cloud or leave it. Furthermore, the strategy depends on the Identification Number for each legal client that use the cloud, it added in the optional field of IP header, to distinguish between the registered user and the non-registered one.

"Natalija" Andet al. in 2019 published their paper that discusses real cloud service providers and ex-

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 9, September 2020, pp. 1–9

plains that Over 50% of them do not protect cloud users from IP spoofing. Finally, they pitch their study results to some real-world public cloud service providers. It showed that statistically speaking, the majority of public cloud service providers do a good job of preventing impostors from using those servers to launch fraudulent IP campaigns, however, they discovered that public cloud service providers could easily become the target of phishing IP packets themselves, or in the worst case. Impact on internet infrastructure, as in [17].

While Subrina Sultana and et al. in the source [18], discussed how to detect and prevent IP spoofing by every TCP / IP packet sent/received over the cloud, packets are scanned based on a modified HCF algorithm, which relies on extracting "SYN flag, TTL, source port, and source IP's information" from these monitored TCP / IP packets. Firstly, the algorithm checks the SYN flag then the IP2HC table with the incoming packet information if they match, It is considered a safe packet. else If the source IP address is included in the table IP2HC then the calculated hop value and the source port for this packet are checked in the IP2HC table. Then, If the information matches the tables, the package will be allowed to further process. Otherwise, the system will update the source port and the number of hops corresponding to the IP address in the IP2HC table. Finally, If the source port and/or the number of hops does not match the tables' content, hence the system considers this packet to be malicious and ignores the packet.

3. PROPOSED SIMULATION OF ATTACKER TOOL

This section deals with how to create and implement an Internet Protocol spoofing programmatically, using the OPNET Modeler 14.5A simulation program. With a brief explanation of the additions made to the program.

3.1 Attack Tool

Although the OPENT simulation program has extensive capabilities, it provides most of the tools needed by the researcher to complete his research, but he lacks the tools of attack. This is the main purpose that prompted the researcher to adopt the idea of creating a tool representing the IP address Spoofing Attack.

The idea of creating and implementing a node representing the attacker, after relentless attempts to find out how to carry out a spoofing attack by using Simulation Program, by supposing adding one data structure, and several functions for reading and/or writings, executing the process of switching Internet addresses before sending packets to its destination. Initially, Adding the node attributes acts as an interface between the higher layer (Network Model) and lower layer (Process Model) to read the node name, deduce the node's IP address, determine the start time of the attack, and the type of IP version, and finally specifying the detection and Prevention of attack., to create a new node, follow the following path:

Topology (from Menu Bar) → *Create Custom Device Model.*

Then start creating an “Attack Tool” by selecting the node, its name, image icon, and set different Models as in Figure 7. Then, determine the attributes of the created node (Explained in section 2.1), finally, add the data structure of this tool and other related functions (as in section 2.1).

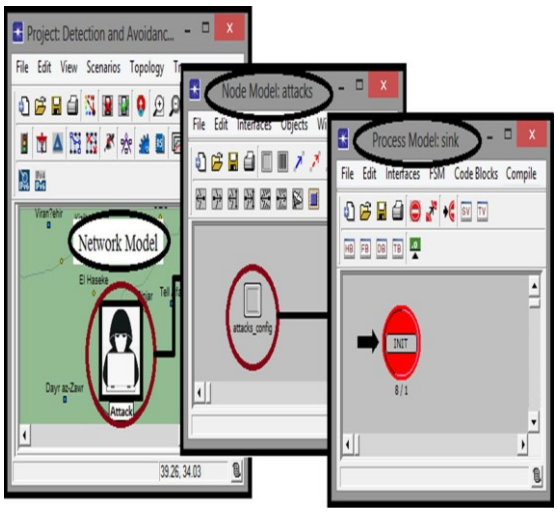

Figure 7 Attack Tool at various OPNET models

3.2 Attack Tool Attributes

Firstly, the ‘Attack Tool’ needs to define attributes and characteristics described in Figure 8. These attributes act as interfaces between the “Network Model” and the “Process Model”. In other words, the user-defined attributes defined at the middle model “Node Model”, which is intermediate between the upper layer (dedicated for the researcher) and lower layer (dealing with the code), “Process Model” is the place dedicated to write code and explain data processing procedure by implementing algorithms, and /or modifying protocols [113].

The attributes contained in the ‘Attack Tool’ can be defined as “Node Model” by following this path and at two stages:

Stage 1: *Node Model → Interfaces (Form menu Bar) → Model Attributes.*

Stage 2: *Attacks_config (Right-click) → Edit Attributes → Extended Attrs.*

Then, add the attributes to define the researcher’s requirements and facilitate the study of the spoofing attacker behavior and the response of the whole net-

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 9, September 2020, pp. 1–9

work to detection and preventing mechanism that has been chosen by the researcher or network layer's user as shown in TABLE I.

TABLE I THE ATTACK TOOL ATTRIBUTES PURPOSES

Attribute	Variable type	Purpose
IP Version	String	This option compares between IPv4, IPv6. The quality of the response is determined accordingly.
Attack Status	Boolean	If **Enabled**: An attack is within the network, or **Disabled**: There is no attack.
Attack Type	String	Compares the IP spoofing (in section 2.1), if Hiding, Reflection or Impersonation Attack.
Detect and Prevent Status	Boolean	In the case of **Enabled**: The existence of an attack and activate the mechanisms and methodology of detection and prevention adopted in this study, while **Disabled**: refers no detection or preventing method.
Start Time	Double	Specifies the start time that hacker began the attack. It is measured in seconds.
Attack Address	String	Address of the Attack Address that steals the Victim Address and routes the packets towards the Target Address. It should be mentioned here that the address must be according to the type of network whether it is a flat or subnet. The subnet name must be used.
Target Address	String	
Victim Address	String	

After defining the required properties, we need to specify a flow chart that explains the detail of how to configure the attacker's tool, as in Figure 9

The flowchart of the *Attack tool* shows the functions and data structure needed to construct an 'Attack Tool's node' (shown in Figure 9). The following is a brief description of each function:

- ***define_specific_node ()***: This is the Data Structure; identifies the names, addresses, IDs of the contract, start-up time, and detection and prevention status. This data structure should be written at one of the Headers; it should facilitate reading and writing purposes.

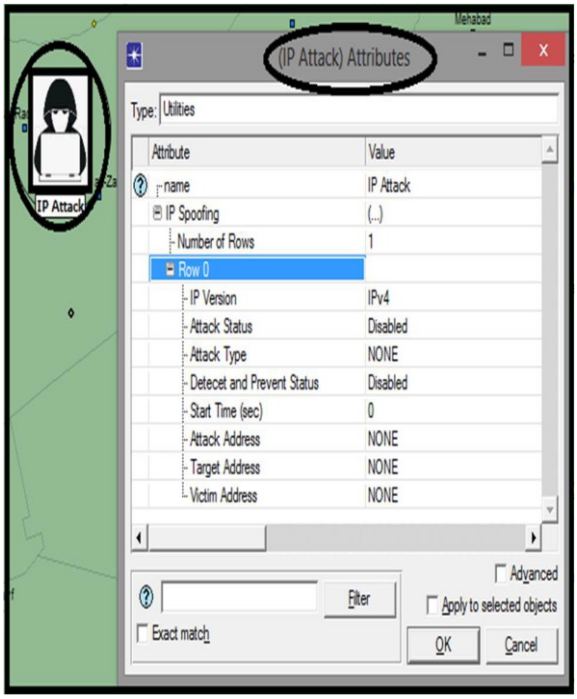

Figure 8 Attack Tool Attributes

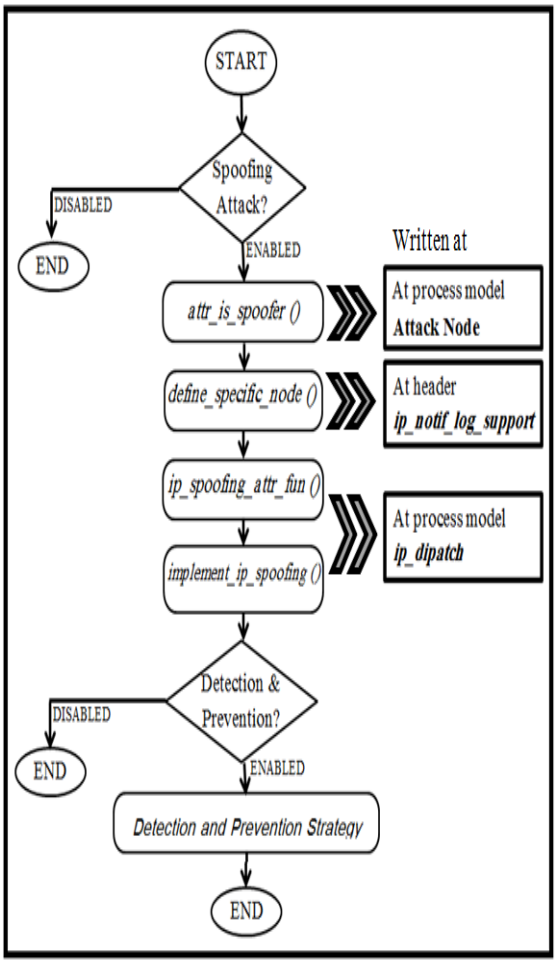

Figure 9 Attack Tool Flowchart

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 9, September 2020, pp. 1–9

- ***attr_is_spoofer ()***: This is a function that is written in the new tool created "Attack, Function Block-FB". This function acts as a reader for all features of this attack. These properties, after being read, are stored in the data structure ***define_specific_node ()***.

- ***ip_spoofing_attr_fun ()***: This function is written in a process called ***'ip_dispatch_Function Block'***. This function serves as a reader for all nodes in the network; when you pick up the Target, Victim or Attack, (IP address), and the ID (ID) and then store this information in the data structure, ***define_specific_node ()***.

- ***implement_ip_spoofing ()***: This function changes the source address in each packet issued in the attacker node with the victim's address and sets the packet destined to the target address when the start time of the attack starts. Add to represent the types of attack mentioned (in section I, C) represented in this document.

- While the ***strategy of detection and prevention*** is a strategy adopted by the author is explained in [16], or any other strategy adopted by the researcher.

4. EXPERIMENTAL SETUP

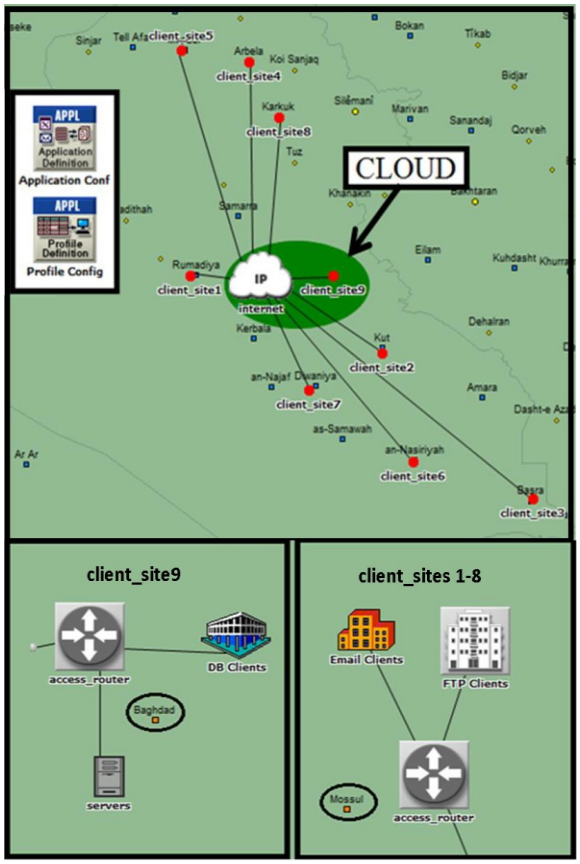

Figure 10 Proposed network

The proposed network is to create a cloud for the Ministry of Higher Education in Iraq. The cloud center is located in Baghdad (the capital); Includes a server that provides Email, Database, and Files services to clients (whose distributed in other governorates) with Database clients; as well as eight sites located in the rest of the governorates, which includes both File and Email clients. Figure 10 shows the proposed network

5. RESULT AND DISCUSSION

This section is performing network analysis. There are three scenarios configured and ran as follows: the first scenario 'without a spoofing attack', and the second one 'with a spoofing attack' the third using 'with detection and prevention strategy', While the routing protocol as RIP (Routing Information Protocol).

It is worth mentioning, that the IP address of 'Network.client_site9_DB clients' is theft by the attackers 'Network.client_site5.Hacker'. The 'Attack Tool' attributes are set as in Figure 11.

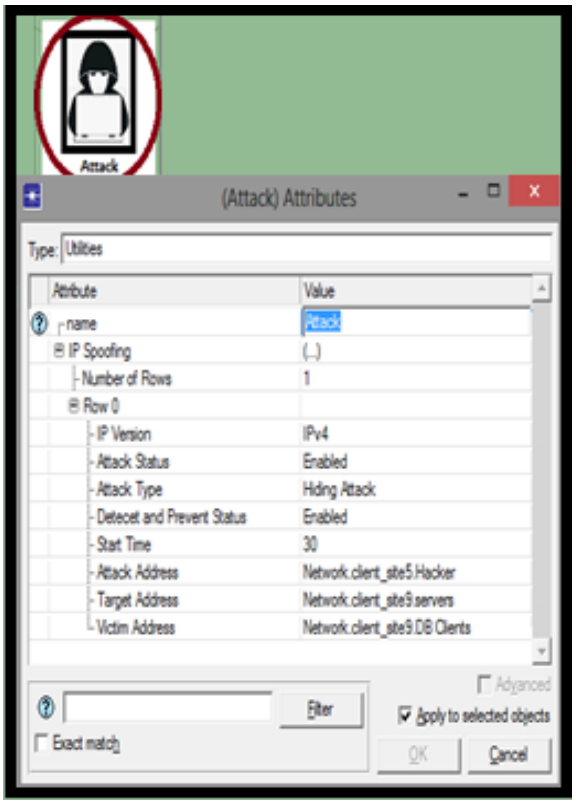

Figure 11 Proposed attributes of Attack Tool

5.1 DES Log Messages

After running the second and third scenarios (which were: 'with a spoofing attack' and 'with detection and prevention strategy'), some warning messages will have appeared, these messages called DES Log. After further going deeply, these messages clearly explain that there are two workstations in the network have the same IP address (shown in Figure 12, 13).

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 9, September 2020, pp. 1–9

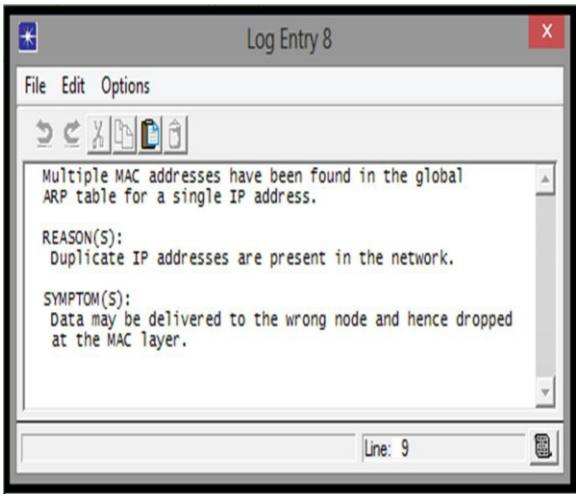

Figure 12 DES Log message Warning

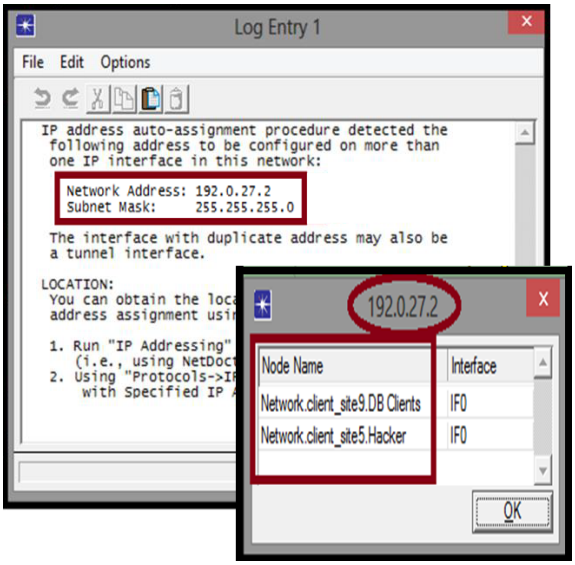

Figure 13 DES Log message shows Duplicate IP address and tracking this Address

5.2 Database Query Traffic

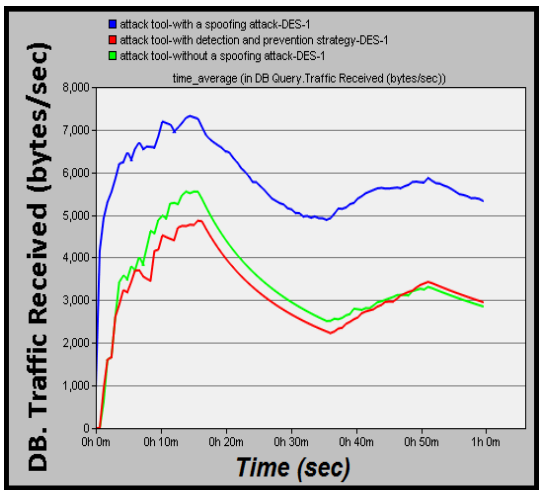

Figure 14 Traffic Received (bytes/sec).

In terms of sending and receiving traffic of the DB(Database) application (as shown in Figure 14, 15); Note that in the second scenario (when the network under the attack), noticed that the traffic was increased compared to the traffic in the first scenario 'without a Spoofing Attack at the network' or third one 'with detection and prevention strategy', While the scenario 'with detection and prevention strategy' the traffic appears more closely as first one; in other words, the attack is blocked [1].and the traffic went smoothly.

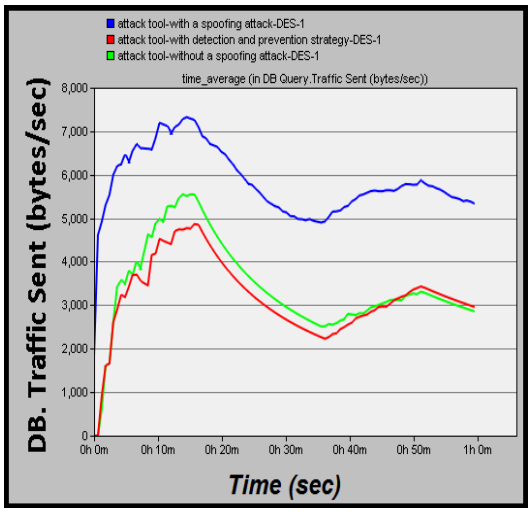

Figure 15 Traffic Sent (bytes/sec)

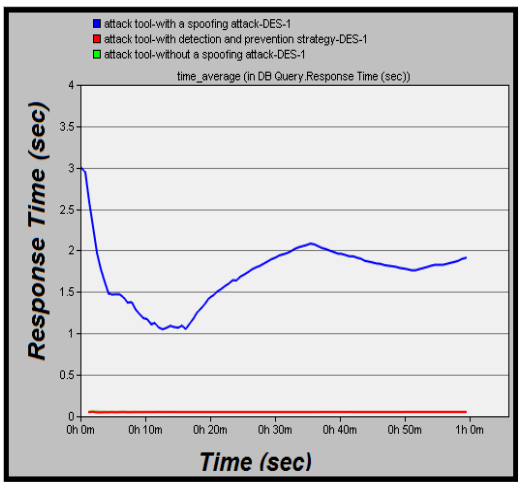

Figure 16 Database Response time

DB response time: is the overall time amount is taken by the server when responding to a user request. The response time appears in Figure 16 is very close for the first and third scenarios, while the response time in the second scenario is very high due to the

[1]This paper focused on the databases because the attacker steals the address of the database clients, in addition; the purpose of adding the detection process does not appear the detection mechanism clearly as much as intends to highlight the DoS IP Spoofing attack which implement in the 'Attack Tool'.

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 9, September 2020, pp. 1–9

large number of plagiarism packets sent from the attacker node 'Network.client_site5.Hacker' to the server that causes waste time in processing, queuing time.

Also, you can see the response time of the first and third scenarios is the same, this refers that the network recovers itself without the need of any waste time after the detection mechanism which is done in the cloud.

5. CONCLUSION AND FUTURE WORK

In this paper, a static node was created with defining its specific data structure and functions, this 'Attack Tool' can receive the required information to implement IP Spoofing procedures, instead of the other ways to propagate defined attributes at each node, or even the restriction using a static or/ and manually addresses. That is easier and faster and also suitable for any network of any size, and executable in wired and wireless networks.

In other words, using this added 'Attack Tool' with its functions to a specific location will cause the purpose of executing the spoofing attacks by rigging the requested source address.

Also, the Spoofing Attacks that launch with DoS/DDoS Attack has affected the traffic, queuing and response time in the network that slows down it, furthermore, the detection and prevention mechanism that related to the Improved Hop Count Filtering (IHCF) return the network's response to right flow.

For future work, expanding the implementation of various types of spoofing attacks such as Spoofed DDoS, Web Service Addressing Spoofing, ICMP Spoofing, or Metadata Spoofing. And try to mix between IHCF and Route Based detection and prevention mechanism.

REFERENCES

[1] Chamandeep Kaur, (2020). "The Cloud Computing and Internet of Things (IoT)" International Journal of Scientific Research in Science, Engineering and Technology, Vol. 7, Issue. 1, pp. 19-22.

[2] Rashmi V. Deshmukh, Kailas K. Devadkar, (2015) "Understanding DDoS Attack & Its Effect In Cloud Environment". Digests International Conference on Advances in Computing, Communication and Control (ICAC3'15), pp. 202-210.

[3] Tanmay A. Abhang, and Uday V. Kulkarni, (2013). "An Integrated Approach to Detect and Limit IP Spoofing" International Journal of Computer Science and Mobile Computing (IJCSMC), Vol. 2, Issue. 7, pp.59 – 65.

[4] Gaurav Somani, Manoj S. Gaur, Dheeraj Sanghi, Mauro Conti, and Rajkumar Buyya,(2017). "DDoS Attacks in Cloud Computing:Issues, Taxonomy, and Future Directions" Elsevier B.V., Vol. 107, pp. 30-48.

[5] Poonam Yadav, and Sujata, (2013). "Security Issues in Cloud Computing Solution of DDOS and Introducing Two-Tier CAPTCHA" International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol. 3, Issue. 3, pp.25-40.

[6] Sonika, Anshu Arora, Kuldeep Vats, and Nisha Rani, (2014). "OPNET based Investigation and Simulation Evaluation of WLAN Standard with Protocols using Different QoS" International Journal of Computer Science and Mobile Computing (IJCSMC), Vol. 3., Issue. 6, pp.852 – 861.

[7] Saroj Rani, Er. Abhilasha , and Er.Swati Jindal, (2015). "Implementation and Analysis of Identity Spoofing Attack Using Epidemic Routing Protocol in DTN" International Journal of Current Engineering and Scientific Research (IJCESR), Vol. 2, Issue. 12, pp. 2394-0697.

[8] Naseer Amara, Huang Zhiqui, and Awais Ali, (2017), "Cloud Computing Security Threats and Attacks with their Mitigation Techniques" International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 244-251.

[9] Frederick Carlson, "Security Analysis of Cloud Computing". Date:[April, 2014], online available at: https://www.researchgate.net/publication/261952355_Security_Analysis_of_Cloud_Computing

[10] Raja Mohamed Jabir, Salam Ismail Rasheed Khanji, Liza Abdallah Ahmad, Omar Alfandi, and Huwida Said, (2016), "Analysis of Cloud Computing Attacks and Countermeasures" 18th International Conference on Advanced Communication Technology (ICACT), ISBN:978-8-9968-6506-3).

[11] Monika Malik, and Dr. Yudhvir Singh, (2017), "A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing" Computer Engineering and Engineering Software, Vol. 9, Issue. 6, pp. 1-19.

[12] Akash Mittal, Prof. Ajit Kumar Shrivastava, and Dr. Manish Manoria, (2015) "A Review: DoS and DDoS Attacks" International Journal of Computer Science and Mobile Computing (IJCSMC) , Vol. 4, Issue.4 , pp. 260 – 265.

[13] N. Jeyanthi, and N.Ch.S.N. Iyengar, (2012), "Packet Resonance Strategy: A Spoof Attack Detection and Prevention Mechanism in Cloud Computing Environment". International Journal of Communication Networks and Information Security (IJCNIS), Vol. 4, Issue. 3, pp. 163-173.

[14] Shahid Akhter, J.Myers, Chris Bowen, Stephen Ferzetti, P. Belko, Vasil Hnatyshin, "Modeling DDoS Attacks with IP Spoofing and Hop-Count Defense Measure Using OPNET Modeler". Date:[2013], online available at: https://www.semanticscholar.org/paper/Modeling-DDoS-Attacks-with-IP-Spoofing-and-Defense-Akhter-Myers/4056bf0822358cfb908f4ca42815b51850425507

[15] P. Indu, Shalom Elza Joseph, M.C. Sreelakshmi and T. RemyaNair, (2017), "Enhancement of HOP Count Filtering Mechanism-An ANTI-IP Spoofing Technique" International Journal of Pure and Applied Mathematics, Vol. 114, Issue. 12, pp. 51-58.

[16] Huda Basim Said, and Turkan Ahmed Khaleel, (2018), "An Improved Strategy for Detection and Prevention IP Spoofing Attack" International Journal of Computer Applications, Vol. 182, Issue.9 , pp.28-31.

[17] Natalija Vlajic, Mashruf Chowdhury and Marin Litoiu, (2019), "IP Spoofing In and Out of the Public Cloud: From Policy to Practice" Multidisciplinary Digital Publishing Institute (MDPI), Vol. 8, Issue. 4.

[18] Subrina Sultana, Sumaiya Nasrin, Farhana Kabir Lipi, Md Afzal Hossain, Zinia Sultana and Fatima Jannat, (2019), "Detecting and Preventing IP Spoofing and Local Area Network Denial (LAND) Attack for Cloud Computing with the Modification of Hop Count Filtering (HCF) Mechanism" International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2).

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 9, September 2020, pp. 1–9

Authors Biography

Huda Basim Said, graduated from the University of Mosul, Iraq/ College of Engineering/ Computer Engineering department at 2012/ then she holds master degree from the same department at 2019, in Computer Engineering. work as a freelancer and Microworker, furthermore, her researches care about Cloud Computing and Security in it.

Dr. Turkan Ahmed Khaleel received the B.Sc., the M.Sc. and Ph.D. degree in Computer Sciences from Mosul University, Mosul, Iraq, in 1993, 2002, and 2013, respectively. She was a Lecturer with Computer Engineering Department, Mosul University, Mosul, Iraq, Her research interests include remote sensing Image Processing, computer networks, IoT, and network security.

Cite this paper:

Huda Basim Hamid, Turkan Ahmad Khaleel, "Analysis and Implementation DoS Spoofing Attacks in the Cloud Computing Environment", International Journal of Advances in Computer and Electronics Engineering, Vol. 5, No. 9, pp. 1-9, September 2020.