CLOUD COMPUTING SECURITY FUNDAMENTALS

Pooja Sharma
Assistant Professor, Ajay Kumar Garg Engineering College, Ghaziabad, UP, India
sharmapooja@akgec.ac.in

***Abstract*— As the cloud gained more thunder, more and more organizations wanted to move toward the river. But an important concern about going to the cloud would be protection. So the information officer of the organization when deciding to move to the cloud may have many questions. Is My Data Safe in the Cloud? Can others access my private data? For example, if a competitor uses the same cloud infrastructure, how secure my data is, how confidential my data is. Also, there are many government regulations and the concept of compliance. So how can I make sure that my infrastructure, my cloud infrastructure complies with government regulations, and what if an attacker downloads my cloud-based operating system? How do I avoid this problem and how do I fix it when such an attack occurs. So these are major security issues that prevent organizations from moving completely into the cloud. So in this article, I will introduce you to the concept of information security. So how cloud security differs from traditional security. What a cloud infrastructure site and how it differs from the old data center. Concerns and threats to cloud infrastructure and security measures to be implemented in the cloud are being discussed.**

***Keywords*— Cloud computing; Security; CIA; Virtual Machine (VM); Cloud Service Provider (CSP); Operating System (OS); IDS**

I. INTRODUCTION

Cloud computing is one of today's most popular technologies as it can reduce computer costs while increasing the flexibility and flexibility of computer systems. Over the past few years, cloud computing has brought new business ideas to one of the most successful segments of the IT industry [1]. It helps the fast-growing IT industry. Various important concerns are raised by IT organizations. One of the biggest concerns is safety. The security problem has been exacerbated under the cloud model as various new computer problems have arisen related to overcrowding, horizontal structures, etc. In this paper, security issues are discussed, providing security threats and security measures / measures.

INFORMATION SECURITY- CIA TRIADS

Confidentiality - Data confidentiality ensures that your data is confidential. Any unauthorized user cannot access your data. Only authorized users can access your data.

Integrity: Integrity ensures that your data stays as it is. So no unauthorized user can change your data. Make sure your data is not medicated with [1].

Availability: Availability ensures that your data and services and applications are always available to authorized users.

CIA triads are therefore an important safety concept. All of our security measures revolve around these three safety measures. Similarly, three A's (AAA) is another popular concept in identifying and controlling authenticity.

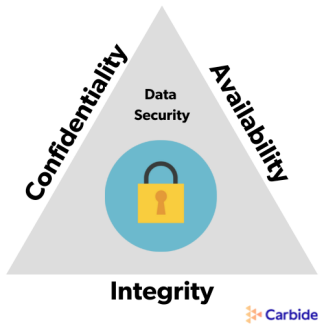

Fig. 1. CIA Triad

Authentication - It is a way of verifying the identity of the user. For example, user says I am user A, How can a person verify that user is user A. So in this case, one of the easiest ways to password. Only passwords will not suffice, further on the paper additional verification methods available are displayed.

Authorization - It is a way of ensuring that only authorized people can gain access to the data. For example, a company's finance department may only have access to financial data. Therefore an HR person trying to access financial data should not be given access if the user does not have access to the data.

As mentioned above, using a password is not enough. Nowadays there is a lot of password fraud software available and maybe some people use simple passwords like their children's names, birthdays, etc., or something like that that is easy to guess. Therefore the password being the only factor in the authenticity is not very secure. To avoid that, we need to add

additional layers of security. So the idea of multi-item verification is that in addition to passwords, you will have multiple security measures. One of the many examples of authenticity is using OTP (One-Password). So there are physical tokens available as well as software tokens available that produce OTP. So when a user tries to verify, the user provides username, password, acquaintance, and personal key. So this has an additional layer of validation. Also, there is the concept of bio-metric validation, in which we have the detection of fingerprints and retinal scanning. [2] Most confidential data therefore use more secure biometric authentication than any other authentication method.

Encryption is often used to protect your data. So it is a process of converting data in a way that can only be used effectively if one has some knowledge. So in the case of symmetric key and asymmetric key or public key cryptography, the user will have a public key and a private key. It is therefore very clear to that user, only if you know what the key is, you can access the data otherwise the encrypted data of another user is unreasonable. So the process of converting encrypted data back to real data is called decryption.

Defence-in-Depth

Deep protection is one way to protect yourself when you have multiple layers of security. So if you only have anti-virus on your desktop, another network attack may not be detected. So you have a lot of layers. Perimeter safety physical protection. Man makes sores to keep their servers in a safe place [2]. An unauthorized user may come in and steal your hard disk, so it is important that you have physical protection first. Usually, you have access cards or other means to ensure that physical security is guaranteed. Network Level Security where there is a firewall and DMZ Compute Security protects against viruses and data loss and blocking products. Storage Security encryption and spatial design. If it is a single layer of security, when the attacker hits your infrastructure, you make sure that in another layer you find this attack and stop this attack. So this will improve the security of the system instead of having a single security system.

Security- Traditional v/s Cloud

The main difference between a standard data center and a modern data center is hosted in the cloud. In a normal data center, all your resources such as server, storage, and everything else may be located in one location or perhaps in multiple locations but are limited to that organization. In the case of a private cloud, it may be limited only to the organization but in the case of a public cloud or a combined cloud, the infrastructure is shared by multiple organizations and used by many users and may be very large, widely distributed. [3]. One server may be in Asia and the other server may be in the US. One can easily use it without knowing where your server is and where your data is [3]. You have mobile applications that try to reach the cloud, so it is much more complex than a normal data center and you need deeper security measures to make sure your cloud infrastructure is secure.

Cloud Deployment Model

Public Cloud: Suppose there is a business P and a business Q and a user may belong to one of the organizations. The public cloud is hosted by CSP (Cloud Service Provider). Your service provider is responsible for maintaining your server, storage space, network, and all other resources and making sure that on request, resources are available to you. But the user does not need to know what is in the end. Also, it is assigned to different organizations, different users. The user therefore does not know who is sharing his or her data.

Private Cloud: In the case of private clouds, limited to an organization. It may be locally (in business) or hosted by a cloud service provider but all infrastructure is restricted to one business. Many different businesses use the same infrastructure.
Hybrid Cloud: Hybrid Cloud is an example of a company where the most important data for deploying its private cloud, in its business cloud where it ensures that my most important private data is not in the cloud but other less important data goes to the public cloud. It is therefore a combination of a private and public cloud which is a mixed cloud [4].

Cloud Security Concerns

So with the introduction of multiple users and multiple enterprises and heterogeneous hardware infrastructure, new security concerns arise.

Fig. 2. Cloud Security Concerns

A. Multi-tenancy

It is a concept where multiple virtual machines are available with a single infrastructure, a single server, or a single server host. Each virtual machine is available seamlessly on the same server. So in the case of a public cloud, for example, My Company may use one machine, while another competing company may use another virtual machine hosted on a server. So this is how most hiring poses a security threat, where the same infrastructure can be shared with different organizations and your virtual machines can be deployed on a single server. Thus in CSP it also presents new challenges [5]. Each com-

pany has its own security policies, so when most organizations have different types of security policies, how does the cloud provider ensure that each company's security policy is fulfilled or implemented in the same way because the underlying infrastructure is the same.

B. Velocity of attack

In public cloud there may be thousands of servers running in the same location or everywhere. So all the infrastructure available to users, which is why the attack face grows with the introduction of the cloud. In the case of a single business with a single data center within its base, its set of servers only manages itself. cloud infrastructure is big so the attack face is big, which is why attack speed is high. This potential loss is also very high because if one VM is attacked, all the infrastructure may be attacked. So in that case, trying to contain an attack somewhere also becomes very difficult. To meet this challenge, CSPs need to have more robust security measures in place compared to the old data center.

C. Information assurance and Data Ownership

How do you ensure that the privacy of your data is maintained because CSP does not have access to your data and another company may be using the same infrastructure? How do you make sure your competitor is not stealing your data? [4] A major security concern is the CIA (Confidentiality, Integrity, and Access). In the cloud environment, your data is hosted by CSP. So CSP has access to data, but the owner is not CSP. The organization is the owner. How to ensure that your data is accessible only to an authorized user and ensure that confidentiality is maintained. Therefore data should also be protected from unauthorized use by encryption. So this becomes one of the biggest concerns in the cloud space.

D. Data Privacy

How does one ensure that the confidentiality of the data is guaranteed in a cloud environment?

Opportunities for unauthorized disclosure of confidential cloud client data. Private data may include:

- Identity of the client
- Client details requested by the client
- Client related data

  CSP needs to ensure that its client's confidential data is protected from unauthorized disclosure.
- Both the collection and distribution of personal data requires protection
- CSP requires the use of data privacy methods, which comply with regional legal rules.

III. CLOUD SECURITY THREATS

A. VM Theft

Visual Theft is a risk that allows the attacker to copy or move the VM illegally. VM Theft is the result of inadequate control over VM files allowing unauthorized copies or distribution of tasks. Copying and distribution restrictions are essential to prevent VM theft.

- These criminals tackle the VM on a virtual machine.
- VM with copy and transmission limit cannot work on hypervisor installed on any other server.
- These limits apply a combination of visual management.
- Limit the use of such restrictions on sensitive / sensitive VMs only.

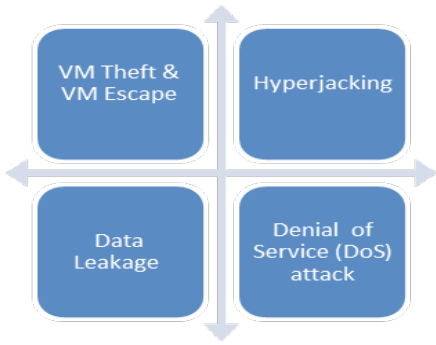

Fig. 3. Cloud Security Threats

B. Hyperjacking

Allows the attacker to install a malicious hypervisor or Virtual Machine Monitor (VMM) that can control sub-server resources. Attacker can use unauthorized applications on the visitor OS to detect that. Attacker can control the interaction between VMs and the sub-server [5]. Normal safety measures do not apply to attacks of hyper jacking. The measure against hyper jacking includes:

- Hardware-assisted introduction of hypervisor
- Scanning the hardware level to check the integrity of the hypervisor and detect the presence of a malicious hypervisor.

C. *Data Leakage*

Confidential data stored in a third party cloud is at risk of unauthorized access or deception.

- Attacks on service provider control systems (eg password lists) can put all client data at risk.
- Cloud users should check data protection measures from end to end with all the appropriate components for any data access level.

Side Channel Attack (SCA) can be used for data leaks in the cloud

- The SCA removes information by monitoring indirect activities for example warehouse data.
- Cross-VM SCA cloud reveals cloud information to another malicious client that uses its VMs on the same server.
- Protection against cross VM SCA requires placing only those clients who do not have conflicts with each other on the same server..

D. Denial of Service (DoS) Attack

It is an attempt to prevent legitimate users from accessing a service or service [6]. DoS attacks may affect software applications and network components. DoS attacks involve

- Disable resources, for example, network bandwidth or CPU Cycle
- Weaknesses in communication protocols, for example resetting TCP times, to corrupt domain name servers.
- Vicious client VM may be used to launch DoS attacks against a hypervisor or other VMs using the same hypervisor.
- As a precautionary measure, the use of VM resources should be limited.

A. Cloud Security mechanisms

Compute a Network Level Security

In the physical environment, computer, network, and storage are all virtual. So at that level, how does one ensure that safety is maintained. Protecting the computer system includes

- Protecting the Virtual Server
- Hypervisor protection
- VM protection (VM isolation and VM durability)
- Guest OS Hardening level (Guest OS Hardening)
- Application level security (Application strength)

Each VM should be protected because if one VM is in danger, it can serve as an attack on all VMs.

Virtual Server Security: Identify virtual server application details including

- Whether the server will be used for a specific program or common purpose
- Network services are provided on the server
- Users and / or groups of users can use the server and their right of access

Determining security measures:

- Determining methods of verification and accreditation
- Disables unused hardware such as NICs, USB ports, or Drive.

Hypervisor Security: Hypervisor attacks affect all VMs running on them. We can say that, and it is one point of failure. Hypervisor Safety Measures are

- Install hypervisor updates
- Strengthen VMs to prevent attacks
- Protection of the hypervisor management system
- Important because an unsafe management system can put existing VMs at risk of attack and allow the creation of new malicious attacks.
- Configure solid firewall security between management system and networks
- Provide direct access only to administrators on administrative servers
- Disable access to admin console to prevent unauthorized access.

VM Security: Isolation and Hardening: VM detachment helps prevent the compromised visitor OS and operating system from affecting other VMs. VM hardening is the process of changing the default configuration to achieve greater security. VM Hardening considerations exist

- Use a VM template to provide new VMs
- Limit the VM resources I can use to prevent DoS attacks
- Disable unused functions and devices on VM
- Use the text service to verify
- Perform a risk scan and check the visitor's OS infiltration.

Guest OS and Application Security: The OS strengthening method includes deleting unused files and using latex leaflets [6]. Using the solid checklist found in a particular Oss. Install guest OS in TCB mode if VM is to be used for critical applications. Requires support from a hypervisor in preparing (trusted) components of the TCB virtual hardware. The action to strengthen the app includes not allowing the compromised app from

- Introducing any reliable (usable) file.
- Creating or editing usable files
- Configuring visitor OS sensitive areas, for example, MS Windows registration

Sandboxing is another important measure of guest OS and app security.

Security at Network Level - Virtual Firewall: Securing VM-to-VM traffic running on a server is difficult in the VDC environment.

- Visible changes may not be visible to management (network and systems)
- Traffic may not leave the server, so it cannot be detected and captured

Visible firewall is a security service that works on a hypervisor.

Security at the network level: A virtual or realistic network or small network that limits the exposure of nodes to an internal network from external networks. Add a layer of protection against external attacks.

- Attacker can only access DMZ, than any other part of the network
- For practical purposes, services provided to users of an external network can be installed on DMZ.

Virtual DMZ DMZ based on a virtual reality environment using virtual network components.

B. Security Data at Rest

Restored data stored on server or in any repository. If the data is not encrypted or raw data is stored in your actual store. Once the attacker has access to your data, it becomes easier for the attacker to use that data [7]. So if you secretly record your rested data, even if the attacker receives your data, it is encrypted, so it does not help the attacker. It is therefore very important to protect your data while resting on encryption.
Rest data refers to data that can be transmitted over a network. Data encryption at recess is performed by

- Provide confidentiality and integrity services
- Reduce CSP Legal Debts due to unauthorized disclosure of data to its cloud.

Full disk encryption is a way to encrypt data when resting on disk.

Security at Network Level: Protects data on the plane. The data will rest as files stored on the server. But there will be data transfer over the network i.e. the transfer where your files are hosted locally and your client is trying to access the file. Even at network level, data can be stolen and compromised, so one needs to have network level security to ensure that the data on the aircraft is also secure. Flight data encryption provides privacy and integrity and is an important step in counter-smelling attacks.

TABLE I. SECURITY AT NETWORK LEVEL

Encryption Method	**Description/ Example**
Application Level	It is used at the application level where the data is generated
Network Level	Used at network level; for example, IPSec encryption IP packets

Data Shredding: This is how data is erased from the desktop permanently and ensures there is no residual data left. Residual data can be used by the attacker, so it should be avoided. The data has been deleted by a client cloud or process, but leaving traces in the system, can be a source of attack.

- Tracking deleted VMs can provide important information to the attacker
- Slightly recoverable “deleted data” may expose client information

Websites permanently delete all traces of deleted data. It is an important part of data security in cloud infrastructure. Tracking deleted data includes

- VM logs or application usage
- Logs for old files, folders, and other resources
- Data connection logs.

Intervention Detection: It is the process of detecting events and / or businesses that could jeopardize system security..

TABLE II. TYPES OF INTRUSION DETECTION

Types of Intrusion Detection System (IDS)	**Description**
Server-based IDS	• Analyzes activity logs, including system calls, application logs, etc. • Better View of the monitored system but high vulnerability for an attack on IDS itself
Network-based IDS	• Analyzes network traffic and communicating nodes • Poorer view of the system and low vulnerability for an attack on IDS itself
Integrated IDS	• Combination of server and network-based approaches

C. Identity Access and Management in Cloud

One-time password

- Every new access request requires a new password
- Rate against password reduction
- Integrated ownership management is provided as a service in the cloud
- Allows organizations to authenticate their cloud service users using a selected ID provider
- User identity in different organizations can be managed together to enable cloud interaction in the cloud
- OpenID
- It is an open standard for distribution authorization and access control
- Can be used while allowing users to access multiple services using the same digital ID

D. Risk Analysis and Compliance

Risk means the result of uncertainty in business objectives. Risk management is the integrated function of directing and controlling the organization and recognizing the potential of the business while managing adverse events [7]. Risk assessment is intended to identify potential risks while operating in a cloud environment. It should be done before moving to the clouds. It should be used to determine the actual width of cloud reception.

TABLE II. TYPES OF COMPLIANCE

Types of Compliance	Description
Internal policy compliance	• Controls the IT operating environment within the organization • It needs to maintain the same compliance even when operating in the clouds
External regulatory compliance	• Includes legal and industry rules • Regulates the environment for IT operations related to data flow outside the organization • It may vary based on the type of information, business, etc.

Compliance means an act of compliance and demonstrate compliance with external laws and regulations as well as business policies and procedures. Cloud hosting and business operations require compliance with compliance policies. Types of compliance are given above TABLE II.

V. CONCLUSION AND FUTURE SCOPE

As companies look to the cloud, one of the main reasons why companies look to the cloud is lower operating costs. So using your apps in the cloud is more expensive than using them in the old data center where you have to buy your hardware and software. But there is the possibility of an additional risk of migration to the clouds. So the main goal of cloud computing is to reduce operating costs and increase revenue and reduce risk. So is cloud security. The cloud security measures and cloud security measures adopted by the company therefore ensure that the risk of cloud transfer is reduced. The company can use cloud computing to reduce its operating costs and increase revenue. This is the ultimate goal of cloud computing.

ACKNOWLEDGMENT

I would like to thank everyone who found great interest and gave me their helpful discussion during the start of this study. Their valuable comments and insightful suggestions have led to improvements in a number of aspects of this manuscript.

REFERENCES

[1] BEHL A. BEHL K. " An analysis of cloud computing security issues" center of Excellence, Cisco Syst. , Information and Communication Technologies (WICT), 2012 world congress on Oct 30, 2012, pp. 109-114.

[2] Sabahi, F. Fac. of Comput. Eng., Azad Univ., Shahrekord, Iran, " Cloud Computing Security Threats and Responses" Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on 27 May 2011, pp. 245-249.

[3] https://www.sans.org/course/cloud-security-fundamentals

[4] International Organization for Standardization (ISO), "ISO/IEC 27000 - Information technology - Security techniques - Information security management systems - Overview and vocabulary," ISO/IEC 27001:2005(E), 2009, <http://webstore.iec.ch/preview/info-isoiec27000%7Bed1.0%7Den.pdf>, Accessed in July 2010.

[5] Cloud Security Alliance Group, "CSA-GRC Stack," <www.cloudsecurityalliance.org/grcstack.html>, Accessed Dec'10

[6] M. Almorsy, J. Grundy, I. Mueller, "An analysis of the cloud computing security problem," In the proc. of the 2010 Asia Pacific Cloud Workshop, Colocated with APSEC2010, Australia, 2010.

[7] R. La'Quata Sumter, "Cloud Computing: Security Risk Classification", ACMSE 2010, Oxford, USA

ABOUT THE AUTHOR

Pooja Sharma received the B.Tech degree in Computer Science and Engineering and M.Tech degree in Computer Science and Engineering from AKTU university. She is currently an Assistant Professor at the Department of Computer Science and Engineering in Ajay Kumar Garg Engineering College, Ghaziabad.

Her research interest includes Cloud Computing Security, Internet of Things, Cyber Security and Steganograpy and Cryptography Techniques. She has published various papers in Cloud Computing, Steganography fields as well. Her current research span include Four level Cloud Computing Security model.