ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)
Vol. 2, Issue 3 (July - Sept. 2015)
International Journal of Advanced Research in Education & Technology (IJARET)

A Survey on Denial of Service Attack in Cloud Computing Environment

[I]R.Ramya, [II]G.Kesavaraj
[I]M.Phil Full Time Research Scholar, Dept. of Computer Science
[II]Assistant Professor, Dept. of Computer Science and Applications
[I,II]Vivekanandha College of Arts and Sciences for Women, Elayampalayam, Tiruchengode, Namakkal(DT), Tamil Nadu, India.

Abstract
Cloud computing is a new technology that allows the clients to get access to the services and resources according to the demand. The success of Cloud Computing is mainly due to its on-demand and self service nature. We can pay only for the for the amount of resources we have used. We don't need to pay for the hardware and software maintenance cost. This flexible nature of cloud makes it suitable for any type of organization. One of the major concern in Cloud Computing is security because the features of cloud computing is based on the sharing of its resources. The security issues acts as a barrier in the growth of cloud computing. Availability of data is the most important part in cloud computing and even for economic growth of the society. An Attack namely Denial of Service (DOS) IS an attempt to make the resources and services unavailable to its intended users by flooding network with more number of requests with an invalid return address. This paper contains a survey on DOS Attack in cloud computing environment.

Keywords
Cloud Computing, Denial of Service(DOS), Cloud Architecture, Benefits, Challenges, Attacks, Security.

I. Introduction

Cloud computing is one of the internet based computing, providing services such as servers, storage, applications. Cloud computing has a greater advantage in corporate data centers making the data centers to operate like the internet, through the process of enabling computing resources to be accessed and shared as virtual resources. Cloud computing employs networks of large group or sectors of servers, which runs on running low cost consumer PC technology with specialized connections. Generally users put theirs confidential and also non confidential data into cloud, so that the users can ultimately decrease their costs on hardware infrastructure as well as maintenance. Whenever a data is moved into a cloud, the user's data becomes vulnerable and unsecure. Security is the major concern in Cloud Computing. The security vulnerabilities and security concerns should take specification to address the issues accordingly.

The Denial of Service attack(DOS) which is a type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service. In a DOS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy. DOS attack is hard to detect if attacker use the spoofed IP. Spoofed IP is used by attacker to ensure that compromised machine remains undetected and attacker can use it for other different kinds of attacks. But even if the source of attack is kept constant, then it is possible to stop the attack and block it. In this paper, we provide a taxonomy of DOS attacks over a network based Cloud components in the cloud environment.

Cloud computing service models

The three main service models of cloud computing are:

1. Software as a service (SaaS): Applications hosted by a provider on a cloud infrastructure are accessed from thin or thick clients over the network or a program interface (for example, web services). Examples are Google Docs, IBM Smart Cloud Docs, IBM Smart Cloud Meetings, Saleforce.com's CRM application and so on.

2. Platform as a service (PaaS): Providers deliver not only infrastructure but also middleware (databases, messaging engines and so on) and solution stacks for application build, development and deploy. IBM SmartCloud Application Services and Google App Engine are two examples of PaaS.

3. Infrastructure as a service (IaaS): It is the delivery of computing infrastructure as a service. IBM Smart Cloud Enterprise+, SoftLayer cloud and Amazon EC2 are some examples of IaaS.

Cloud Computing Deployment Models

Public cloud. This is where computing resources provided by a cloud provider are used by different organizations through public Internet on a pay as you go (PAYG) model. Cloud providers ensure some sort of separation for resources used by different organizations. This is known as multitenancy.

Private cloud. This is where cloud infrastructure is solely owned by an organization and maintained either by this organization or a third party and can be located on site or off-site. Computing resources are behind the corporate firewall.

Community cloud. Here, cloud infrastructure is owned and shared by multiple organizations with a shared concern.

Hybrid cloud. It is the combination of any type of cloud model mentioned above connected by standardized or proprietary technology.

II. Cloud Architecture

Cloud computing architectures consist of front-end platforms called clients or cloud clients. These clients comprise servers, fat (or thick) clients, thin clients, zero clients, tablets and mobile devices. These client platforms interact with the cloud data storage via an application (middleware), via a web browser, or through a virtual session.

The zero client

The zero or ultra-thin client initializes the network to gather required configuration files that then tell it where its OS binaries

ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)

are stored.[1] The entire zero client device runs via the network. This creates a single point of failure, in that, if the network goes down, the device is rendered useless.[2]

Cloud Storage

An online network storage where data is stored and accessible to multiple clients. Cloud storage is generally deployed in the following configurations: public cloud, cloud, community, or some combination of the three also known as hybrid cloud.[3]

In order to be effective, the cloud storage needs to be agile, flexible, scalable, multi-tenancy, and secure.[4]

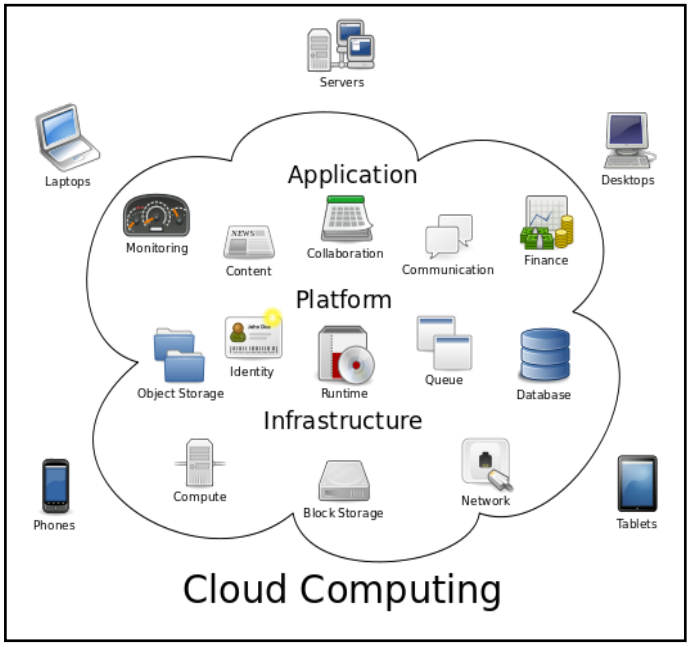
Cloud Networking

Generally, the cloud network layer should offer:

- High bandwidth (low latency)
  Allowing users to have uninterrupted access to their data and applications.
- Agile network
  On-demand access to resources requires the ability to move quickly and efficiently between servers and possibly even clouds.
- Network security
  Security is always important, but when you are dealing with multi-tenancy, it becomes much more important because you're dealing with segregating multiple customers.[8]

III. Benefits And Challenges Of Cloud Computing

In recent years, cloud computing has emerged as an important solution offering enterprises a potentially cost effective model to ease their computing needs and accomplish business objectives. Wilson Law, a manager at member firm, Moore Stephens LLP Singapore, provides some key benefits below worth considering:



Benefits

a) **Optimized server utilization** - as most enterprises typically underutilize their server computing resources, cloud computing will manage the server utilization to the optimum level.

b) **Cost saving** - IT infrastructure costs are almost always substantial and are treated as a capital expense (CAPEX). However if the IT infrastructure usually becomes an operating expense (OPEX). In some countries, this results in a tax advantage regarding income taxes. Also, cloud computing cost saving can be realized via resource pooling.

c) **Dynamic scalability** - many enterprises include a reasonably large buffer from their average computing requirement, just to ensure that capacity is in place to satisfy peak demand. Cloud computing provides an extra processing buffer as needed at a low cost and without the capital investment or contingency fees to users.

d) **Shortened development life cycle** - cloud computing adopts the service-orientated architecture (SOA) development approach which has significantly shorter development life cycle that that required by the traditional development approach. Any new business application can be developed online, connecting proven functional application building blocks together.

e) **Reduced time for implementation** - cloud computing provides the processing power and data storage as needed at the capacity required. This can be obtained in near-real time instead of weeks or months that occur when a new business initiative is brought online in a traditional way.

Challenges:

a) **Data location** - cloud computing technology allows cloud servers to reside anywhere, thus the enterprise may not know the physical location of the server used to store and process their data and applications. Although from the technology point of view, location is least relevant, this has become a critical issue for data governance requirements. It is essential to understand that many Cloud Service Providers (CSPs) can also specifically define where data is to be located.

b) **Commingled data** - application sharing and multi-tenancy of data is one of the characteristics associated with cloud computing. Although many CSPs have multi-tenant applications that are secure, scalable and customizable, security and privacy issues are still often concerns among enterprises. Data encryption is another control that can assist data confidentiality.

c) **Cloud security policy / procedures transparency** - some CSPs may have less transparency than others about their information security policy. The rationalisation for such difference is the policies may be proprietary. As a result, it may create conflict with the enterprise's information compliance requirement. The enterprise needs to have detailed understanding of the service level agreements (SLAs) that stipulated the desired level of security provided by the CSPs.

d) **Cloud date ownership** - in the contract agreements it may state that the CP owns the data stored in the cloud computing environment. The CSP may demand for significant service fees for data to be returned to the enterprise when the cloud computing SLAs terminates.

e) **Lock-in with CSP's proprietary application programming interfaces (APIs)** - currently many CSPs implement their application by adopting the proprietary APIs. As a result, cloud services transition from one CSP to another CSP, has become extremely complicated, time-consuming and labour-intensive.

f) **Compliance requirements** - today's cloud computing services, can challenge various compliance audit requirements currently in place. Data location; cloud computing security policy transparency; and IAM, are all challenging issues in compliance auditing efforts. Examples of the compliance requirement including privacy and PII laws; Payment Card Industry (PCI) requirements; and financial reporting laws.

g) **Disaster recovery** - it is a concern of enterprises about the resiliency of cloud computing, since data may be commingled and scattered around multiple servers and geographical areas. It may be possible that the data for a specific point of time cannot be identified. Unlike traditional hosting, the enterprise knows exactly where the location is of their data, to be rapidly retrieved in the event of disaster recovery. In the cloud computing model,

the primary CSP may outsource capabilities to third parties, who may also outsource the recovery process. This will become more complex when the primary CSP does not ultimately hold the data.

Businesses are under increasing pressure to sharpen their business practices. Too few people are aware of the security threats that are emerging. Nevertheless, they are responsible for ensuring that sensitive data will remain authentic, accurate, available, and will satisfy specific compliance requirements. Thus, it is essential for an organization to understand their current IT risks profile in order for them to determine the company's levels of IT risk tolerance and IT risk policies, and oversee management in the design, implementation and monitoring of the risk management and internal controls system.

IV. Cloud Computing Attacks

Since companies are moving towards cloud computing, care must be taken against hackers. The attacks which criminals or hackers may attempt include:

i) **Denial-of-Service attack (DoS)**

Cloud is more penetrable to DOS attacks, because so many users are involved in the usage of cloud services and resources, therefore DOS attacks can be more damaging. A denial-of-service (DOS) is a type of attack where the attacker tries to prevent the authorized users from accessing the services from the cloud service provider. The attacker usually sends more number of requests to the cloud server thereby creating network traffic and the connection between the machines get interrupted. The DOS attacks Prevents a particular individual from accessing the cloud service. Another variant of the DOS is the smurf attack. This involves emails with automatic responses. If the fake email address actually belongs to someone, this can overwhelm that person's account.

ii) **Cloud Malware- Injection Attack**

Malware is the term used to generally describe malicious software, i.e., software that is designed to compromise the confidentially, integrity or availability of computer systems.

The term "Malware" is broader than the better known expression "Virus" as it also encompasses Worms, Trojan Horses, Rootkits, Spyware, Adware, Crimeware, Robot (botnet) Clients, etc.

Malware Injection attack results in activities such as

- Degraded computer operations;
- Intrusive pop-up windows that may or may not solicit payment for goods and services;
- Spam email promoting unwanted products, services or activities deemed distasteful or even illegal;
- Theft of personal, financial or corporate information; or
- Installation of remote control software that allows hackers to control and monitor computer activities

iii) Side Channel attack

In side-channel attacks, the attacker runs a virtual machine on the same physical host of the victim's virtual machine and takes advantage of a shared physical component (e.g. the processor cache) in order to steal information (e.g. a cryptographic key) from the victim. More precisely, the attacker tries to retrieve the value of a cryptographic key by observing the activity of the processor cache. It is worth pointing out that we are assuming that the attacker managed somehow to place his virtual machine on the same physical host of the victim. Actually, this operation is not trivial and requires to launch tens of virtual machines. Moreover, after a virtual machine has been launched, a co-residency check is needed.

V. Conclusion

The cloud security issues are attracting great attention since its beginning. Many solutions exist and many are evolving. Issues like information security, data protection, virtualization and isolation are active research area for academics and Industry. The analysis of security issues in the area of cloud computing is done and various categories identified based on the type of security. Various trust based solution are also categorized based on the way of providing trust in a collaborative environment. Through the usage of proper security algorithms in future we can ensure security in cloud computing environment.

References

[1]. *Meiko Jensen, Jorg Schwenk, Nil Gruschka "On technical issues in cloud computing", IEEE International Conference on cloud computing, 2009.*

[2]. *Bhaskar Parsad Rimal, Eunmi Choi, Ian Lumb "A taxonomy and survey of cloud computing system" Fifth International joint Conference on INC, 2009.*

[3]. *Minqi Zhou, Rong Zhang, Wei Xie "Security and Privacy in Cloud computing: A Survey" sixth International Conference on Semantics, 2010.*

[4]. *Pearson, S. "Taking account of privacy when designing cloud computing services" Software Engineering Challenges of Cloud Computing, 2009, pages, 44 – 52, Vancouver, BC.*

[5]. *Jensen, M. Schwenk, J. Gruschka, N. Iacono, "On technical security issues in Cloud" IEEE International Conference on Cloud Computing, 2009, pages 109-16, Germany.*

[6]. *Arshad, J. Townend, P. Jie Xu , "Quantification of Security for compute Intensive Workloads in Clouds", 15th International Conference on Parallel and Distributed Systems, School of Computation, pages 478-486, Dec. 2009, UK.*

[7]. *Mell, P. and T. Grance, The NIST definition of cloud computing. National Institute of Standards and Technology, 2009. 53(6): p. 50.*

[8]. *Foster, I. and C. Kesselman, The grid: blueprint for a new computing infrastructure. 2004: Morgan Kaufmann.*

[9]. *Buyya, R., High performance cluster computing: programming and applications, vol. 2. Pre ticeHallPTR, NJ, 1999.*

[10]. *http://www.customis.com/resources/library/VirtualizationWhitePaper.*

[11]. *http://www.csc.villanova.edu/~nadi/csc8580/S11/AnushaUppalapati.pdf.*

[12]. *Dillon, T., C. Wu, and E. Chang. Cloud computing: Issues and challenges. 2010: Ieee.*

[13]. *Hovav, A. and J. D'Arcy, The Impact of Denial of Service Attack Announcements on the Market Value of Firms. Risk Management and Insurance Review, 2003. 6(2): p. 97-121.*

[14]. *K. Thirupathi Rao "Prospective of Cloud Computing" an article in International Journal of Computers and Communications, Volume1, Isuue1, ISSN 2319 – 8869, Pp. 5-8 (2012).*

[15]. *Mehmud Abliz,'Internet Denial of Service Attacks and Defense Mechanisms', Department of Computer Science, University of Pittsburgh.*

[16]. *K., Thirupathi Rao et al., "Secure multi-tenancy cloud storage in cloud computing" Global Journal of Mech., Engg. & Comp. Sciences, review paper, Pp.79-82 (2012).*