A MULTI-LEVEL SECURITY FOR PREVENTING DDoS ATTACKS IN CLOUD ENVIROMENTS

Subramaniam.T.K[1*] and Deepa.B[2]

[*1]M.E.Scholar, Department of Computer Science & Engineering Nandha Engineering College, Erode, Tamil Nadu, India

[2]Assistant Professor, Department of Computer Science & Engineering, Nandha Engineering College, Erode, Tamil Nadu, India

ABSTRACT

Incredible and amazing growths in the meadow of extranet, internet, intranet and its users have developed an innovative period of great global competition and contention. Denial of service attack by several computers is accomplished of distressing the services of competitor servers. The attack can be done for various reasons. So it is a key threat for cloud environment. Distributed-Denial of Service (DDoS) is a key intimidation to network and cloud computing security. Cloud computing Network is a group of nodes that interrelate with each other for switch over the information. So security is the major issue. There are several security attacks in cloud computing. One of the major intimidations to internet examine is DDoS attack. It is a malevolent effort to suspending or suspends services to destination node. DDoS or DoS is an effort to create network resource or the machine is busy to its intentional user. Numerous thoughts are developed for avoid the DDoS or DoS. DDoS occur in two different behaviours they may happen obviously or it may due to some attackers.

KEYWORDS

DDoS, Security, botnets.

1. INTRODUCTION

Cloud computing is one of the technology which is deployed with the help of internet. It helps the business enterprises and business people to improve their business. The cloud computing consists of hardware and software property. The cloud computing property are virtualized and also programmed so that they can be easily accessible. Resources are given to the cloud user as payable model. The properties of cloud such as express provisioning, payable model, scalability, trustable, virtualized and wide system of network access has made business enterprises to acclimatize the cloud. The cloud computing tools also helps business enterprises to reduce their transportation cost, communication cost and equipped cost. The resources that are required for

DOI:10.5121/mlaij.2016.3202

every day operation of an industry can be access by end users of cloud. The end users of cloud are charged only for the resources that are used [1]. This kind of self-motivated allocation or on required allocation of resources is very useful for industries which have self-motivated infrastructure, where the property is needed only for certain period of time. Cloud computing employs networks of large group sectors of servers, which runs on running low cost consumer computer technology with specific connections.

Normally end users put their secret data and also non private data into cloud storage, so that the users can eventually decline their expenses on hardware resources as well as maintenance. Every time a record is moved into a cloud, the user's records become susceptible and vulnerable. At this position there is sheathing in security. In cloud computing environment, hardware infrastructure and software services are transported through the internet. Cloud computing consists of some of key quality such as Application programming interface (API), expenditure, locality freedom, trustable, scalability, maintenance, empower and protection [2].

2. CLOUD SERVICE MODELS

2.1. Software as a Service (SaaS)

The cloud service provider grant services to their end users. And with they can be able to deploy their end user applications on cloud environment. The cloud service gives licenses to the applications. The licenses are provided according to its users based on payable model or it may with non payable. SaaS was installed for sales, service force computerization and client association management. In addition to SaaS, this can also extensive for much business administration such as human resource organization, receipting, and economic administrative solutions [3].

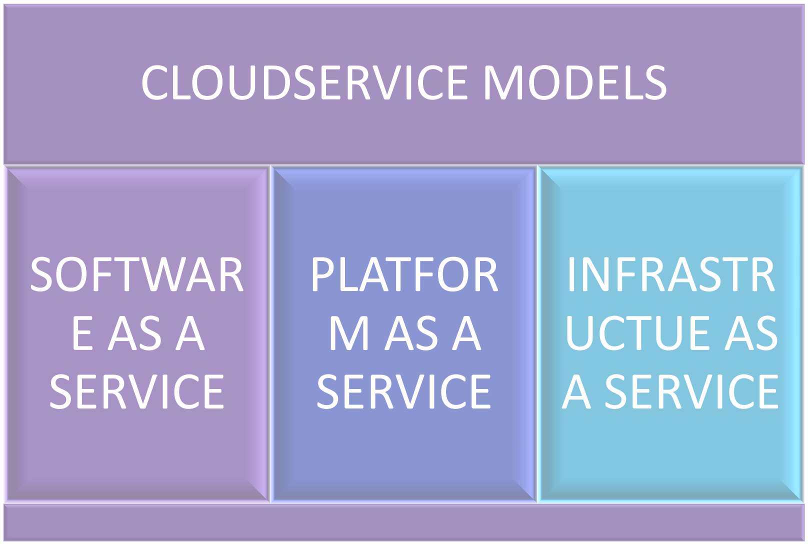

Fig 1: cloud deployment model

2.2. Platform as a Service (PaaS)

Cloud Service Provider (CSP) leases hardware resources, operating system, storage space, network capacity over the internet to the cloud end users to construct their application on top of podium. PaaS gives an expansion and operation middleware layer. The virtualized server systems can be used to check the new application system. With the PaaS operating system features can be modified and improved regularly. Industries in its place of maintaining many hardware services that often bear from mismatched issues, they can adapt PaaS that would supply an improved result to get rid of irreconcilable issues [4].

C. Infrastructure as a Service (IaaS)

The hardware property such as servers, network and storage devices are virtualized and provisioned to the customers based on their application. Gartner's Cloud IaaS investigates and lead on basis, infrastructure, and best carry out, hybrid cloud, security, threat administration and local market evolution. The customers can use Application Program Interface to begin a service, to commune with network elements and add novel procedure. The user does not have control of the core hardware in the cloud instead they can only control the operating system, storage and delivered applications.

3. CLOUD COMPUTING SECURITY CHALLENGES

Cloud computing faces one or more security challenges such as Administrative access, Dynamic Virtual machine, Virtual machine attack and data reliability.

3.1. Administrative Access:

Administrative access to server machines and applications: In cloud computing access to property through internet, which has more revelation to risks, so it is, required to control executive access and to maintain perceptibility of modifications in system control. Different level of user may access

3.2. Dynamic Virtual Machine:

Virtual Machines are self-motivated in nature. They can slowly rollback to prior illustration, duplicated and stirred between different corporal servers. This self-motivated nature and potential for Virtual machine makes it hard to accomplish and sustain reliable security. Vulnerabilities are arrangement mistakes can be dispersed. It is also complicated to sustain auditabilty and protection of virtual machine [5].

.

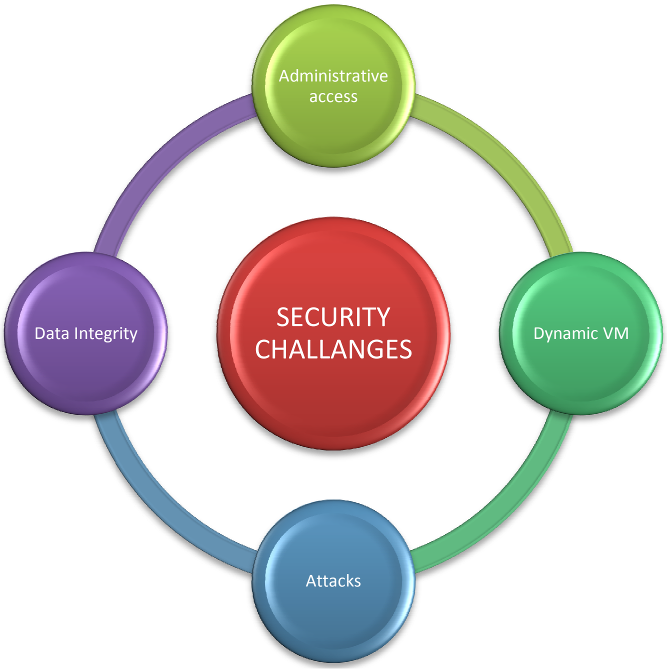

Fig 2: Security Challanges

3.3. Virtual Machine Attacks

Vulnerability exploits and virtual machine to virtual machine attacks. Cloud computing servers use the same operating systems. The ability for a mugger or hacker to tenuously utilize vulnerabilities in these systems and appliances is a serious danger to virtualized cloud computing environments. Also the location of several implicit machines increases the attack surface and risk of Virtual Machine-to-Virtual Machine compromise [6].

3.4. Data Reliability

Data Breaches are happening owed to hacking and incursion, devoted property are necessary to be secured. The cloud Environment moderately or entirely shared is more uncovered to danger. Enterprise needs assurance and auditable evidence that cloud property is not origin neither forged nor compromised. Operating system application files and behaviours need to be observed and give a data security.

4. CLOUD COMPUTING SECURITY ATTACKS

Cloud computing faces one or more number of attacks. These attack much harmful to the cloud environments. The attacks such as Denial of Service Attacks, Malware Injection attacks, destination shared memory attacks, fishing attack, botnets attack, flooding request attacks [7].

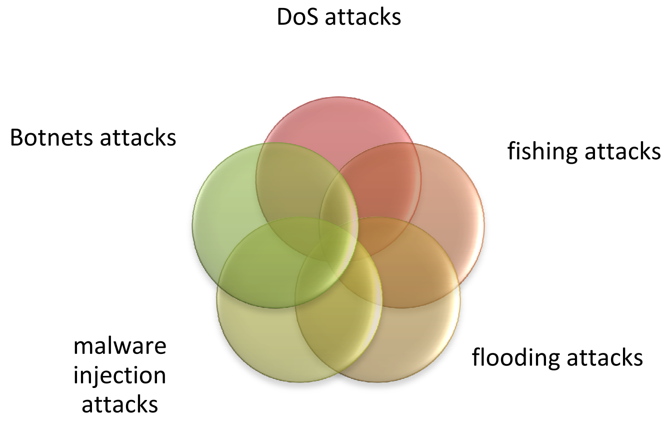

Fig 3: Different types of Attacks

4.1. Denial of Service Attacks (Dos)

Denial of service attacks (DoS) occurs in cloud when the user of cloud overloads the target servers. Denial of Service attack makes an effort to network resource or the machine is engaged to its proposed user .Attacker gives one or more number of requests to the server which results in Denial of service attacks.

4.2. Malware Injection Attacks

The impostors make his/her own virtual machine and insert them into presented infrastructure. Cloud thinks it as new service completion and redirects the request to malicious module. The intruder learns about user request, data, and admission rights. This injected new service will affect all other servers in the cloud environments [8].

4.3. Phishing Attacks

Phishing is a way of reclaim private information from unsuspicious user via sending emails, direct message and webpage linker. These associations appear to the authenticated but leads to false access locations. Phishing attacks are of two kinds they are abuse actions an attacker hosts a phishing attack sites in the cloud environment by using a cloud services and another type is hijack the accounts using social business technique.

4.4. Botnets Attack

In botnets attack the impostor attempt to admission the records by secrete his/he their own individuality and position to decrease finding. This is done by not directly interfering in to intention victims host by a sequence of other hosts. When the Server is jammed and arrives at the maximum threshold capability it will share out its job to a nearest server. This sharing Approach creates the cloud faster. When the malicious enlarges his admission to cloud environments, forged data can be simply formed and send request to the Server. The server verifies the authentications of these arrived requests which can devour CPU Memory results overloading and failure of target servers [9].

5. EXISTING DDOS PREVENTION TECHNOLOGIES

5.1. Filter Based Solutions to Ddos Attacks

Markku Antikainen et al. [13] have proposed a Bloom-Filter based solution. In this bloom filter based forwarding approach is used to prevent DDoS attacks. It solves the fundamental problem of routing table and growth table issue. Multicast allow the dispatcher to make a large number of beneficiaries even though it only sends each packet once. This bloom filter based approach reduces the vulnerability of DDoS attacks.

Zhenhai Duan et al., [14] introduces networking spam zombie. It is a computer connected to the internet that is conciliation by hacker. Compromised machine are one of the key security threat to internet, they often used to launch many security attacks Spam zombies detection tool named SPOT by monitoring outgoing messages on network. SPOT was designed based on a easy and dominant tool named Sequential Probability Ratio Test to detect the compromised machines that are involved in the spamming activities.

5.2. Client Puzzle Based Solution to Prevent DDos Attacks

A client puzzle protocol, the client is enforced to answer a cryptographic puzzle before it can set up a link with a remote server. The author introduces a novel client puzzle protocol that utilizes a adjustment of the Extended Tiny Encryption Algorithm by Zhang et al.,[13,14] More importantly, it is very effective against connection depletion DoS attacks and other resource exhaustion DDoS attacks because minimal calculation load is imposed on the server to confirm the solution to a given puzzle. The client puzzle protocol is also efficient against various other resource fatigue attacks within the transport layer, and can help prevent attacks that exist at the application layer. In this, author describe about client puzzle protocol in detail, and show its efficiency against DDoS attacks..

Ari Juel et al.,[15,16] introduce a cryptographically based solution against correlation depletion attacks. Correlation depletion is a denial of services attack in which attackers try to find to initiate and leave unresolved a large number of connection requests to server. Exhausting its source and rendering it incapable of servicing rightful request. TCP SYN is a well known example of such an attack. The author introduces a client puzzle protocol. When the server comes under attack it allocates small cryptographic puzzles to clients making service requests. To complete its request a client must solve its puzzle correctly. According to the status of server the puzzles are generated. With help of tome parameter the puzzles are authenticated by server and attacks are prevented [17].

6. PROPOSED SYSTEM

6.1. Problem Definition

The DDoS attack plays a vital role in cloud computing. Detection of DDoS attacks is a complex task. Finding where the attacks occurs and removes that occurs need more time. In existing methodologies the attacks are filtered through network routers. This process needs a continuous monitoring of network resources. This need more time to complete a task. Security is an important factor in cloud computing. By eliminating these kinds of attacks in cloud computing we make a successful cloud computing environments. Hence we can prevent the attacks before it happens.

The attackers can perform the DDoS attacks by sending a huge number of requests to the server. This can be done by attackers through a computer programs. They develop a code in some programming languages that request a multiple time to some target address. By executing these kinds of programs the DDoS attacks may occurs. To avoid these kinds attacks and we want to identify the weather user will give request or some other robots gives the request to server. By puzzle technology we can identify the attackers and others machines.

To avoid this kind of situation such we propose an approach called software puzzle. We can able to identify an accessing user is attacker, normal user or robots. We can identify the users by puzzle technology. The user can only able to solve a puzzle by which we can determine who accessing the cloud system. By limiting the requests we can able to prevent the attackers.

6.2. Client Puzzle Technology

A software puzzle is a new technology. The client end users of a cloud need to solve a puzzle before granting a service. Normally cloud computing provides on demand services to end user, whenever user need a service or any other thing they request to cloud server. The cloud service provider or cloud server offers a service when the end user requests a service. The attacks may occur easily in cloud environment [18, 19]. These DDoS attacks seriously threat to cloud servers. The proposed system software puzzle which may help to prevent those DDoS attacks.

In this software puzzle scheme the end user request to the server that is cloud server or cloud service providers. The service provider or server responses to the particular client with software puzzle. The client needs to solve the puzzle where it is send by the server. The client again sends it to the server [20,21]. The server verifies whether the puzzle is right or wrong it is correct the server provides the requested service to the end user.

6.3. Core Puzzle Generation

The puzzles are generated dynamically when the users are requested the cloud server or cloud service providers.

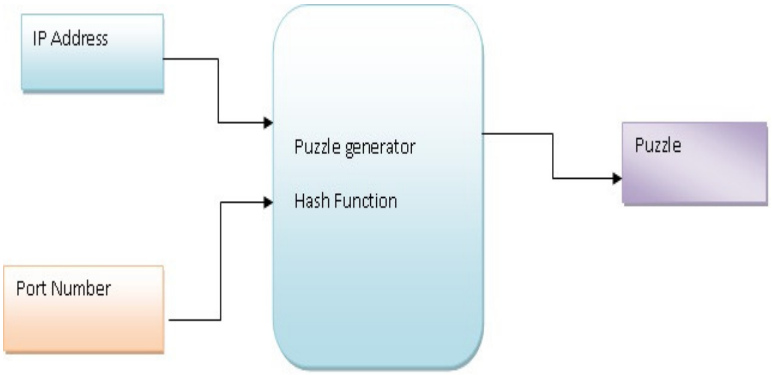

Fig 4: Puzzle Generator

The puzzle generator takes the input of Internet protocol address and port number. Then it performs the hash function. With the help of hash functions they generate a puzzle to the users. This process will perform at each and every time user's requests service providers [23].

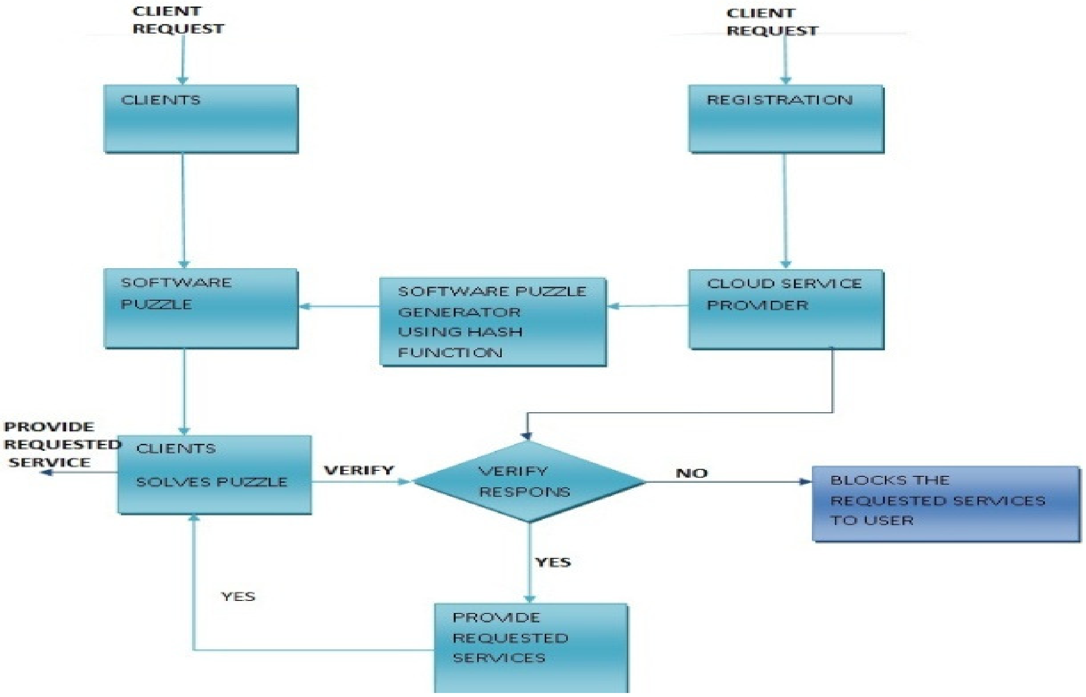
CLIENT REQUEST
CLIENT REQUEST
CLIENTS
REGISTRATION
SOFTWARE PUZZLE
SOFTWARE PUZZLE GENERATOR USING HASH FUNCTION
CLOUD SERVICE PROVIDER
PROVIDE REQUESTED SERVICE
CLIENTS SOLVES PUZZLE
VERIFY
VERIFY RESPONS
NO
BLOCKS THE REQUESTED SERVICES TO USER
YES
YES
PROVIDE REQUESTED SERVICES

Fig 5: flow Diagram

The user can avail service by solving the puzzle. Only the valid user can solve the puzzles .At the time of registration user are request to answer the security puzzle question. The user may mandatory to answer the security questions. Sometime users can change the security questions. Some of the questions that will generate cannot change by users. These questions and answers will be stored in the service provider's database [23]. Whenever user login to cloud environment they are authenticated by password. In second level of security the puzzles will be generated. With help of hash function the puzzle questions will generated dynamically. The users need to solve the puzzles answers. If they fail to answer the question they may be blocked to access the service.

6.4. Puzzle Validation

The users login to the cloud environment. Its take the input of port number and IP address the puzzle will be generated to the users. It means that the software puzzle generation questions will generate. Users are requested to answer the questions. After answering all the questions it will be validated through the server. The server will validate the puzzle solved by user. Comparing the database values it will be validated. The user successfully completed the puzzle they can able to access the service [23].

6.5. Service Providers

The service providers can upload a data or some other services to the cloud.tha administrators are also need to solve the puzzle. After successfully logged to the cloud the service providers are also need to solve a puzzle. After solving a puzzle they can make access to the cloud environments. Now the service providers can upload the data to the cloud servers. Now the software verifies the uploaded files whether it contains any worms or any another malware files inside the executable. Without need of third party auditor the cloud system itself verified the uploaded files .This system provides a more security to the cloud environments.

6.6. Limiting DDos Attacks

The attackers can perform the DDoS attacks by sending a huge number of requests to the server. In which the server cannot be respond the user requests. This type of DDoS attacks can may occurs in two ways. The first way is an attack happens naturally by sending a multiple request in the client browser windows. The second way can be done by attackers through a computer programs. They develop a code that request a multiple time to some target address. By executing these kinds of programs the DDoS attacks may occurs. To avoid these kinds of attacks we limit the user's requests by threshold value. For particular amount of time, limited numbers of requests can only given by user or particular IP address. If the requests reached the threshold limit users are considered as attackers and block the users.

7. EXPERIMENTAL SETUP

The DDoS attacks happen due to attackers, by machines and by normal users. We make a difference to each request to cloud. By analysis these type of attacks. We consider time factors for analysis of users. The time taken to solve a puzzle is an important factor. The machines can solve a puzzle faster than user. This puzzle prevents the robots accessing the system. The authenticated users can only able to solve the puzzle. If they solve a puzzle we can identify that users are normal users. The authorized users can easily solve the puzzle in particular time. If user needs more time to solve a puzzle they are considered as attackers. If they solve a puzzle more quickly they are considered as robots. The graph given below shows the time period of attackers and normal users. The authenticated users can easily solve the puzzle in short period of time. The unauthorized user takes more time to solve a puzzle.

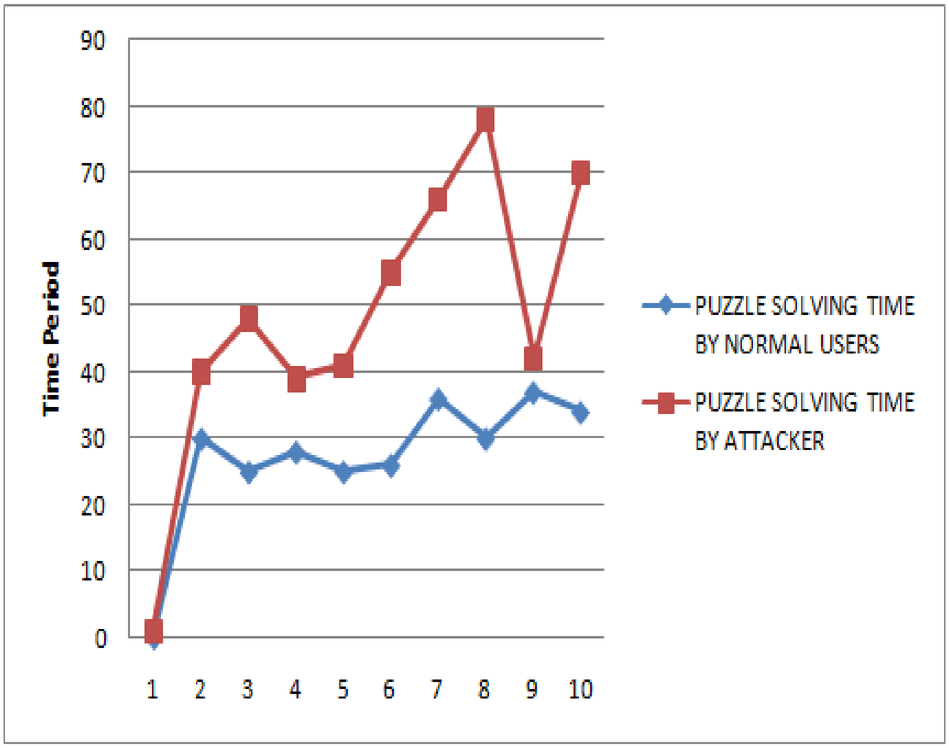

Fig 6: chart puzzle solving time

The attackers perform DDoS attacks by machines through computer programs. They gradually increase the numbers of request to target address. The graph given below shows the request given by attackers and normal users.

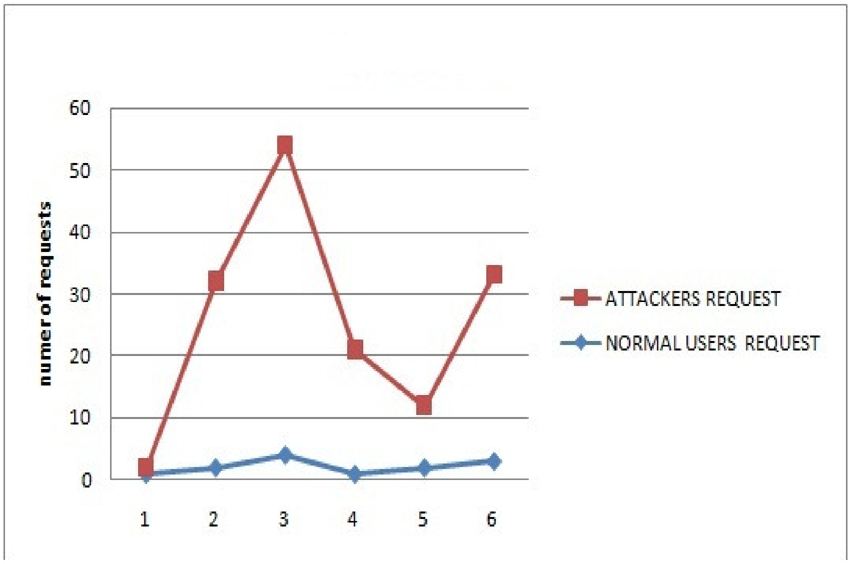

Fig 7: chart users request

With help of these graphs we can analyses who are all attackers and who are all normal users. These graphs show the behaviors of attackers and users. Attackers take more time t solve a puzzle and gives a multiple request to deny the services.

8. CONCLUSION

Cloud Computing is a comparatively new technology that provides a good more numbers of benefits for its users. Cloud computing also economically profitable to the business people and IT industry .Simultaneously cloud computing also lift up some protection problems which may cause and down its use .Accepting and understanding the vulnerabilities, loop hole exist in Cloud Computing environment will help organizations and business, IT industry to make secure towards the Cloud environments. The success of cloud computing will depends on security. In this paper software puzzle scheme is proposed. The proposed scheme will help to prevent DDoS attacks. This also helps to prevent a machine made attacks. The proposed system will completely prevent the DDoS attacks the cloud computing Environments.

9. REFERENCES

[1] Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N " Cloud Computing: A Statistics Aspect of Users. In: First International Conference on Cloud Computing (CloudCom)," Beijing, China. Springer Berlin, Heidelberg, pp 347–358,2009.

[2] Zhang S, Zhang S, Chen X, Huo X "Cloud Computing Research and Development Trend. In: Second International Conference on Future Networks (ICFN'10), Sanya, Hainan, China" IEEE Computer Society, Washington, DC, USA, pp 93–97, 2010.

[3] Cloud Security Alliance "Security guidance for critical areas of focus in Cloud Computing V3.0.. Available: https://cloudsecurityalliance.org/ guidance/csaguide.v3.0.pdf, 2011.

[4] Marinos A, Briscoe G "Community Cloud Computing. In: 1st International Conference on Cloud Computing (CloudCom), Beijing, China. Springer-Verlag Berlin, Heidelberg"2009.

[5] Grobauer B, Walloschek T, Stocker E ,"Understanding Cloud Computing vulnerabilities." IEEE Security Privacy 9(2):50–57,2011.

[6] Subashini S, Kavitha V ,"A survey on Security issues in service delivery models of Cloud Computing. J Netw Comput Appl 34(1):1,2011.

[7] Onwubiko C," Security issues to Cloud Computing. In: Antonopoulos N, Gillam L (ed) Cloud Computing: principles, systems & applications. Springer-Verlag,2010.

[8] National Institute of Standards and Technology. Guide for mapping types of information and information systems to security categories, NIST 800-60,2008.

[9] Morsy MA, Grundy J, Müller I ," An analysis of the Cloud Computing Security problem. In: Proceedings of APSEC 2010 Cloud Workshop. APSEC, Sydney, Australia",2010.

[10] K. Zunnurhain and S. Vrbsky, "Security attacks and solutions in clouds," in Proceedings of the 1st international conference on cloud computing, pp. 145–156, Citeseer, 2010.

[11] B. Sevak, "Security against side channel attack in cloud computing," International Journal of Engineering and Advanced Technology (IJEAT), vol. 2, no. 2, p. 183, 2013.

[12] Sanjeev Khanna, Santosh S. Venkatesh, Member, IEEE, Omid Fatemieh, Fariba Khan, and Carl A. Gunter, Senior Member, IEEE, Member, ACM," Adaptive Selective Verification: An Efficient Adaptive Countermeasure to Thwart DoS Attacks", IEEE/ACM Transactions On Networking, Vol. 20, No. 3, June 2012.

[13] Moti Geva, Amir Herzberg, and Yehoshua Gev l," Bandwidth Distributed Denial of Service: Attacks and Defenses", Copublished by the IEEE Computer and Reliability Societies January/February 2014 .

[14] Zahid Anwar and Asad Waqar Malik," Can a DDoS Attack Meltdown My Data Center?A Simulation Study and Defense Strategies", Ieee Communications Letters, Vol. 18, No. 7, July 2014.

[15] Shui Yu, Senior Member, IEEE, Yonghong Tian, Senior Member, IEEE,Song Guo, Senior Member, IEEE, and Dapeng Oliver Wu, Fellow, IEEE," Can We Beat DDoS Attacks in Clouds?", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 9, September 2014.

[16] Xinlei Ma and Yonghong Chen," DDoS Detection Method Based on Chaos Analysis of Network Traffic Entropy", IEEE Communications Letters, Vol. 18, No. 1, January 2014.

[17] Markku Antikainen, Tuomas Aura, and Mikko Särelä," Denial-of-Service Attacks in Bloom-Filter-BasedForwarding", IEEE/ACM Transactions On Networking, Vol. 22, No. 5, October 2014.

[18] Zhenhai Duan, Senior Member, IEEE, Peng Chen, Fernando Sanchez, Yingfei Dong, Member, IEEE, Mary Stephenson, and James Michael Barker," Detecting Spam Zombies by Monitoring Outgoing Messages", IEEE/ACM Transactions On Networking, Vol. 22, No. 5, October 2014.

[19] Changwang Zhang, Zhiping Cai, Weifeng Chen , Xiapu Luo, Jianping Yin," Flow level detection and filtering of low-rate DDoS", Computer Networks 56 (2012) 3417–3431.

[20] T. J. McNevin, J.-M. Park, and R. Marchany, "pTCP: A client puzzle protocol for defending against resource exhaustion denial of service attacks," Virginia Tech Univ., Dept. Elect. Comput. Eng., Blacksburg, VA, USA, Tech. Rep. TR-ECE-04-10, Oct. 2004.

[21] A. Juels and J. Brainard, "Client puzzles: A cryptographic countermeasure against connection depletion attacks," in Proc. Netw. Distrib. Syst.Secur. Symp., 1999, pp. 151–165.

[22] R. Shankesi, O. Fatemieh, and C. A. Gunter, "Resource inflation threats to denial of service countermeasures," Dept. Comput. Sci., UIUC, Champaign, IL, USA, Tech. Rep., Oct. 2010. [Online]. Available: http://hdl.handle.net/2142/17372 520092 .

[23] Yongdong Wu, Zhigang Zhao, Feng Bao, and Robert H. Deng ," Software Puzzle: A Countermeasure to Resource-Inflated Denial-of-Service Attacks", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 1, January 2015.

[24] Subramaniam.T.K, Deepa.B, "Security Attack Issues And Mitigation Techniques In Cloud Computing Environments", International Journal of Ubi Comp (IJU), Vol.7, No.1, January 2016.

[25] Subramaniam.T.K, Deepa.B, "A Review towards DDoS Prevention and Detection Methodology" International Journal of Computational Science and Information Technology (IJCSITY) Vol.3,No.1/2/3,August 2015.

[26] Subramaniam.T.K, Deepa.B, "A Survey on DDOS Attack Detection And Prevention Methodology" International Journal of Intellectual Advancements and Research in Engineering Computations, JUNE 2015.

Authors

T.K.Subramaniam Received the B.Tech degree in Information technology from Nandha Engineering College in the year 2014.He is currently doing his M.E Computer science and Engineering in Nandha engineering college, Erode, India. His area of interest is web services. He has published many journal papers.

B.DEEPA received the M.E degree in Computer Science and Engineering from Nandha Engineering College in the year 2011.She is currently working as Assistant Professor in Nandha Engineering College, Erode, India. She has published many international and national research papers. Her area is Network security and web services. She has depth knowledge of her research area.