Volume 5, No. 7, September-October 2014

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

REVIEW ARTICAL

Available Online at www.ijarcs.info

A Review on Cloud Computing Security Issues

Amarbeer Kaur
M. Tech Computer Science
Punjab Technical University, India

Nitin Bhagat
AP, M.Tech Computer Science,
Department of CSE

Abstract: Cloud computing has different meaning to different people, the privacy and security issues also differ between a consumer using a public cloud application, a medium-sized Company using a customized Design of business on a cloud platform, and Some Companies are using Platform on Public level which are Public to Public Network The security requirements in cloud computing environment is to find the Security threats in the Structure of clouds To find the security solutions, and finding Reason so that Pre Security Step Should be taken in concerned with security proposed model. In this paper is to build a trusted computing environment for cloud computing system by Combining the trusted computing platform into cloud computing system Which is free from vulnerabilities and threats and system is designed with a model system in which cloud computing system is combined with trusted computing platform and trusted platform models.

Keywords: cloud computing, data breaches, Api Attack Deniel Attack, Account high Jacking, Deniel of Services

I. INTRODUCTION

Cloud Computing holds the potential to eliminate the requirements for setting up of high – cost computing infrastructure for IT - based solutions and services that the industry uses. Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements [1]. The principle of Cloud computing is the provision of computing resources via a network. Cloud computing shifts the responsibility of configuring, deploying, and maintaining computing infrastructure from clients to cloud- providers. Providers generally expose an interface for clients to interact with their resources; however, number of resources may be aggregated on the same computer or cluster of computers. The user does not necessarily know the details of the location, equipment or configuration of their resources. they are provided with a "virtualised" computer resource hosted in "the Cloud"[2]. Clouding computing emtraces cyber infrastructure and builds upon decades of research in virtulization, distributed computing, grid computing, web and software services and leave developers and IT administrators to concentrate on the specific details of the application they wish to provide [3]. In addition to public Cloud services, many organisations are implementing internal private Clouds to reduce costs, complexity and consolidate infrastructure with various models cloud computing.

A. Software as a Service (SAAS):

SAAS clients rent usage of applications running within the Cloud‟ s provider infrastructure, for example SalesForce. The applications are typically offered to the clients via the Internet and are managed completely by the Cloud provider. SAAS run on cloud and multiple end users are uses it. Basically It runs on web browser e.g. Gmail- a popular SAAS product. That means that the administration of these services such as updating and patching are in the provider's responsibility[4].

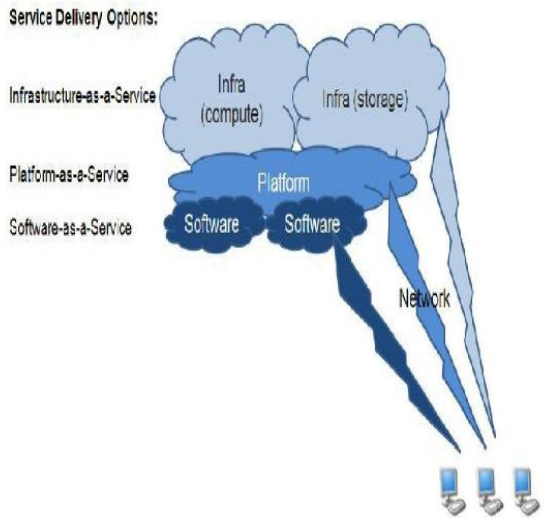

Figure: 1 Service Model of Cloud Computing

One big benefit of SaaS is that all clients are running the same software version and new functionality can be easily integrated by the provider and is therefore available to all clients.

B. Platform as a Service (PaaS):

PaaS Cloud providers offer an application platform as a service, for example Google App Engine. SaaS is cloud based application development and used by deployers and developers [4]. This enables clients to deploy custom software using the tools and programming PaaS Cloud providers offer an application platform as a service, for example Google App Engine. This enables clients to deploy custom software using the tools and programming languages offered by the provider. Clients have ++control over the deployed applications and environment related settings. As with SaaS, the management of the underlying infrastructure lies within the responsibility of the provider. languages offered by the provider. Clients have control over the deployed applications and environment related settings. As

with SaaS, the management of the underlying infrastructure lies within the responsibility of the provider.

C. Infrastructure as a Service (IaaS):

IaaS delivers hardware resources such as CPU, disk space or network components as a service. IaaS allow accessibility of infrastructure using Internet technology consist of server, storage and other peripherals devices[4]. These resources are usually delivered as a virtualization platform by the Cloud provider and can be accessed across the Internet by the client. The client has full control of the virtualised platform and is not responsible for managing the underlying infrastructure.

a. Main Body:

At an unprecedented pace, cloud computing has simultaneously transformed business and government, and created new security challenges. The development of the cloud service model delivers business-supporting technology more efficiently than ever before. The shift from server to service-based thinking is transforming the way technology departments think about, design, and deliver computing technology and applications. Yet these advances have created new security vulnerabilities, including security issues whose full impact is still emerging. Among the most significant security risks associated with cloud computing is the tendency to bypass information technology (IT) departments and information officers. Although shifting to cloud technologies exclusively is affordable and fast, doing so undermines important business-level security policies, processes, and best practices. In the absence of these standards, businesses are vulnerable to security breaches that can quickly erase any gains made by the switch to SaaS.

Cloud Security Alliance is a renowned community in the scope of cloud security. It has proposed interface, insiders, shared, data/account loss and snipper attacks security threats [5]. Recognizing both the promise of cloud computing, and the risks associated with it, the Cloud Security Alliance (CSA) has pioneered the creation of industry-wide standards for effective cloud security. In recent years, CSA released the "Security Guidance for Critical Areas in Cloud Computing" and the "Security as a Service Implementation Guidance." These documents have quickly become the industry-standard catalogue of best practices to secure cloud computing, comprehensively addressing this within the thirteen domains of CSA Guidance and ten categories of service associated with the SaaS. Implementation Guidance series. Already, many businesses, organizations, and governments have incorporated this guidance into their cloud strategies.

However, CSA recognizes that a central component of managing risks in cloud computing is to understand the nature of security threats. The purpose of the "The Notorious Nine: Cloud Computing Top Threats in 2013" report is to provide organizations with an up-to-date, expert-informed understanding of cloud security threats in order to make educated risk-management decisions regarding cloud adoption strategies.The top threats report reflects the current consensus among experts about the most significant threats to cloud security. While there are many vulnerabilities to cloud security, this report focuses on threats specifically related to the shared, on-demand nature of cloud computing.To identify the top threats, CSA conducted a survey of industry experts to compile professional opinion on the greatest vulnerabilities within cloud computing. The Top Threats working group used these survey results alongside their expertise to craft the final 2013 report. The survey methodology validated that the threat listing reflects the most current concerns of the industry. In this most recent edition of this report, experts identified the following nine critical threats to cloud security (ranked in order of severity):

a) Data Breaches
b) Account Hijacking
c) Insecure APIs
d) Denial of Service
e) Malicious Insiders
f) Abuse of Cloud Services
g) Insufficient Due Diligence
h) Shared Technology Issues.

b. Data Breaches:

Information management is critically important to all of us - as employees and consumers. For that reason, the Identity Theft Resource Center has been tracking security breaches since 2005, looking for patterns, new trends and any information that may better help us to educate consumers and businesses on the need for understanding the value of protecting personal identifying information.

2005 to August 5, 2014
Total Number of Recorded Breaches = 4,695
Total Number of Records Exposed = 633,469,530
(Note: This cumulative number of reported breaches and records exposed will be updated monthly.)

The ITRC breach list is a compilation of data breaches confirmed by various media sources and/or notification lists from state governmental agencies. This list is updated daily, and published each Tuesday. Breaches on this list typically have exposed information that could potentially lead to identity theft, including Social Security numbers, financial account information, medical information, and even email addresses and passwords. ITRC follows U.S. Federal guidelines about what combination of personal information comprise a unique individual, and the exposure of which will constitute a data breach. To achieve the service of cloud computing, the most common utilized communication protocol is HTTP and Secure Shell (SSH). [6]

c. Account Hijacking:

IT professionals expressed a belief that the risks of using a cloud based service currently outweighed the benefits. The main reason cited was a concern over data security. This concern has made many business leaders hesitant to switch over to the cloud, but the reality is the cloud is growing and is not going away, especially with the possibility of big data cloud computing. Account hijacking attackers can access sensitive information and compromise the confidentiality, integrity, and availability of the services offered [7].

In fact, Forrester In a recent survey, 69 percent of North American Research predicts that the cloudbusiness will grow from its current worth at $40billion to $160 billion by 2020. Rather than ignoring the cloud, business leaders should learn about the vulnerabilities, what their implications are and the steps they can take to protect their data. This article will specifically address the vulnerability to service traffic hijacking and how it can be addressed.

d. Insecure APIs:

APIs, or application programming interfaces, are nothing new; they give developers programmatic access to services. API provides accessibility to software that enable interaction with the cloud software in the same way that a traditional user interface.(e.g. A computer desktop) facilitates interaction between user and computer [8]. This includes cloud services, such as storing data, updating a database, moving data, pushing data into a queue, provisioning a server, etc.APIs are important in the world of cloud computing because of how they're used. Lines are being drawn around groups of cloud providers that rely on certain types of APIs. And enterprises are beginning to notice, and while it makes an interesting conversation, consumer concerns still surround vendor lock-in and portability issues. Central to this issue is that Amazon Web Services (AWS) now dominates the market, making its API the de facto standard. And many companies use AWS, making it an "emerging standard" because of the availability of third-party support and skilled cloud developers - even though the IP around the API belongs solely to AWS.

What makes DoS attacks so difficult to prevent is because it not only affect open services on devices, but also closed ports, as long as the service request reaches the device, the bandwidth utilization will be effected. Due to the nature of the attack which can be crafted in many forms, targeted at many services and devices, it is most difficult to prevent devices from being susceptible to such attack. Even a legitimate request packet can turn into malicious traffic if it creates recursive effect such as opening multiple simultaneous connections. DoS attack in cloud environment has been suggested consisting three phases. (1) The first-phase is to model the normal traffic pattern for baseline profiling and (2) the second phase is the intrusion detection processes and (3) finally prevention phase [9]. That is another reason why DoS is very difficult to prevent. However, like other network threats, there is no silver bullet solution to the problem.

e. Prevention:

a) High redundancy and high availability network design:

In order to prevent a network from falling trap into a DoS attack it is crucial to design the network as such that there is not a single point of failure. However, such high availability will incur additional cost, especially in maintaining dual connection to the Internet. It is also desired that ISPs provide load balancing on the upstream router to load share the redundant link.

f. Perimeter Defense:

The router and firewalls should pass through only legitimate packets to reach its internal network. An example is, limiting the internal web server from initiating port 80 connection destined to external hosts. Such filtering can prevent propagation of Code Red Worm attacks which causes a stream of scanning to various IP Addresses on port 80.

Preventing IP Address Spoofing using egress [10] and ingress filtering [2] are examples of filtering at the gateway or router level to prevent packet spoofing from internal hosts, and to internal hosts respectively. However, it will not prevent attacks from legitimate IP Addresses within the network. Every interface on a router should prohibit packets that logically could not come from that network interface.

g. Defense In-depth:

Implementation of Intruder Detection System (IDS) will allow detection of "slave","master" or "agent" machines communications. Action can be taken to remove those infected host from the network [9]. However, IDS may be able to detect known attacks but not new variations of these attacks.

h. Host Hardening:

Hardening the respective device on the network will prevent the host from DoS attack. Host hardening involves upgrading the operating system, applying relevant patches for the operating system and required applications, closing irrelevant services, customizing and tightening configurations, and applying Access Control Lists on the required services. Changing default passwords and applying good password policies. Known buffer overflow attacks can be prevented by keeping the host up to date with patches or version upgrades.

i. Malware Detection and Prevention:

The hosts and the network must have antivirus installed and scanning any introduction of new data, while file integrity checkers is used to detect any unauthorized attempt to change the original data [11]. This will prevent infection of malicious codes and attempts to rootkit the host. Compromised host could make the host a potent host to become handlers for malicious users who wish to conduct DoS attack.

j. Periodic Scanning:

Periodic network vulnerability scanning will detect vulnerable host and detect new infection. It is necessary to conduct periodic vulnerability since in any network, there are always new production host going on-line, or new devices being connected to the network.

k. Policy Enforcement:

Last but not least is having a strong policy enforcement on acceptable use and management of computing resources. It is also a daunting task to ensure that all in house and outsource code development apply good programming practices to avoid loopholes such as buffer overflow and DoS. Rigorous testing of preproduction system is inevitable to avoid unwanted loopholes.

Despite applying all these measures there is still no guarantee that one will be immune to any DoS attacks but it will mitigate the effect of DoS attacks. However, applying the above recommendations would also mitigate other forms of malicious activities such as session hi-jacking, buffer overflow attacks and reconnaissance. It will not only prevent your network from becoming targets of DoS attacks, but also prevent it from becoming the launching pad for such attacks.

l. Legal infrastructure:

The legal framework in handling DoS and DDoS attacks differ based on the country's legal establishment. However, one common issue is that the legal definition of threats often misses out on DoS attack. The legal framework often defines "destruction of a communication device" as a

crime, which defines it as a hardware. In a DoS and DDoS attack; the system may be recovered easily after a simple reboot, without damaging the hardware device [10]. The legal framework should define attacks as such attacks which causes failure of devices to function, or attacks which degrade the ability of the device to function, or attacks which attempt to overwhelm the bandwidth capacity of the network device to reflect DoS and DDoS attacks instead.

Another issue is spoofed IP addresses in DoS and using multiple points of attacks such as in DDoS, increases complexity of determining the original attacker's machine. It is often difficult to obtain the information from the infected host, unless with full cooperation from the affected organization and acted upon in a short period of time. Prolonged delay in investigation may cause the data to be lost. Even after the relevant information are being preserved, and analyzed, the integrity of the data will be questioned. These factors make it difficult to identify the person behind the computer.

Legal proceedings require such information to be entangled and objectively determined and analyzed. Applying computer forensics procedures are crucial in the early process of evidence gathering.

II. CONCLUSION

Cloud computing is the promising paradigm for delivered IT services as computing utilities Cloud are designed to provide services to external user provider need to be compensated for sharing their resources and capabilities. This paper gives an overview of cloud computing service and deployment model to evaluate and improve the existing systems.

III. REFERENCES

[1]. Mohsin Nazi , "Cloud Computing: Overview & Current Research Challenges". IOSR Journal of Computer Engineering (IOSR -JCE) ISSN: 2278-0661, ISBN: 2278-8727 Volume8, Issue1 (Nov.-Dec. 2012), PP14-22 .

[2]. S. Saraswathi, P. Yogesh, " Ingress Filtering at Egde Network to Protect VPN Service from DOS Attack". CCSEA, pp35-44, 2012

[3]. Mladen A Vouk, "Cloud Computing – Issues, Research and Implementations". Journal of Computing and Information Technology- CIT, 16, 2008. PP 235-246

[4]. Dimpi Rani, Rajiv Kumar, " A Comparative Study of SaaS, PaaS and IaaS in Cloud Computing". International Journal of Advanced Research in Computer Science and Software Engineering. Vol. 4, Issue 6, June-2014.

[5]. Vahid Ashktorab, Seyeb Reza, " Security Threats and Countermeasures in Cloud Computing". IJAIEM, Vol-1, Iss-2, October, 2012.

[6]. Rabi Prasad, Manas Ranjan, Suresh Chandra, " Cloud Computing: Security Issues and Research Challenges". IRACST-IJCSITS, Vol-1. No-2, Dec, 2011

[7]. Chimere Barron, Huiming Yu and Justin Zhan, "Cloud Computing Security Case Studies and Research", Proceedings of the World Congress on Engineering 2013 Vol II, WCE 2013, July 3 - 5, 2013, London, U.K

[8]. Dr. Sunil Batra, Anju Chhibber, " Preliminary Analysis of Cloud Computing Vulnerabilities", journal of Engineering, Computer & Applied Sciences (JEC&AS). Vol.2, No.5, May,2013

[9]. Mohd Nazri, Abdulaziz, Shahrulniza, Aamir Shahzad, "Detecting Flooding based DOS Attack in Cloud Computing Environment using Covariance Matrix Approach". ICULMC (IMCOM) 2014, January. 17-19, 2013, Kota Kinabalu, Saba, Malaysia.

[10]. J. Rameshbabu, B. Sam, R. Wesley, K. Malathi, " A Prevention of DDOS Attacks in Clouds Using NEIF Techniques". International Journal o f Scientific and Research Publications, Vol.4, No. 4, April 2014.

[11]. Ajayi Adebowale and Omotosho O. J., "An overview of Data driven Intrusion Detection Frameworks for Cloud Computing Environments". International Journal of Innovative and Applied Research (2014), Volume 2, Issue (7): 61-64.

Short Bio Data for the Authors

Amarbeer Kaur She obtained her B.Tech (computer science & engineering) from College of Engineering and Management, Kapurthala, Punjab, India, pursuing M.Tech (computer science & engineering) from Sai Institute of Engineering and Technology, Manawala, Amritsar, Punjab, India. Her area of interest is Cloud Computing and Security threat in cloud computing

Nitin bhagat is working as an assist. professor in Department of Computer Science & Engineering, Sai Institute of Engineering and Technology, Manawala, Amritsar, Punjab, India. He obtained his B.Tech (computer science engineering) from Guru Nanak Dev University, Punjab, India, M.Tech (computer science & engineering from Guru Nanak Dev University, Punjab, India.