International Journal of Computer Sciences and Engineering Open Access
Survey Paper Volume-2, Issue-11 E-ISSN: 2347-2693

A Survey on Security Threats and Attacks in Cloud Computing

Mr.V.P.Muthukumar[1] and R.Saranya[2*]

[1]*Department of computer science*
[2] *Department of Computer Science*
[1,2*]*Vivekananda College of Arts and Sciences For Women, Namakkal, Tamil Nadu, India*

www.ijcaonline.org

Received: Oct/22/2014 Revised: Nov/04/2014 Accepted: Nov/18/2014 Published: Nov/30/2014

Abstract -Cloud computing is one of today's most exciting technologies due to its ability to reduce costs associated with computing while increasing flexibility and scalability for computer processes. During the past few years, cloud computing has grown from being a promising business idea to one of the fastest growing parts of the IT industry. IT organizations have expresses concern about critical issues (such as security) that exist with the widespread implementation of cloud computing. The security for Cloud Computing is emerging area for study and this paper provide security topic in terms of cloud computing based on analysis of Cloud Security threats and Technical Components of Cloud Computing.

Keywords: Cloud Computing, Security, Threats, attacks, Cloud Service Provider

I. INTRODUCTION

Cloud computing is a model for enabling service user's ubiquitous, convenient and 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. Cloud computing enables cloud services. The security architecture and functions highly depend on the reference architecture, and this paper shows the reference architecture and the main security issues concerning this architecture.

A. Technical Components of Cloud Computing

As shown in the Figure 1, key functions of a cloud management system is divided into four layers, respectively the Resources & Network Layer, Services Layer, Access Layer, and User Layer. Each layer includes a set of functions:

- The Resources & Network Layer manages the physical and virtual resources.
- The Services Layer includes the main categories of cloud services, namely, NaaS, IaaS, PaaS, SaaS/CaaS, the service orchestration function and the cloud operational function.
- The Access Layer includes API termination function, and Inter-Cloud peering and federation function.
- The User Layer includes End-user function, Partner function and Administration function.

Other functions like Management, Security & Privacy, etc. are considered as cross-layer functions that covers all the layers. The main principle of this architecture is that all these layers are supposed to be optional. This means that a cloud provider who However, from the security perspective, the principal of separation requires each layer to take charge of certain responsibilities. In event the security controls of one layer are by passed (e.g. access layer), other security functions could compensate and thus should be implemented either in other layers or as cross-layer functions.

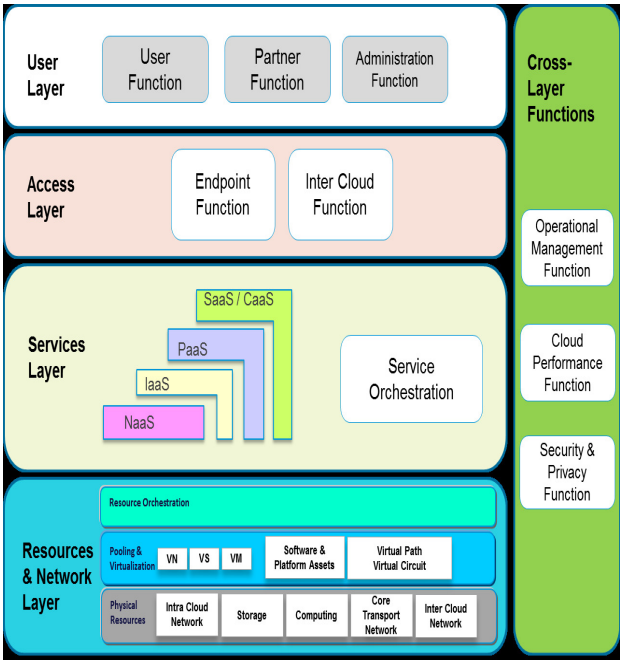

Figure 1: The Cloud Computing Components

Corresponding Author: R. Saranya

II SERVICE MODELS

a. *Software as a Service (SaaS)*

Cloud based applications or software run on distant computers in the cloud that are owned and operated by others and that connect to user's computers via Internet usually by a web browser.

b. *Platform as a Service (PaaS)*

Platform as a Service provides a cloud based environment with everything required to support the complete life cycle of building and delivering web based(cloud) applications, without the cost and complexity of buying and managing the underlying hardware, software, provisioning and hosting.

c. *Infrastructure as a Service (IaaS)*

Infrastructure as a Service provides companies with computing resources including servers, networking, storage and data centre space on a pay-per-use basis.

.III ESSENTIAL CHARACTERISTICS

a. *On-Demand Self-Service*

This means that cloud services can be used as and when required without prior subscription. A consumer can unilaterally upgrade/degrade computing capabilities, such as server time, data storage and network storage, automatically as and when needed without requiring human interaction with each service provider.

b. *Ubiquitous Network Access*

The cloud offers infinite network access to vast infrastructure and computing resources such as storage facility, memory, processor, hosting etc. The available resources can be accessed over the Internet through standard mechanisms.

c. *Resource Pooling*

The cloud uses shared pool of resources which is located at various parts of world, making the cloud location-independent. The providers serve multiple clients, customers or tenants with different physical and virtual resources dynamically assigned and reassigned according to the customer demand.

d. *Rapid Elasticity*

The computing capabilities can be elastically assigned and released, in some cases automatically, with demand. But to the consumer, the capabilities available for provisioning often appear to be unlimited and can be changed in any quantity at any time.

e. *Measured Service*

The cloud services are controlled and monitored by the cloud service provider. Measured service is crucial for billing, resource optimization, access control, capacity planning and others. This also provides transparency for both the provider and the consumer of the utilized service.

IV RISKS TO CLOUD COMPUTING

In cloud computing the service provider provides resources such as software, platform and infrastructure. The user information/data also resides in the cloud. The risk with this type of service is that the data can be abused, stolen, distributed, compromised or harmed. There is no guarantee that the user's data will not be sold to its competitor.

Other risks include privacy, data protection, ownership, location and lack of reliable audit standard to data security procedure of most cloud service providers.

a. *Privacy Issues*

Privacy is difficult to achieve using traditional information security systems, and so is one of the challenging area of Cloud Computing. Cloud computing has significant implications for the privacy of personal information as well as maintaining the confidentiality of business and government information. In public cloud various sensitive information are given to the hands of a third party service provider whose cloud infrastructure may not have proper regulations and could propagate through geographical borders that impact both legal and regulatory requirements of the information being propagated or stored. Cloud users must be aware of the contract they sign with service provider and should be informed about the service provider's privacy and security guidelines and practices.

b. *Data Ownership and Content Disclosure Issues*

Another issue which is to be considered before migrating to cloud is data ownership of the information residing on the cloud. Once the data is put to the cloud, not only the privacy is lost, the data ownership and the right of data content disclosure is also lost. Cloud users must protectively mark(TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED, PROTECT) their information and explicitly specify the ownership of information in the service contract.

c. *Data Confidentiality*

The confidentiality of a system is guaranteed if it prevents unauthorized gathering of information. Cryptographic techniques and access controls based on strong authentication are normally used to protect confidentiality. The data in a cloud computing system is very often in motion due to the system's dynamic and open nature. A cloud provider must be able to store this data on a server of its own choice in order to optimize its infrastructure capacity and ensure the necessary performance. These processes are usually outside the customer's sphere of influence and can lead to confidentiality problems, for instance, if the data crosses territorial borders or is stored on a less secure system.

d. Data Location

Another major concern about cloud computing is the data location. Cloud computing offers high degree of data mobility. After the data is handed over to the cloud provider, the data owner have no control over the location of data in the cloud. Where does the data reside that has been created by data owners? The countries legal protection will not be applicable to the data once it is moved outside the country. A foreign government may be able to access the data. If that country has laws that you are comfortable with, data may be physically stored in database with other company's data. To achieve regulatory compliance in the cloud, it requires effort from both users and cloud provider, the users know about the information requirements and can communicate that clearly to the cloud provider and the cloud provider is transparent and willing to provide regulatory rules required to protect the assets.

e. Data Breaches

A malicious hacker can extract private cryptographic keys if the multi-tenant service provider database is not designed properly, a single flaw in one client's application could allow to get not just client's data but every other client's data as well. You can encrypt the data to reduce the impact but if the encryption key is lost, your data will be lost.

f. Control Issues

Cloud especially public cloud is highly uncontrollable. In order to control cloud services and practices use of legal, regulatory, compliance and certification practices are recommended which is quite difficult to maintain. The location-independency makes it more difficult to achieve regulatory security compliance.

g. Service Traffic Hijacking

If an attacker gain access to user's credentials, the attacker can monitor user activities, manipulate user data and can return falsified information and can redirect client to illegitimate sites. The user's account will become new base for the attacker. To prevent this protect the credentials; avoid sharing of credentials between users and services.

h. Insecure Interfaces and APIs

Administrators rely on interfaces for cloud provisioning, management, orchestration and monitoring and APIs are integral to security and availability of general cloud services. Organizations and Third parties build on these interfaces injecting add-on services. This increase risk as organization may be required to exchange the credentials to the third party. An organization must properly understand the implications associated with cloud provisioning, management, orchestration and monitoring.

i. Denial of Service

The organizations are dependent on 24/7 availability of one or more services. A cloud provider uses virtual machines that run on physical hosts which are shared resources. These resources which include networking systems can be overloaded in certain situations. If one customer is target of attack it is possible that unrelated customer is also affected by the same attack. The cloud provider must protect customers from such attacks. The customer must be aware of the potential and take steps to provide assurances that their services are not adversely affected.

V INFORMATION SECURITY POLICIES

In Cloud computing technology there are a set of important policy issues, which include issues of privacy, security, anonymity, telecommunications capacity, government surveillance, reliability, and liability, among others . But the most important between them is security and how cloud provider assures it. Generally, Cloud computing has several customers such as ordinary users, academia, and enterprises who have different motivation to move to cloud. If cloud clients are academia, security effect on performance of computing and for them cloud providers have to find a way to combine security and performance. For enterprises the most important problem is also security but with different vision. For them high performance may be not as critical as academia. Well-known Gartner's seven security issues which cloud clients should advert as mentioned below .

a. Privileged user access

Sensitive data processed outside the enterprise brings with it an inherent level of risk because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs.

b. Regulatory compliance

Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications.

c. Data location

When clients use the cloud, they probably won't know exactly where their data are hosted. Distributed data storage is a usual manner of cloud providers that can cause lack of control and this is not good for customers who have their data in local machine before moving from local to cloud.

d. Data segregation

Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure all. Encryption and decryption is a classic way to cover security issues but heretofore it couldn't ensure to provide perfect solution for it.

e. Recovery

If a cloud provider broke or some problems cause failure in cloud sever what will happen to users' data? Can cloud provider restore data completely? Moreover clients prefer don't get permission to third-party companies to control their data. This issue can cause an impasse in security.

f. Investigative support

Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers.

g. Long-term viability

Ideally, cloud computing provider will never go broke or get acquired by a larger company with maybe new policies. But clients must be sure their data will remain available even after such an event.

VI THREATS FOR CLOUD SERVICE PROVIDERS

a. Responsibility Ambiguity

Different user roles, such as cloud service provider, cloud service user, client IT admin, data owner, may be defined and used in a cloud system. Ambiguity of such user roles and responsibilities definition related to data ownership, access control, infrastructure maintenance, etc, may induce business or legal dissention (Especially when dealing with third parties. The cloud service provider is somehow a cloud service user).

b. Protection Inconsistency

Due to the decentralized architecture of a cloud infrastructure, its protection mechanisms are likely to be inconsistency among distributed security modules. For example, an access denied by one IAM module may be granted by another. This threat may be profited by a potential attacker which compromises both the confidentiality and integrity.

c. Evolutional Risks

One conceptual improvement of cloud computing is to postpone some choices from the design phase to the execution phase. This means, some dependent software components of a system may be selected and implemented when the system executes. However, conventional risk assessment methodology can no longer match such an evolution. A system which is assessed as secure during the design phase may exploit vulnerabilities during its execution due to the newly implemented software components.

d. Business Discontinuity

The "as a service" feature of cloud computing allocates resources and delivers them as a service. The whole cloud infrastructure together with its business workflows thus relies on a large set of services, ranging from hardware to application. However, the discontinuity of service delivery, such as black out or delay, may bring out a severe impact related to the availability.

e. Supplier Lock-in

The platform of a service provider is built by some software and hardware components by suppliers. Some supplier-dependent modules or workflows are implemented for integration or functionality extension. However, due to the lack of standard APIs, the portability to migrate to another supplier is not obvious. The consequence of provider locked-in could be a lack of freedom regarding how to replace a supplier.

f. License Risks

Software licenses are usually based on the number of installations, or the numbers of users. Since created virtual machines will be used only a few times, the provider may have to acquire from more licenses than really needed at a given time. The lack of a "clouded" license management scheme which allows to pay only for used licenses may cause software use conflicts.

g. Bylaw Conflict

Depending on the bylaw of hosting country, data may be protected by different applicable jurisdiction. For instance, the USA Patriot Act may authorize such seizures. EU protects cloud service user's private data, which should not be processed in countries that do not provide a sufficient level of protection guarantees. An international cloud service provider may commit bylaws of its local datacenters which is a legal threat to be taken into account.

h. Bad Integration

Migrating to the cloud implies moving large amounts of data and major configuration changes (e.g., network addressing). Migration of a part of an IT infrastructure to an external cloud service provider requires profound changes in the infrastructure design (e.g. network and security policies). A bad integration caused by incompatible interfaces or inconsistent policy enforcement may evoke both functional and non-functional impacts.

i. Unsecure Administration API

The administration middleware standing between the cloud infrastructure and the cloud service user may be not sure with insufficient attention devoted to sanitation of cloud service user inputs and authentication. Non-protected APIs, mostly administration APIs becomes a target of choice for attackers. This is not specific to cloud environment. However, the service-oriented approach makes APIs a basic building block for a cloud infrastructure. Their protection becomes a main concern of the cloud security.

j. Shared Environment

Cloud resources are virtualized, different cloud service users (possibly competitors) share the same infrastructure. One key concern is related to architecture compartmentalization, resource isolation, and data segregation. Any unauthorized and violent access to cloud service user's sensitive data may compromise both the integrity and confidentiality.

VII CLOUD COMPUTING IN SECURITY ISSUSES

a. Cloud Computing Security

Cloud Computing Security as "Cloud computing security (sometimes referred to simply as "cloud security") is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing."

b. Security Issues Associated with the Cloud

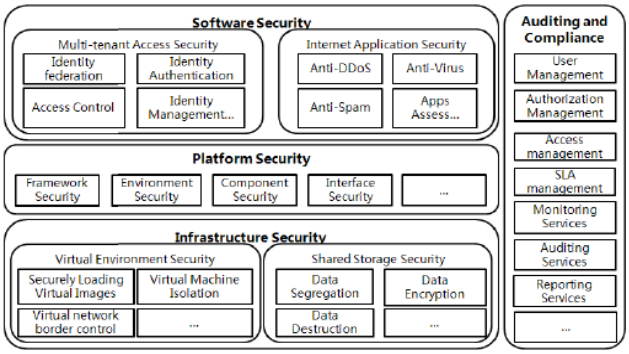

Figure 1 Cloud computing security architecture

There are many security issues associated with cloud computing and they can be grouped into any number of dimensions. Before making a choice of cloud vendors, users should ask the vendors for seven specific safety issues such as Privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support and long-term viability Cloud Security Alliance (CSA) is gathering solution providers, non-profits and individuals to enter into discussion about the current and future best practices for information assurance in the cloud. The CSA has identified thirteen domains of concerns on cloud computing security .According to the SPI service delivery models, deployment models and essential characteristics of cloud, there are security issues in all aspects of the infrastructure including network level, host level and application level.

Attacks in cloud

Nowadays, there are several attacks in the IT world. Basically, as the cloud can give service to legal users it can also service to users that have malicious purposes. A hacker can use a cloud to host a malicious application for achieve his object which may be a DDoS attacks against cloud itself or arranging another user in the cloud. For example, assume an attacker knew that his victim is using typical cloud provider, now attacker by using same cloud provider can sketch an attack against his victim. This situation is similar to this scenario that both attacker and victim are in same network but with this difference that they use virtual machines instead of physical network.

a. DDoS attacks against Cloud

Distributed Denial of Service (DDoS) attacks typically focus high quantity of IP packets at specific network entry elements; usually any form of hardware that operates on a Blacklist pattern is quickly overrun and will become in out of- service situation. In cloud computing where infrastructure is shared by large number of clients, DDoS attacks make have the potential of having much greater impact than against single tenanted architectures. If cloud has not plenty resource to provide services to its costumers then this is may be cause undesirable DDoS attacks. Solution for this event is a traditional solution that is increase number of such critical resources. But serious problem is when a malicious user deliberately done a DDoS attacks using bot-net. Most network countermeasures cannot protect against DDoS attacks as they cannot stop the deluge of traffic and typically cannot distinguish good traffic from bad traffic. Intrusion Prevention Systems (IPS) are effective if the attacks are identified and have pre-existing signatures but are ineffectual if there is legitimate content with bad intentions. Unfortunately, similar to IPS solutions, firewalls are vulnerable and ineffective against DDoS attacks because attacker can easily bypass firewalls and also IPSs since they are designed to transmit legitimate traffic and attacks generate so much traffic from so many distinct hosts that a server, or for cloud its Internet connection, cannot handle the traffic . It may be more accurate to say that DDoS protection is part of the Network Virtualization layer rather than Server Virtualization. For example, cloud systems use virtual machines can be overcome by ARP spoofing at the network
layer and it is really about how to layer security across multivendor networks, firewalls and load balances.

b. Cloud against DDoS attacks

DDoS attacks are one of the powerful threats available in world, especially when launched from a botnet with huge numbers of zombie machines. When a DDoS attack is launched, it sends a heavy flood of packets to a Web server from multiple sources. In this situation, the cloud may be part of the solution. it's interesting to consider that websites experiencing DDoS attacks which have limitation in server resources, can take advantage of using cloud that provides

CONCLUSION

Doubtless, Cloud computing helps IT enterprises use various techniques to optimize and secure application performance in a cost-effective manner. Additionally, just because the software can run in a Virtual machine does not mean that it performs well in cloud environment necessarily. Thereupon, in cloud there are risks and hidden costs in managing cloud compliance. The key to successful cloud computing initiatives is achieving a balance between the business benefits and the hidden potential risks which can impact efficacy. Cloud providers often have several powerful servers and resources in order to provide appropriate services for their users but cloud is at risk similar to other Internet-based technology. In the other hand, they are also at risk of attacks such as powerful DDoS attacks similar other Internet-based technology. As a solution, cloud providers can add more resource to protect themselves from such attacks but unfortunately there is no defense against a powerful DDoS attack which has good sapience. These issues which discussed in this paper are the main reasons that cause many enterprises which have a plane to migrate to cloud prefer using cloud for less sensitive data and store important data in their own local machines. It doesn't mean that all business IT needs to move to cloud. In addition, As a result, Moving toward cloud computing require to consider several parameters and most important of them is security.

REFERENCES

[1]. S. Roschke, et aI., "Intrusion Detection in the Cloud," presented at the Eighth IEEE International Conference on Dependable, AutonomIc and Secure Computing, Chengdu, China, 2009.

[2]. J Brodkin. (2008). Gartner Seven cloud-computing security risks. Available: http://www.networkworld.com/news/200S!07020Scloud. Html

[3]. D. L. Ponemon, "Security of Cloud Computing Users," 2010.

[4]. S. K. Tim Mather, and Shahed Latif, Cloud Security and Privacy: O'Reilly Media, Inc , 2009.

[5]. C. Almond, "A Practical Guide to Cloud Computing Security," 27 August 2009 2009.

[6]. http://cloudsecurity.trendmicro.com/

[7]. N. Mead, et ai, "Security quality requirements engineering (SQUARE) methodolgy," Carnegie Mellon Software Engineering Institute.

[8]. J. W.Rittinghouse and J. F.Ransome, Cloud Computing: Taylor and Francis Group, LLC, 2010.

[9]. T. Mather. (2011). Data Leakage Prevention and Cloud Computing. Available: http://www.kpmg.com/Globa1/Pages/default.aspx.

[10]. P. Coffee, "Cloud Computing: More Than a Virtual Stack," ed: salesforce.com. [II] z. Zorz, "Top 7 threats to cloud computing," 2010.

[11]. Security Management in the Cloud. Available http://mscerts.net/programming/Security%20Management%20in%20t he%20Cloud.aspx

[12]. (2010). Security Management in the Cloud – Access Control.

[13]. P. Sefton, "Privacy and data control in the era of cloud computing.