Volume 5, Issue 7, July 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Service Model Specific Security Requirements and Threats in Cloud Computing

Kulvinder Singh*, Sarita Negi
Department of Computer Science
Doon Institute of Engineering & Technology
Uttarakhand, India

Abstract: Cloud computing offers an innovative business model for organizations to avail IT services without a huge upfront capital expenditure on hardware and software. Cloud computing shares resources never shared before, creating new risks and demanding new security practices. With the drastic growth in the use of the cloud environment, that is increase in number of users, (CSP's) cloud service providers and cloud based applications, threats and risk area is also growing rapidly. Despite of a low cost business opportunity, the organizations are less impressed by this paradigm. Privacy and security concerns are among the top hurdles to the wider adoption of the cloud technology and services. The primary concern of cloud provider's is to provide security and trust architecture to the customers so that their data is isolated from each other in multitenant environment. The goal of this paper is to explore the most recent threats which are brought into account through various literatures with the help of various surveys and case studies worldwide. We have inculcated the severe security demands of cloud while it is adopted as public, private or hybrid form, or delivered as SaaS, PaaS or IaaS.

Key words: Cloud computing, Reverse Proxy, SaaS, PaaS, IaaS and Security threats

I. INTRODUCTION

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It provides us with online data storage, infrastructure and applications. Cloud computing becoming popular day by day as the user getting aware of this cost effective and user friendly environment. However users still doubt the reliability of the cloud applications and security of personal data in cloud databases. Today the cloud computing business giants like Amazon, Microsoft, Google and IBM etc are working hard to convince and demonstrate to the cloud customers the security, integrity and reliability of cloud environment. Cloud computing is emerging as a replacement to Grid computing, Distributed computing and Parallel computing. However security has been a primary and high priority concern since the evolution of this technology, but it have evolved very fast within a decade. Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's (IT) existing capabilities. In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Despite of all the hype surrounding the cloud, customers are still reluctant to deploy their business in the cloud. Security issues in cloud computing has played a major role to slow down its acceptance, in fact security ranked first as the greatest challenge of cloud computing.

II. ESSENTIAL CHARACTERISTICS OF CLOUD

A typical cloud has five essential characteristics.

A. On demand self service. A consumer can unilaterally customize computing capabilities, such as server time and network storage, as and when needed automatically without requirement human interaction with cloud service's provider.

B. Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and personal digital assistants (PDAs))

C. Resource pooling. (Location independence) The cloud provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the subscriber generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data centre). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

D. Rapid elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

E. Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

III. DEPLOYMENT MODELS

Deployment models define the type of access to the cloud, i.e., how the cloud is located? Cloud can have any of the four types of access: Public, Private, Hybrid and Community.

A. Private Cloud It is also known as Internal Cloud or on-premises Cloud. It is managed and operated by single organization or a group. It is also known as internal cloud or on-premise cloud, a private cloud provides a limited access to its resources and services to consumers that belong to the same organization that owns the cloud. In other words, the infrastructure that is managed and operated for one organization only, so that a consistent level of control over security, privacy, and governance can be maintained.

B. Public Cloud Public clouds are owned and operated by third parties; they deliver superior economies of scale to customers, as the infrastructure costs are spread among a mix of users, giving each individual client an attractive low-cost, "Pay-as-you-go" model. All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. These organizations in a community that shares common concerns (like security, governance, compliance etc).

C. Hybrid Cloud The Hybrid Cloud is mixture of public and private cloud. However, the critical activities are performed using private cloud while the non-critical activities are performed using public cloud. The Hybrid cloud environment is capable of providing on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload. are managed and supported by the cloud provider. One of the advantages of a Public cloud is that they may be larger than an enterprises cloud, thus providing the ability to scale seamlessly, on demand.

D. Community Cloud The Community Cloud allows systems and services to be accessible by group of organizations. It refers to an special purpose cloud environment which is shared and managed by number of related organization participating in a common domain or vertical market. This deployment model share resources with many

IV. SERVICE MODELS OF CLOUD COMPUTING

There are many other service models all of which can take the form like XaaS, i.e., Anything as a Service. This can be Network as a Service, Business as a Service, Identity as a Service, Database as a Service, Management as a Service or Strategy as a Service. The Infrastructure as a Service (IaaS) is the most basic level of service. Each of the service models makes use of the underlying service model, i.e., each inherits the security and management mechanism from the underlying model, as shown in the following diagram:

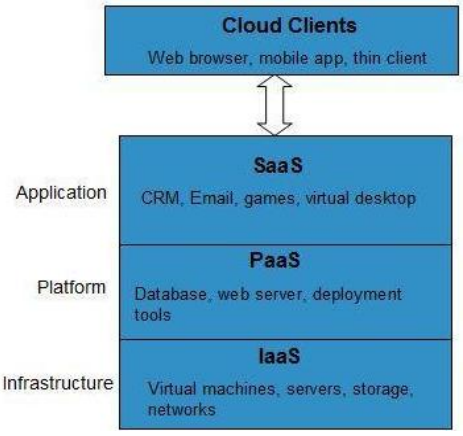

Fig.1 Service model inheritance mechanism

A. IAAS: Infrastructure as a Service delivers computer infrastructure (such as a platform virtualization environment), storage, and networking. Instead of having to purchase software, servers, or network equipment, users can buy these as a fully outsourced service that is usually billed according to the amount of resources consumed. Basically, in exchange for a rental fee, a third party allows you to install a virtual server on their IT infrastructure. Compared to SaaS and PaaS, IaaS users are responsible for managing more: applications, data, runtime, middleware, and O/S. Vendors still manage virtualization, servers, hard drives, storage, and networking. What users gain with IaaS is infrastructure on top of which they can install any required platforms. Users are responsible for updating these if new versions are released. It is most basic layer in service models, it deals with Virtual Machines, Storage (Hard Disks), Servers, Network, Load Balancers etc. Examples: Amazon EC2, Windows Azure, Rackspace, Google Compute Engine.

Table I Security threats and requirements in IaaS

Security Requirements	**Security Threats**
Hardware security	Hardware theft
Hardware reliability	Hardware modification
Infrastructure control	Hardware interruption
Network protection	Network attacks
Infrastructure control	Connection flooding
Network resources protection	DDOS
Legal not abusive use of cloud computing.	Natural disaster
	Misuse of infrastructure

B. PAAS (Platform as a Service). The most complex of the three, cloud platform services or "Platform as a Service" (PaaS) deliver computational resources through a platform. What developers gain with PaaS is a framework they can build upon to develop or customize applications. PaaS makes the development, testing, and deployment of applications quick, simple, and cost-effective, eliminating the need to buy the underlying layers of hardware and software. One comparison between SaaS vs. PaaS has to do with what aspects must be managed by users, rather than providers: With PaaS, vendors still manage runtime, middleware, O/S, virtualization, servers, storage, and networking, but users manage applications and data.It is a layer on top of IaaS, it includes runtimes (like java runtimes), Databases (like mySql, Oracle), Web Servers (tomcat etc), AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos.

Table II Security threats and requirements in PaaS

Security Requirements	**Security Threats**
Cloud management control security	Exposure in network
Secure images	Session hijacking
Application security	Software modification
Data security, (data in transit, data at rest)	Traffic flow analysis
Access control	Defacement
Virtual cloud protection	Disrupting communication
Communication security	Software interruption (deletion)
	DDOS
	Impersonation
	Connection flooding

C. SAAS*:* Cloud application services or "Software as a Service" (SaaS) are probably the most popular form of cloud computing and are easy to use. SaaS uses the Web to deliver applications that are managed by a third-party vendor and whose interface is accessed on the clients' side. Most SaaS applications can be run directly from a Web browser, without any downloads or installations required. SaaS eliminates the need to install and run applications on individual computers. With SaaS, it's easy for enterprises to streamline their maintenance and support, because everything can be managed by vendors: applications, runtime, data, middleware, O/S, virtualization, servers, storage, and networking. Gmail is one famous example of an SaaS mail provider. It is a layer on top of PaaS, it includes applications like email (Gmail, Yahoo mail etc), Social Networking sites (facebook etc), Microsoft Office 365 etc.

Table III Security threats and requirements in SaaS

Security Requirements	**Security Threats**
Access control	Privacy breach
Privacy in multitenant environment	Traffic flow analysis
Service availability	Exposure in network
Software security	Session hijacking
Communication protection	Data interruption (deletion)
Data protection from exposure (remnants)	Interception
	Impersonation
	Modification of data at rest/transit.

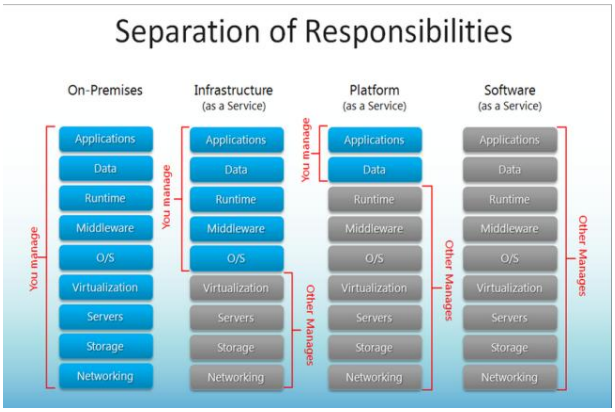

Fig. 2 Separation of responsibilities in IaaS, PaaS & SaaS

V. COMMON SECURITY CONCERNS

A. Data breaches.

It constitutes leakage, manipulation or loss of data by intrusion attack on the cloud. A virtual machine could use side-channel timing information to extract private cryptographic keys in use by other VMs on the same server. A malicious hacker wouldn't necessarily need to go to such lengths to pull off that sort of feat, though. If a multitenant cloud service database isn't designed properly, a single flaw in one client's application could allow an attacker to get at not just that client's data, but every other client's data as well.

Possible solution to this attack is use of proper encryption techniques or probably using multilayered encryption.

B. Account or service traffic hijacking.

Cloud computing adds a new threat to account & traffic problems. If an attacker gains access to your credentials, he or she can track your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. "Your account or services instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks," according to the report. An example to this is XSS attack on Amazon in 2010 that let attackers hijack credentials to the site.

Organizations should not allow employees to share or transfer credentials on the network and also aware clients about threats of sharing users credentials of cloud, and they should use strong two-level authentication techniques where possible.

C. Insecure interfaces and APIs.

IT administrators rely on interfaces for cloud provisioning, management, orchestration, and monitoring. APIs are integral to security and availability of general cloud services. From there, organizations and third parties are known to build on these interfaces, injecting add-on services. "This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third parties in order to enable their agency," the report notes.

Possible solution to this attack is that the developers should put more efforts in the design of APIs so that there may be no loop hole for the attackers to break through APIs, and design should be compatible to the underlying SSL libraries.

D. Denial of Service

DoS are mostly flooding attacks & has been an Internet threat for years, but it becomes more problematic in the age of cloud computing when organizations are dependent on the 24/7 availability of one or more services. DoS outrages can cost service providers & customers both. It is proved pricey to customers who are billed based on compute cycles and disk space consumed. While an attacker may not succeed in knocking out a service entirely, he or she "may still cause it to consume so much processing time that it becomes too expensive for you to run and you'll be forced to take it down yourself,"

DoS attacks can be avoided using a reverse proxy server and they can also be reduced using advanced firewalls that may filter repeating messages or requests.

E. Malicious Insiders

Malicious insiders can be a current or former employee, a contractor, or a business partner who gains access to a network, system, or data for malicious purposes. In an improperly designed cloud scenario, a malicious insider can wreak even greater havoc. From IaaS to PaaS to SaaS, the malicious insider has increasing levels of access to more critical systems and eventually to data. In situations where a cloud service provider is solely responsible for security, the risk is great. "Even if encryptions is implemented, if the keys are not kept with the customer and are only available at data-usage time, the system is still vulnerable to malicious insider attack,"

One best way to avoid malicious insider is to enable two or three stage password protection mechanism which require two or more person to get the cloud credentials. Another technique is to keep minimum person in administration of cloud server credentials.

F. Cloud Abuse

An example of cloud abuse is a bad guy using a cloud service to break an encryption key too difficult to crack on a standard computer. Another example might be a malicious hacker using cloud servers to launch a DDoS attack, propagate malware, or share pirated software. The challenge here is for cloud providers to define what constitutes abuse and to determine the best processes for identify it.

G. Insufficient Due Diligence

Insufficient due diligence may be understood as an organization that embrace the cloud without fully understanding the cloud environment and associated risks. For example, entering the cloud can generate contractual issues with providers over liability and transparency. What's more, operational and architectural issues can arise if a company's development team isn't sufficiently familiar with cloud technologies as it pushes an app to the cloud.

Legal formalities and basic resources must be available to the organization before joining a cloud computing environment.

H. Shared Technology Vulnerabilities

Cloud service providers share infrastructure, platforms, and applications to deliver their services in a scalable way. "Whether it's the underlying components that make up this infrastructure (e.g. CPU caches, GPUs, etc.) that were not designed to offer strong isolation properties for a multi-tenant architecture (IaaS), re-deployable platforms (PaaS), or multi-customer applications (SaaS), the threat of shared vulnerabilities exists in all delivery models,".

VI. CONCLUSION

The basic characteristics of cloud that are essential to work in a cloud environment is *on demand self service, elasticity, availability, resource pooling and measured service.* However all of these properties of cloud are highly affected by security threats in different service models. This paper focused on service model level threats and corresponding security requirements. With a keen eye on the security requirements provided in this paper, a cloud business can work better in all respects and enhance the ability to achieve business goals with less investment in recovery after attacks. An example of this was in 2011 Amazon EC2 was attacked by black hats and services of Amazon cloud was down for one day, this results in loss of billions of dollars to Amazon. Such incidents also question the credibility of cloud services and customers are jeopardize whether to use cloud services or not which they think are vulnerable. Apart from implementation of security checks service model wise as given in this paper, there are possibilities that deployment models may be considered separately for the threats which they are prone to, and also smaller categories of service models (business as a service, network as a service, learning as a service, storage as a service, anything as a service) may be researched reviewed and tested against security threats.

REFERENCES

[1] Shuai Zhang, Shufen Zhang, Xuebin Chen, Xiuzhen Huo, "*Cloud Computing Research and Development Trend"*, 2010 Second International Conference on Future Networks.

[2] Siyuan Xin, Yong Zhao, Yu Li, "*Property-Based Remote Attestation Oriented to Cloud Computing"***,** 2011 Seventh International Conference on Computational Intelligence and Security2011 .

[3] Amazon.com, Amazon Web Services (AWS). Online at http://aws.amazon.com.

[4] http://www.pcmag.com/article2/0,2817,2372163,00.asp.

[5] http://www.ibm.com/cloud-computing/in/en/what-is-cloud-computing.html.

[6] Kangchan Lee, "*Security Threats in Cloud Computing Environments1"***,** International Journal of Security and Its Applications Vol. 6, No. 4, October, 2012

[7] P. A. Karger, "*Multi-Level Security Requirements for Hypervisors*", ISBN: 0-7695-2461-3, 21st Annual Computer Security Applications Conference, **(2005)** December 5-9, pp. – 275.

[8] http://www.informationweek.com/cloud/infrastructure-as-a-service/9-worst-cloud-security-threats/d/d-id/1114085.

[9] Cloud Computing and Security, A Natural Match, http://www.trustedcomputinggroup.org/files/resource_files/1F4DEE3D-1A4B-B294-D0AD0742BA449E07/Cloud%20Computing%20and%20Security%20Whitepaper_July29.2010.pdf, **(2010)**.

[10] www.sersc.org/journals/IJSIA/vol6_no3_2012/9.pdf.

[11] Sun-Ho Lee and Im-Yeong Lee, "*Secure Index Management Scheme on Cloud Storage Environment*", International Journal of Security and Its Applications Vol. 6, No. 3, July, 2012.

[12] Mahima Joshi, Yudhveer Singh Moudgil, "*secure cloud storage***",** ISSN:2249-5789 International Journal of Computer Science & Communication Networks,Vol 1(2), 171-175 **.**

[13] www.ijarcsse.com/docs/**papers**/9_September2012/.../V2I900174.pdf.

[14] http://www.academia.edu/2179974/Research_Challenges_and_Security_Issues_in_Cloud_Computing.

[15] https://en.wikipedia.org/wiki/Cloud_computing_security.

