SECURITY ARCHITECTURE OF CLOUD NETWORK AGAINST CYBER THREATS

Mohammad Faisal[1], Attiq-Ur-Rehman[2], Samina Naz[3], Zahida Perveen[3]
[1]Department of Computer Science, University of Malakand, KPK,
mfaisal@uom.edu.pk/mfaisal_1981@yahoo.com
[2]SZABIST Islamabad, Pakistan,
attiqbaluch@gmail.com
[3]Department of computer science the university of Hail. Hail, KSA,
s.naz@uoh.edu.sa, z.malik@uoh.edu.sa

ABSTRACT: *Cloud computing is contemporary technology in which services are provided in the form of infrastructure, software, and platform. Cloud computing enables the users and clients to remotely access the server(s) and avail numerous services on a demand basis. Cloud Computing is rapidly growing due to the cheapest cloud services in the form of Platform as a Service-PaaS, Infrastructure as a Service-IaaS, Software as a Service-SaaS and zero level maintenance cost for end-users. Various types of attacks may be launched to destroy the services or even to make them unavailable for the users. A few of the well-known attacks are Denial of Service-DoS, Distributed Denial of Service-DDoS attacks. In this paper, we propose a hybrid security model that will not only provide protection from DoS attack, DDoS attack, EDoS attack, but also will detect these attacks and generate the intrusion alarm. The study floats from a critical analysis of the already proposed solutions to the proposed solution through a proposed hybrid model. The proposed hybrid model will check and filter each generated request. After monitoring and filtering the behavior of requests, responses will be generated to the end-users. The proposed model will not only achieve the availability services but also will save the processing time and bandwidth usage also.*

Keywords: Cloud Computing, Cyber Threats, DoS Attack, DDoS Attack, E-DoS Attack, Denial of Service. Distributed Denial of Service.

I. INTRODUCTION

Cloud computing is a modern technology that provides unique services to the user with zero level maintenance. Cloud computing encapsulates all the latest technology services and provides resources via the web. Cloud computing is significant because it encapsulates a range of different technologies that have developed through the history of commercial computing. It is an important evolutionary step. The rise of the Internet, increasing bandwidth at the desktop and on the backbone, the movement towards outsourcing, the development of service-oriented architecture (SOA), mobile and wireless computing.

Cloud computing is a contemporary technology through which services are provided to users in the form of PaaS, IaaS, and SaaS. These services are provided in the web format to end-users. Intruders and competitors always try to launch different types of attacks to achieve the mission of laying down of availability of services so that end-users can't avail of the services on time. For instance, an intruder may try to launch a DoS and DDoS attack on a cloud service provider server, so that the server becomes so busy and can't respond to clients on a timely basis.

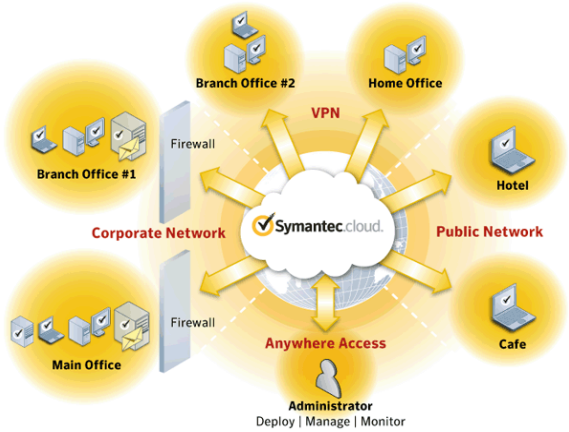

Figure 1: A Sample Cloud Security Model [7]

In cloud computing, services are provided to users instead of any product. Services are provided on a demand basis And customers are also charged on a demand basis. Services are provided in the form of software, platform, and infrastructure. The major objective of cloud service providers is to provide the services to users without any interruption and through a secure channel. Cloud computing is facing different types of threats and challenges. The ratio of threats and challenges are increasing day by day due to full control of client/users on the infrastructure of cloud service providers. DoS, DDoS attacks are commonly launched from intruder having the objective to interrupt the cloud services. Bandwidth is another major issue for cloud service providers because all services are provided through the internet that's why cloud services also become dependent on internet service providers so that they can also provide the services without any interruption and interval.

Cloud computing is a heterogeneous distributed cloud environment that accomplishes the virtual environment and provides cloud services to users in the form of PaaS, SaaS, and IaaS. The objective of the cloud service provider is always constant so that the availability service should be never compromised.

Users can access the recourses on a timely basis and secure communication sessions should be established between the cloud service provider and users. Security assurance in a cloud environment is a major challenge for a cloud service provider. Different types of security threats are involved in cloud computing i.e. DoS, DDoS, ID Management. The proposed security model is designed to protect from Denial of service attacks and to save the processing time, memory and also.

II. An Overview Of The Past Related Security Work

All the organizations are rapidly shifting their business to cloud networks due to its services and applications. Author Eman M.Mohamed et al [1] designed and implement a data security model on the base of cloud architecture. The data security model is designed to provide security at three levels. The first one is the security of data transmission, second is data security at the storage level and the third one is at data transmission to make sure the availability services and to protect from denial of service attack[8]. In a particular model, the software is designed and a list of eight encryption algorithms is predefined which can use any one of these on the base of high security in cloud architecture [9]. Designed model resolve the security problems and can't fully protect from Denial of service attack and distributed denial of service attacks. In this solution, the main focus is on confidentially and integrity but availability service is ignored [10].

To achieve CIA (Confidentiality, Integrity, Availability) services are the [2] major goal of cloud service providers. Among these services, the most important service in the cloud network is availability is the most important security service which is based on cloud infrastructure and has the largest challenge to date. In cloud computing where infrastructure is shared by potentially among millions of users, DDoS attacks have the potential to have a much greater impact than against single tenanted architectures. Denial of Service and Distributed Denial of Service is a type of attack that aims to make services or resources unavailable for an indefinite amount of time by flooding it with useless traffic. The objective of these attacks is to exhaust computer resources i.e. CPU processing time, Bandwidth so that it makes the service unavailable for end users. The second objective of these types of attack is to hide their identity from victim and attack from different system simultaneously so that maximum resources should be availed at a time and server become so busy that it can't respond to users. Distributed Denial of service attack aim is to make the services unavailable by sending indefinite unnecessary requests to the server [3].

Different types of tools and techniques are design to protect from these attacks and to make sure the availability services. A cloud traceback technique is one of these. In this type of method, the objective is to find the source of the attack. Research on the protection of DDoS attacks is in progress and various types of techniques are designed [4]. Major research is categorized into three areas. The first one is attack detection, attack filtering, and third one attack traceback. Confidence based filter process is introduced which filters each request on the nonattack period and attack period [11].

Flooding attacks on the network layer cause the extra usage of bandwidth and system resources also [5]. These types of attacks are launched through webpages. Semantic concepts and formulate grammar methods are used to detect the behavior of web pages so that malicious browsing can be detected. Flooding attacks are launched through malicious behaviors' and use extra resources such as bandwidth, processing, and memory [8-13].

III. Existing Security Model

The existing Security model is designed to provide the cheapest cloud services to users and make sure of the availability of services. These services are provided in the SaaS, PaaS, and IaaS. Cloud Model is also designed in three layers to make sure these services. These layers [6] are System Layer, Platform Layer and application layer Computing is an invention to support the organization to save the infrastructure cost. Due to the distributed environment of cloud services, various types of intrusion and attacks are involved. Various types of techniques and technologies are used to overcome and protect from cyber-attacks such as an intrusion detection system to protect from DoS and DDoS attacks. These IDS generate an alarm in case of finding any intrusion in the request. The predefined set of rules is prepared to filter the request and IDS evaluate the packets on the base of these rules. The multithread intrusion detection system has been proposed by the author which captures the traffic, analyzes and evaluates the traffic and report preparation on the base of analysis. The capture module receives the in-bound and out-bound data packets and captured data are sent for analysis purposes.

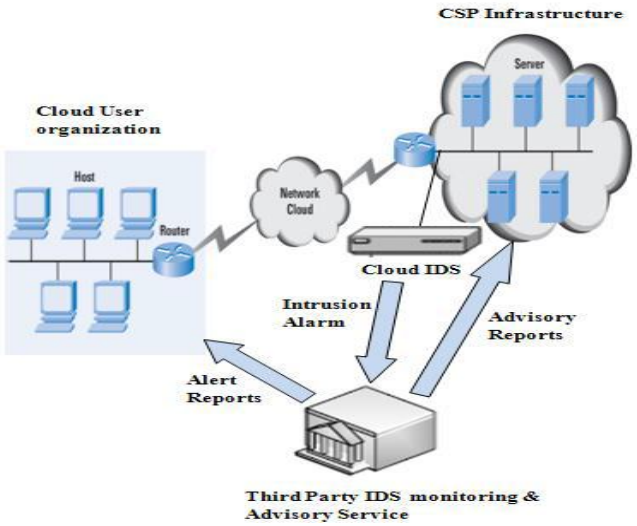

Figure 2: Existing Security Model Ref [6]

In this model, each time the request will be analyzed. If intruder launches a DDoS attack on a continuous basis than a multithread IDS model also continuously generates an infinite alarm, infinite reports, and another request will become so busy that all the services will be distressed and availability service will become down.

IV. Proposed Model

The proposed cloud security model is shown in figure 3 which is designed to provide the security from Denial of Service attack, Distributed Denial of Service attacks and prevent Electronic Denial of Sustainability. Designed Cloud security model provides the extra security feature and saves the usage of resources i.e. processing time, usage of memory and to save the bandwidth. According to the proposed model request analyzer filter the request and after verification

request passes to a cloud network for response and issuance of cloud services. Whenever the request analyzer will detect any intrusion/ continuously the same request is repeating it will sense that request is generating from an intruder on the behalf of clients than request analyzer will send the information of the particular client to the blacklist database and will add it. Now the request from a particular user will be blocked and new be checked again and again. After the interval set time period request analyzer will send the code generated from the database to detect the request is generating from human being clients or any intruder. If the client will enter the same code which was generated from the database than the request analyzer will establish a session and passed the request to the cloud network. The algorithm of the proposed model is categorized in two parts. In the first part, it gets the Message Authentication Code address with IP Address and store in the database. The second part processes the request accordingly.

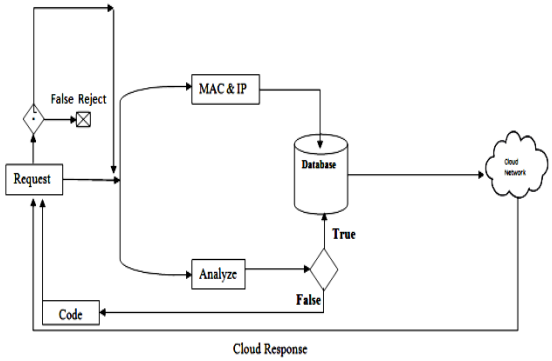

Figure 3: Proposed Cloud Security Model

Procedure GetMacAddress (m, wmi, e, s)
[Where m is the mac address of client machine, Wmi is used to store Windows Management instrumentation object, e-stores Enumerator object]
Step1: Call method GetObject("winmgmts:{impersonationLevel=impersonate}") and store object to wmi.
Step2: store e = new Enumerator (wmi.ExecQuery("SELECT * FROM Win32_NetworkAdapterConfiguration WHERE IPEnabled = True"))
Step 3: store s = e.item ()
Step 4: store m = s.MACAddress
Step 5: call e.moveNext() to iterate and Repeat step 3 and 4 untill e.atEnd() returns false.
Step 6: Check whether this mac address exists in analyzer db or not
Step 7: if mac address is not in analyzed then store m (mac address) in the analyzer database.
Step 8: store m in session
Step 9: End
Procedure to Process the Request
Procedure ProcessRequest (m, c)
[Where m is used to store macAddress, stores' count of macAddress in from db]
Step 1: Get mac address from session and store in m.
Step 2: Get the total count of the current mac address from analyzer db and store in c.
Step 3: Check from the analyzer database this mac-Address is not in blocked mac-Addresses.
Step 4: If c > 3 then block the request.
Step 5: Redirect the client to a verification page to enter the verification code
Step 6: if the verification code is correct then continue processing requests.
Step 7: if code is incorrect then call Response. End ()
Step 8: store this mac address in analyzer db in blocked mac-address.
Step 9: End

V. Comparison of Existing Model and Proposed Model On The Basis Of Performance and Security

The existing security model is compared with the proposed model on the basis of security and performances. In existing model requests sending to server from single thread and multithread and results are noted down. The existing model treats as a different for single thread and multithread request. The calculated result shows the existing system performance level becomes up for single thread and performance may down for multithread requests. It means that if intruder sends launch attacks from multiple threads and launch a DDoS attack, the existing system will become down. On the other side in proposed system attacks were launched from a single thread and multithread simultaneously. On this basis of results, it shows that the designed model treats as same for single thread and multithread. Performance may not down and detection/prevention speed also increased with the block of requests and secret stamp. Time stamp is the variable time period in which secret code is sent to the user to known that request is generating any human being or it is generated from an intruder to deny the services.

VI. Implementation of Proposed Model

The proposed cloud security model is designed and implemented to trace and prevent the DoS, DDoS attacks and to save the processing time, memory consumption and bandwidth usage. The proposed model is implemented in Centos 5, a flavor of Linux using .NET and SQL Database. The virtualation environment was created using VMWare by creating multiple workstations on a single node. This virtual machine can be run simultaneously and can connect to the internet. VMware allows assigning the unique IP address for each machine. The request analyzer machine was installed and configured in front of the cloud network, through which all requests are passed and then forwarded to the cloud network. Request analyzer machine is also configured with Centos 5 Operating System, .NET and SQL database to set the rules and store the logs/record of blocked hosts. To evaluate the functionality of the request analyzer, we launched multiple intrusion attacks on the target machine within the wrapper of request.
DOS attacks cause the flooding of traffic to victim and usage of the system and network resources i.e. consumption of processing speed, utilization of memory and declining of availability service. Intruder sends continuous same requests within a short time period of time to utilize the network and

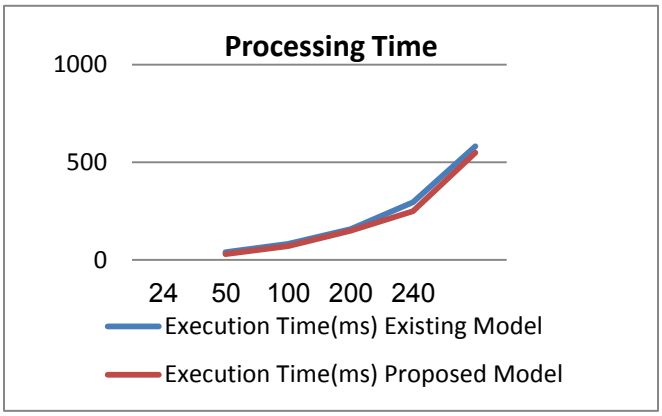

Figure 4: Comparison of Existing and Proposed Model

system resources so that it became so busy and can't respond to the user. The intrusion packet was sent to the server within the wrapper of requests. The test was conducted to evaluate the system resources for a single thread and multiple threads. First of all, attack launched in the form of a request from one machine and concluded the time, consumption of bandwidth, resources, etc. After that attack launched from multiple nodes and then calculates the network bandwidth and system resources. Results calculated from requests are shown in Figure 3 to evaluate the performance of the existing model and proposed model and shown in table 1.

Table 1 Comparison of Execution time

Data Size (KB)	Execution Time(ms) Existing Model	Execution Time(ms) Proposed Model
24	40	30
50	82	70
100	158	150
200	296	250
240	582	550

I

Table2BandwidthComparisoninMB

Data Size in KB	Existing Model Bandwidth Consumption in MB	Proposed Model Bandwidth Consumption in MB
1000	02	01
10000	10	06
100000	100	60
1000000	500	270

n proposed model execution time for filtration and prevention of requests is faster than the proposed results. For multithread requests including DDoS attacks were also calculated. The proposed Model execution time is lower than the existing model. Proposed model proof the fast execution time for single thread and multithread requests. The proposed model not only reduces the execution time but detection speed of attacks, prevention speed of attack is much better than the existing model. Bandwidth consumption for an existing model. and CPU consumption time was also calculated and tested. The proposed model reduces bandwidth because it filters the new requests twice a time instead of each time.

If DoS, DDoS is generating from the same hosts within a short period of time request analyzer block the requests for a specific period of time. In a particular period, it can't pass the specific and cant evaluate the requests which are generated from the same system. After an interval to know to verify the request a secret code is sent to the host to verify that the request is generating any human being or any intruder compromised the system and generating requests automatically. Bandwidth is also calculated for the existing model and proposed which is shown in figure 4 and table 2

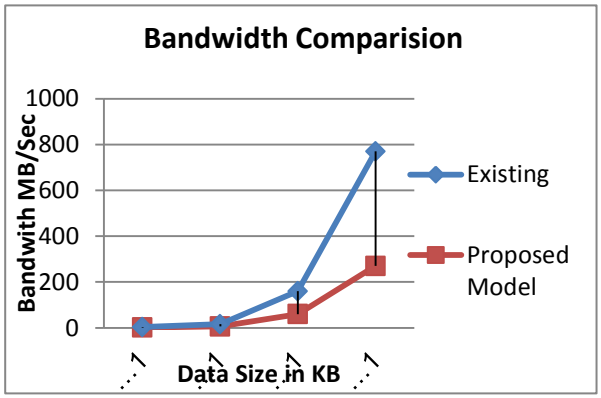

Figure 5: Bandwidth Comparison

Proposed model used to low bandwidth as compared to existing model. Existing model verify and filter the each request which is generated from the client and generate intrusion alarm and advisory report. The proposed model filter the request twice the time for each host. If the analyzer detects that request is continuously generating from the host with intrusion than the request analyzer block the host for a period of time. After an interval a secret token is sent to a particular host to check that request is generating from a human being any compromised machine. If a particular host verifies the secret token than the request analyzer checks the request for intrusion and passes to a cloud network. Bandwidth Comparison ratio is also shown in Figure which clearly indicates the performance of the proposed model.

VII. CONCLUSION AND FUTURE WORK

The proposed Cloud network security model is definitely a valuable model to protect from DoS, DDoS attack to save the bandwidth, processing time and memory. The proposed model of cloud network security is implemented and results are validated. The result discussed above shows the resultant improvement in processing time and bandwidth usage. It also shows that our implementation worked well in capturing packets on the base of analysis and resistance to attacks. In the future, we plan to enhanced the proposed model which will achieve all other security services i.e. Confidentiality, integrity, and authentication. We also plan to design hardware devices with the implementation of the proposed model. The particular device will be installed and configured dynamically according to the requirements of cloud service providers.

VIII REFERENCES

[1]. Eman M.Mohammed, Hatem.S.AbdelkaderEnhanced Data Security Model for Cloud Computing " , The 8th International Conference on INFOrmatics and Systems (INFOS2012) - 14-16 May Cloud and Mobile Computing Track.

[2]. Bansidhar Joshi , A. Santhana Vijayan , Bineet Kumar Joshi, "Securing Cloud Computing Environment Against DDoS Attacks" , 2012 Internation Conference on Computer Communication and Informatics (ICCCI-2012) , Jan 10-12,2012 Comibartore India.

[3]. P. Du, and A. Nakao, "DDoS Defense Deployment with Network Egress and Ingress Filtering," Communications (ICC), 2010 IEEE International Conference, 2010.

[4] Qi Chen, Wenmin Lin, Wanchun Dou , Shui Yu , "A Packet Filtering Method for DDoS Attack Defense in Cloud Environment " , 2011 Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing.

[5]. Chu-Hsing Lin , Chen-Yu Lee , A Detection Scheme for Flooding Attack on Application Layer Based on Semantic Concept.

[6]. Irfan Gul, M. Hussain , " Distributed Cloud Intrusion Detection Model " , international Journal of Advanced Science and Technology Vol. 34, September, 2011.

[7]. http://smallbusiness.norton.com/norton-sep-cloud.html

[8] Abbas, S., M. Faisal, et al. (2018). "Masquerading Attacks Detection in Mobile Ad Hoc Networks." pages 55013-55025, volume 6, September 2018, in IEEE access.

[9] Ali, I., M. Faisal, et al. (2017). "A Survey on Lightweight Authentication Schemes in Vertical Handoff." International Journal of Cooperative Information Systems Vol. 26, No. 1 (2017) 1630001 (18 pages) published in International Journal of cooperative information System, IJCIS.

[10] Faisal, M., S. Abbas, et al. (2018). "Identity attack detection system for 802.11-based ad hoc networks." EURASIP Journal on Wireless Communications and Networking 2018(1): 128.

[11] M Zeeshan, Khan, M. Z., H. U. Rahman, and M Faisal. "Performance Comparison of Structured Based Data Aggregation Schemes in Wireless Sensor Networks." Journal of Information Communication Technologies and Robotic Applications: 6-18.

[12] Faisal, M., S. Abbas, et al. "An Analysis of DDoS Attacks on the Instant Messengers." Security and Communication Networks 2019.

[13] http://smallbusiness.norton.com/norton-sep-cloud.html