Security Mechanisms at different Levels in Cloud Infrastructure

Harpreet Saini
M. Tech CSE
Sri Balaji College of Engineering and Technology
Jaipur, Rajasthan

Amandeep Saini
M. Tech CSE
Jayoti Vidyapeeth Women's University
Jaipur, Rajasthan

ABSTRACT
Cloud computing refers to a set of services and resources offered to its consumers through internet. The user data and applications software shift to highly optimal data i.e. cloud. Either it may be a small or medium business infrastructure must focus on resource and information sharing among various users due to minimization of infrastructure cost. Cloud computing provides a lot of benefit, instead of its security is key inhibitor to cloud adoption. So, Cloud computing has brought various security threats which leads to lack of wide adoption of Cloud computing. This study aims to identify major security threats and security mechanisms and how to assess these security threats or vulnerabilities.

Keywords
Cloud Computing, Types of Cloud, Security Concerns, Security Mechanisms in cloud.

1. INTRODUCTION
Initially Cloud computing is a combination of cluster (all machines resides at same place) and grid computing (all machines at different place), where services and application run on a distributed network. These networks offers shared pool of services such as data storage, access services on-line and many more. Today, various companies such as Google (Google App Engine), Amazon (Amazon Web Services), IBM (Smartcloud), SalesForce.com and Microsoft (Azure) provides cloud services on the bases of pay-per-use. Unlike traditional computing , cloud computing do not need to set up any network like laying out wires, cooling systems, installing required software into each machine. But with cloud infrastructure, the thing only we need is a browser in each workstation along with internet connection and the work is ready to go. This helps to shift the organizations to cloud platform. In the Cloud infrastructure resources are virtual, limitless and detail of the physical system is abstracted from user. These services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). A public cloud is available publically whereas a private cloud is restricted to a particular organization. A hybrid cloud combines multiple clouds whereas a community cloud share resources and services between various organizations. Even though, there are lot of benefits provided by Cloud computing but various security threats and risks are introduced in cloud infrastructure.

1.1 Organization of the Paper
In this paper, the integrals of cloud computing are reviewed first, then security concerns and vulnerabilities in cloud computing followed by a survey of the security mechanisms. Finally we discuss about the assessment of the risk.

2. INTEGRALS OF CLOUD COMPUTING
2.1 Cloud Computing
Cloud computing is a term used to describe a new class of network based computing that take place over the internet, where machines with large data centers controlled, configured and provisioned to deliver services in a expandable manner. The "cloud" symbol is used to represent specifically the boundary of a cloud environment. A cloud has a finite boundary to remotely provision the IT resources such as virtual server, physical server, software program, storage device, network device and services (Cloud) in a specific environment.

Fig 1: The Cloud Environment

The key characteristics of cloud computing is as follows.

- **On-demand Capabilities:** The required computer services provided by cloud service provider without any human interaction. Amazon web services (AWS), IBM, Google, and Salesforce.com are the on demand self-services provided by cloud service provider.
- **Ubiquitous Network access:** Cloud computing resources are available over the network using standard mechanisms. These mechanisms used to provide services on heterogeneous client platforms such as laptops, mobile devices and workstations.
- **Flexibility:** As per business scale up/down any number of nodes can be added or removed at any time in the cloud infrastructure.

- **Location Independent Resource Pooling:** Using multiple-tenant model, IT resources such as virtual machines, storage, network, e-mail services are pooled together to serve multiple consumers. As per user requirement physical and virtual resources dynamically allocated or reallocated.
- **Measured Services:** Cloud computing services provided to consumers on the basis of **"pay per use"**, more the consumption higher the bill.
- **Maintenance:** Application software does not require to be installed in each workstation, which supports easy maintenance.
- **Cost Effectiveness:** Sharing of cost in between large number of users from same or different locations due to centralized infrastructure.

2.2 Types of Clouds

Cloud has two classifications on the basis of deployment model and service model**.**

2.2.1 Cloud Deployment Models: Deployment model refers to where the cloud is located and for what purpose it is used. The four fundamental deployment models are:

- **Private Cloud:** Private clouds are restricted to particular organization. Private clouds may be either on-premise which is hosted in the enterprise or off-premise which can be hosted by third party. The key objective of private cloud is to provide extreme level of security and privacy.
- **Public Cloud:** Public cloud infrastructure represents a cloud environment which is available for public use and managed by an organization or a third party cloud service providers. Public cloud provides greatest level of effectiveness in shared resources, but instead of it they are also weak in terms of security and control than private clouds.
- **Community Cloud:** This model of cloud infrastructure is shared between organizations and communities that have communal concerns such as security, operation, strategy. Service are possessed and managed by organizations and third parties.
- **Hybrid Cloud:** A hybrid cloud is composition two or more clouds models (public, private or community) that offer standardized access to application and data. Even though, they are bound together as a unit but still they retain their unique identities.

*2.2.2 Cloud Service Models***:** Cloud computing can be comprises three service models that deliver the service.

- **Software as a Service (SaaS):** In cloud infrastructure, SaaS is a full-fledged operating environment that provides applications to the end users through a browser. SaaS reduces the need to organize the background of cloud infrastructure which includes technology, storage, network etc.
- **Platform as a Service (PaaS):** Paas is a platform for the creation of software that deployed over the web. Paas provides a platform that depends on application software, middleware and operating systems and may comprise the development environment that is presented to a customer as a service. A consumer does not require to controls the integrals of cloud infrastructure but only has to control the deploy applications such as: middleware data integration tools.
- **Infrastructure as a Service (IaaS):** The bottom of cloud pyramid is the infrastructure as a service along with virtual storage, virtual network, virtual machines (e.g. VMware, hypervisor) as resources that client can provision. IaaS is neither the software nor the database, it just the infrastructure.

3. SECURITY- TRADITIONAL V/S CLOUD

In traditional data centers all resources such as storage, server everything might be co-located in single location or is limited to that organization. But in case of private cloud resources and management of the cloud is restricted to only within the organization. On the other hand, the public and hybrid cloud infrastructure is shared by multiple organizations and users across the geography. So, the one server might be located in America and another server in Europe and user takes advantage of services without knowing where the data centers are located. Security is one of the biggest concerns to moving mission-critical data to the cloud, but cloud computing may be more secure than the traditional approach such as client-server. Instead of building security into each application, security-as-a-service permits to the organization to build security at once and reuse it widely. Encryption provides more secure data that is exchanged between organizations in the private cloud, so no one can see or track the transactions that happened between them.

4. SECURITY CONCERNS IN CLOUD INFRASTRUCTURE

With the introduction of multiple users, multiple enterprises and a heterogeneous hardware infrastructure, numerous security concerns arises in cloud computing such as:

4.1 Multi-Tenancy

Multi-tenancy is a key security concern for both cloud clients and cloud service provider, virtual machines are co-located in a single server and sharing the same resources increases the data being exposed and enforcing steady security controls and measures is difficult respectively. Mutual client isolation is primary concern against multi-tenancy concerns. So, to overcome such kind of multi-tenancy concern isolation is required such as isolation of virtual machines, data, network communication, memory, executions. Multiple organizations have own security policies so, cloud service provider make sure that security policy is enforced very correctly in a steady way because underlying infrastructure is the same.

4.2 Velocity of Attack

Security threats amplify and spread quickly in a cloud known as velocity of attack factor. Cloud infrastructure is comparatively larger. So, similarity in the platforms or components employed by a cloud service provider increases the speed at which an attack can spread. This attack leads to potential loss due to an attack is comparatively higher. So, it is difficult to mitigate the spread of the attack. To counter the challenge of velocity of attack, cloud service provider need to adopt more robust security enforcement mechanisms (e.g. Defense-in-depth).

4.3 Data Ownership and Information Assurance

Information assurance concern for cloud users involves CIA triad.

- **Confidentiality:** Ensures unauthorized can't access the data.
- **Integrity:** Make sure that your data remain as it is, no modification should take place.
- **Availability:** Data and applications should be always available to authorized users.

Data ownership concerns for cloud clients such as:

- **Data and applications:** These are hosted by cloud service provider, who has access to the data, but owner is not the cloud service provider. This leads to unauthorized data access and misuse.
- **Encryption:** Data should be protected using encryption and access control mechanisms to ensure data ownership. So, data ownership becomes one of the major concerns in cloud environment.

4.4 Data Privacy

It is potential concern in private cloud because only legitimate clients can access data in the cloud environment. Private data may include individual identity of the client, details of the services requested by client and proprietary data of the client. So, the cloud service provider needs to ensure that private data of its clients is protected from unauthorized disclosure, because multiple organizations or users uses the same infrastructure and might have access your data.

5. VULNERABILITIES IN CLOUD INFRASTRUCTURE

5.1 VM Theft

VM Theft is a vulnerability that enables an attacker to copy or move a VM (Virtual Machine) in an unauthorized manner which results of inadequate control on VM files allowing unauthorized copies. So, copy and move restrictions are essential to safeguard against such kind of threat. A VM along with copy and move restrictions can't run on a hypervisor that installed on any other server.

5.2 Hyper Jacking

It enables an attacker to install a rogue hypervisor or virtual machine monitor (VMM) that can take control of the under laying server resources. An attacker can run unauthorized applications on a guest OS without the OS realizing it and also an attacker could control the interaction between the VMs and the under laying server. So, we need effective measures against hyper jacking such as secure launching of the hypervisor, scanning details of hardware-level to assess the integrity of the hypervisor and locating the presence of the rogue hypervisor.

5.3 Data Leakage

Confidential data stored on a third party cloud is potentially vulnerable to unauthorized access or manipulation but attacks on cloud service provider's control systems such as passwords lists could make all the client's data vulnerable. A concept of SCA (Side Channel Attacks) can be used for data leakage in cloud. SCA hosted at the same server and trying to get access data from another VM through common logs and cache data, then there is a possibility of data leakage.

5.4 Denial-of-Service Attack

It is an attempt to prevent legitimate users from accessing a resource or service by flooding various connection requests to the server. DoS attacks might affect software applications and network components that involves such as exhausting resources (e.g. network bandwidth or CPU cycles) and exploiting weaknesses in communication protocol (e.g. resetting of TCP session, corrupting domain name server's cache). A malicious client VM might be used to launch a DoS attack against the hypervisor. So, as a protective measure, resources consumption of a VM needs to be restricted.

6. SECURITY MECHANISMS IN CLOUD INFRASTRUCTURE

Security mechanisms in cloud infrastructure security at various levels such as at compute level, network level, application level etc.

6.1 Security at Compute Level

Securing system at compute level includes such as:

6.1.1 Physical Server Security: Identifying physical server application details including whether server will be used for specific applications or general purpose and these services provided on the server. User and/or user groups who can operate the server and their access privileges helps to secure the system. So, as protection measures in physical server security have to determine the authentication and authorization mechanisms, disabling unused hardware such as USB ports or drives.

6.1.2 Securing Hypervisor: Hypervisor security make sure that hypervisor is not attacked by an attacker. Attacks on the hypervisor impact all the VMs running on it. It is a single point of security failure in a cloud infrastructure. Protection of the hypervisor management system is critical because an insecure management system can make existing VMs vulnerable for attacks, can enable creation of new malicious VMs. The hypervisor security can be achieved by configuring strong security on the firewall between the management system and the network, providing direct access only to administrators to management server.

6.1.3 Securing VM: VM isolation and hardening is one of the security mechanism. So, if one particular VM in a cloud infrastructure has been compromised then it has to be isolated from rest of the resources and VMs to make sure that this attack doesn't get control over the rest of the virtual machine (VM) or infrastructure. VM hardening is a process of changing the default configuration in order to achieve greater security by using VM templates to provision new VMs, where antivirus software, security software such as data loss prevention product and other security measures are already installed.

6.1.4 Guest OS and Application Security: Guest OS hardening measures include deleting unused files and applying hardening checklists available for specific operating systems. Always install the guest OS in TCB (Trusted Computing Base) mode if the VM is to be used for critical applications. Basically TCB provide the security mechanisms to the OS such as user authentication, protection against viruses and many more. Application hardening measures include disallowing a vulnerable application from launching any executable files which is not trusted, creating or modify executing files and modifying sensitive areas of the guest OS. The OS has to be updated and software mechanisms such as

antivirus products should be up to date and applications also have to be secure and do regular updates on applications.

6.2 Security at Network Level

We covered security at compute level but we have to make sure that hypervisor and server is also secured. To do this securing system at network level includes such as:

6.2.1 Virtual Firewall: Regular firewall takes care of the communication between virtual infrastructure and rest of the network. But VM-to-VM communication have to be secured, because there will be some network communication between each of the virtual machine. In case of public cloud infrastructure several VMs might be belong to a particular organization and rest of the VMs might be belonging to another organization. So, this communication will not be protected by regular firewall and virtual firewall will ensure the traffic between each of the machines is secured.

6.2.2 Demilitarized Zone (DMZ): Two kind network we consider that is external and internal, internal network that we have. So, if all of internal network is exposed to external network becomes easy for an attacker to get access the network. Demilitarized zone provides relief from such kind of situation. It is a physical or logical network that limits the exposure of the nodes in the internal network from external network that adds additional layers of security against external attacks. An attacker has access only to the DMZ rather than any other part of the network.

6.2.3 Security Data-at-rest: Data-at-rest is that data which is not being transferred over a network because it is stored in a server or any other storage location. If data is not encrypted or if it is raw data that stored in physical storage, becomes easier for the attacker to use of the data. So, encryption provides confidentiality and integrity and reduces legal liabilities of a CSP due to an unauthorized disclosure of data on its cloud. Full disk Encryption is a key method to encrypt data-at-rest that resides on a disk.

6.2.4 Security Data-at–flight: Data-in-flight is that data which is being transferred over a network. As we explained earlier, data-at-rest which is stored like a file in a server but there will be data which is being sent in e-mail communication and client is trying to access that file. So, at network level data can be stolen or can be compromised but using encryption confidentiality and integrity can maintain and encryption is a key measure against sniffing (observing data) attacks.

6.2.5 Data Shredding: The deleted data by cloud client or a process leaves traces on the system, can be potential source of attacks because traces of deleted VMs can provide essential information to an attacker. Data shredding is a mechanism that permanently remove all the traces of the deleted data includes logs of VM, logs of data communication, logs of old files and folders.

6.3 Security at Application Level

Security at application level refers to provide security to applications by using software and hardware resources such that attackers are not able to get control over these applications. DoS is such kind of attack that affect the software application by sending a lot of request to access the site and unable to access that site by a legitimate user. Intrusion Detection is most popular method to protect against the DoS attack.

Intrusion Detection: It is a process of detecting such kind of entities and/or events that could compromise the security of the system. Intrusion detection system has following types.

- **Server Based IDS:** Analyzes activity logs, system calls, application logs and better view of the monitored system but high vulnerability for an attack on IDS itself.
- **Network Based IDS:** Analyzes communicating nodes, network traffic and poorer view of the system and low vulnerability for an attack on IDS itself.
- **Integrated IDS:** Combination of server and network based approaches.

6.4 Role based Access Control

To improve the security resource access or permission is given to subjects (users and processes) based upon their roles. Basically, role may represent a job function and permissions are associated with the role which provides simple and scalable control ability. Subject gets access to perform operations on resources based upon the roles assigned to them. In cloud infrastructure, Role based Access Control (RBAC) can be enabled for cloud clients by importing user groups using directory services of the client organization and CSP may use RBAC to control an administrative access to the hypervisor management system.

Table 1: Security at different levels

S.No.	Security at Different Levels	Target
1	**Security at Compute Level**	
1.1	Physical Server Security	Disabling unused h/w such as USB ports or drives.
1.2	Securing hypervisor	Configuring strong security on the firewall b/w the management system and the network.
1.3	Securing VM	Limit the resources that VM can consume to prevent DoS attack.
1.4	Guest OS and Application Security	Deleting unused files and installing the guest OS in TCB mode.
2	**Security at Network Level**	

2.1	Virtual Firewall	Ensures the traffic b/w each of the VMs is secured.
2.2	Demilitarized Zone	Add additional layers of security against external attacks.
2.3	Securing Data-at-rest	Full disk encryption is used.
2.4	Securing Data-in-flight	Encryption is key measure against sniffing attacks.
2.5	Data Shredding	Permanently removes all the traces of the deleted data.
3	**Security at Application Level**	Detecting events that compromise the security.
3.1	Intrusion Detection	
4	**Role Based Access Control**	Permissions are given to subjects based upon their roles.

7. RISK ASSESSMENT

The primary aim of risk assessment is to identify potential risks while operating in a cloud environment and it should be performed before moving to a cloud and also used to determine the actual scope for cloud adoption. So, risk assessment is very essential while decide into move application and data to cloud.

Steps to perform risk assessment such as:

1. Identify critical and sensitive assets includes data, applications and processes. Critical assets are necessary for the operation of the business and sensitive assets are those having high business values.
2. Identify potential risks such as user access control, data location etc, while they pose risk to the organization but if they planned or identify at beginning they can be managed.
3. After identification of the potential risk classify them into security levels.
4. Associating potential risks with critical assets and progress monitoring.
5. According to process monitoring if some risks are not assessed then reassess existing risks and identify new risks.

Compliance: Cloud adoption and operation for enterprise businesses need to abide by compliance policy. There are two kind of compliance such as internal policy compliance that control the nature of IT operations within an organization and also needs to maintain same compliance even when operating in cloud, and second is external regulatory compliance that includes legal legislation and industry regulations. External regulative compliance also controls the nature of IT operations related to flow of data out of an organization and it may differ based upon the type of business and information.

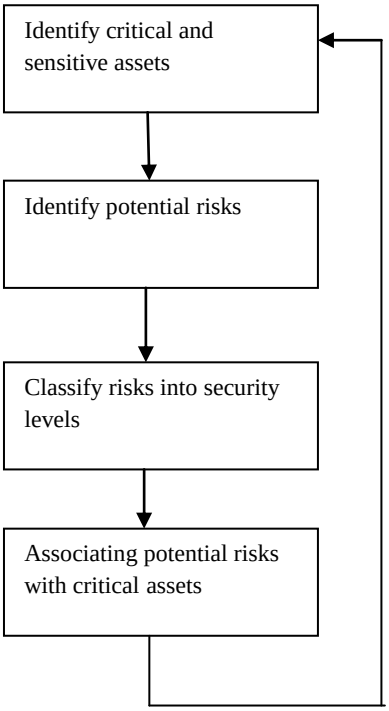

Fig 2: Steps of Risk Assessment

8. CONCLUSION

Cloud computing is becoming more and more popular, for the sake of securing cloud, the vulnerabilities in cloud need to be controlled. In this paper emphasis on primary security concerns and vulnerabilities which are currently faced in the cloud computing and security mechanisms at different levels such as compute, network and application are highlighted. To guard against external threats in cloud regular evaluation should be performed. In spite of a lot of benefits provided by cloud, but to achieve security is quite difficult due to the complexity of cloud. In Future using suitable framework the security issues can be resolved.

9. REFERENCES

[1] Deepak Panth, Dhananjay Mehta, Rituparna Shelgaonkar, "A Survey on Security Mechanisms of Leading Cloud Service Providers", International Journal of Computer Applications, vol. 98-No.1, July 2014.

[2] Rajarshi Roy Chowdhury, "Security in Cloud Computing", International Journal of Computer Applications, vol. 96-No.15, June 2014.

[3] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy, " Cloud Computing: Security Issues and Research Challenges", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol. 1, No. 2, December 2011.

[4] Parminder Singh, Sarpreet Singh, "A New Advance Efficient RBAC to Enhance the Security in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013.

[5] Samy Gerges, Sherif Khattab, Hesham Hassan, Fatma A Omara, "Scalable Multi-Tenant Authorization in Highly-Collaborative Cloud Applications", Vol.2, No.2, April 2013, pp 106~115.

[6] Te-Shun Chou, "Security Threats on Cloud Computing Vulnerabilities", International Journal of Computer Science & Information Technology (IJCSIT) Vol 5, No 3, June 2013.

[7] Rajani Sharma, Rajender Kumar Trivedi, "Literature review: Cloud Computing –Security Issues, Solution and Technologies", International Journal of Engineering Research ISSN:2319-6890)(online),2347-5013(print) Volume No.3, Issue No.4, pp : 221-225 01 April 2014.

[8] Subashini, V. Kavitha "A survey on security issues in service delivery models of cloud computing." Journal of Network and Computer Applications 34(1): 1-11.

[9] Qian, Ling, et al. "Cloud computing: An overview." Cloud Computing. Springer Berlin Heidelberg, 2009. 626-631.

[10] Piplode,k.singh.‖An Overview and Study of Security Issues & Challenges in Cloud Computing ―.Volume 2, Issue 9, September 2012, ISSN: 2277 128X.

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

[12] W. Li and L. Ping, "Trust Model to Enhance Security and Interoperability of Cloud Environment", Cloud Computing, Proceedings on First International Conference, CloudCom 2009, Beijing, China, December 1-4, 2009, Lecture Notes in Computer Science, vol. 5931, (2009), pp. 69-79.

[13] T. Ormandy, "An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments", Whitepaper, (2008).

[14] B.P. Rimal, Choi Eunmi, I. Lumb, "A Taxonomy and Survey of Cloud Computing Systems", Intl. Joint Conference on INC, IMS and IDC, 2009, pp. 44-51, Seoul, Aug, 2009. DOI: 10.1109/NCM.2009.218.

[15] Fernandes, Diogo AB, et al."Security issues in cloud environments: a survey" International Journal of Information Security (2013): 1-58.