IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

REVIEW OF CLOUD COMPUTING DATA SECURITY AND THREATS

Harish C. Sharma, Pradeep Semwal
SGRR University
Dehradun, India

ABSTRACT - Cloud Computing is performing computing using the internet facility. Computing is performed as on demand of the user. The Cloud Computing data security is a very hot topic. As now more and more user are using cloud services and data storage. The data stored in the cloud is vulnerable to security and threats. There are many such situation under which the data is vulnerable to security. The paper reviews different security threats and vulnerabilities and their possible solution for a better cloud computing usage of resources.

Keywords: *Cloud Computing, Data Security, Threats,, Cloud Vulnerabilities.*

I. INTRODUCTION

Cloud Computing [1] provides pool of resources to its end-user that can be reallocated to different purposes within short time frames. Cloud computing power is delivery of computing services and resources such as hardware or software from computing power to computing infrastructure, applications etc. to end users as and when it is needed. The cloud computing combines the set of hardware, software, storage, networks services and interfaces that combine to deliver aspect of computing as a service.

There are different reasons for using cloud computing.

- No hardware, software is required.
- Operating System software
- Dynamic allocation
- Movement of programs
- Scalability
- Pay as you go
- No commitments
- Massive, Web-scale abstracted infrastructure.

Cloud Computing is a term that describes the means of delivering any and all information technology, it uses requirement based hardware as its base. The hardware can be replaced at any time without affecting the cloud. It uses an item or commodity – based software container system. For example, a service should be able to be moved from one cloud provider to any other cloud provider with no effect on service. Cloud Computing requires virtualization, abstraction layer for hardware and software. The some services provided by the Cloud Computing are:[6][7][8]

- Software-as-a-service (SaaS)
- Platform-as-a-Service (PaaS)
- Infrastructure-as-a-Service (IaaS)

Cloud Computing is based on the four different models these are public, private, community and hybrid.

Cloud Deployment Model

Cloud service can be assigned in different ways depending on the organizational structure and need of use. Cloud Computing have mainly four deployment models Private cloud, Public cloud, Community cloud and Hybrid cloud.

Private Cloud.

The cloud infrastructure is provisioned for exclusive use by the single organization comprising multiple consumers. It may be owned, managed and operated by the organization, a third party, or some combination of them. It may exists on or off premises. [11].

Example of Private Clouds

- Eucalyptus
- Amazon VPC (Virtual Private Cloud)
- Microsoft ECI
- VMware Cloud Infrastructure Suite.

Community Cloud.

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have common or shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may or may not be owned, managed, and operated by one or more of the organizations or institutions in the community, a third party, or some combination of them, and it may exist on or off premises [11].

Example of Community Clouds

- Google Apps for Government
- Microsoft Government Community Cloud

Public Cloud.

The infrastructure is provisioned for open use by the general public. It may be owned, managed and operated by business academic or government organizations. A public cloud is a model which allows users' access to the cloud via interfaces using mainstream web browsers. It's typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization. This helps cloud clients to better match their IT expenditure at an operational level by decreasing its capital expenditure on IT infrastructure. [11].

Example of Public Cloud

- Microsoft Windows Azure,
- IBM smart cloud, Amazon EC2 etc.

Hybrid Cloud.

The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology, that enables data and application portability (e.g., cloud bursting for load-balancing between clouds)

Example of Hybrid Cloud

- Windows Azure (capable of Hybrid Cloud)
- VMware Cloud (Hybrid Cloud Services)

II. DATA SECURITY

Data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle. It's a concept that encompasses every aspect of information security from the physical security of hardware and storage devices to administrative and access controls, as well as the logical security of software applications. It also includes organizational policies, rules and procedures.

Data security is about keeping your data safe from accidental or malicious damage. Security has different dimensions. The physical security refers to storing data in devices or computer systems which are kept in safe place such as the rooms having some physical lock to protect the data. The other type security is the password.[2][3]

Password

Password security which means protecting your data with some password key. A good practice is to make password strong using alphanumeric and special characters.

Encryption

Encryption is a technique to secure the data with the help of some encryption methods Encryption maintains the security of data and documentation through an algorithm to transforming information into something unreadable requiring a "key" to decrypt and return to comprehension. Some of the encryption algorithms are as follows:

- Data Encryption Standard (DES)
- 3 Data Encryption Standard (3DES)
- Rivest–Shamir–Adleman (RSA)
- Advance Encryption Standard (AES)
- Message Digest (MD5)
- Hash Based Message Authentication Code (HMAC)

Access management and controls

The principle of "least-privilege access" should be followed throughout your whole or entire IT environment. This means granting database, network, and administrative account access to as few people as possible, and only those who absolutely need it to get their jobs done.

III. DATA SECURITY AND THE CLOUD

Data Security in the cloud based infrastructure is different from the tradition data security. Depending on the cloud service model one uses. The field covers all processes and mechanism which digital equipment, information and services are protected from unintended or unauthorized access. The Cloud monitoring tools can sit between a cloud provider's database-as-a-service (DBaaS) solution and monitor data in transit or redirect traffic to your existing security platform. This allows for policies to be applied uniformly no matter where the data resides.

Table 1: Security Threats [10]

S.No.	Threat	Description	Layer
1	Account or service hijacking	Account theft performed by different ways social engineering weak credentials.	SPI
2.	Data Leakage	When data goes in wrong hands	SPI
3.	Denial of Service	It is possible that malicious user take all resources	SPI
4.	Customer data manipulation	Data manipulated through SQL injection etc.	S
5.	VM escape	Designed to exploit hypervisor	I
6.	Malicious VM Creation	Attacker create VM with malicious code	I

Data Breaches

A data breach is related or associated with the release of protected or confidential information to unauthorized or other group of information. Being the human, programmer and other developer make mistake, most of which are unintentional and non malicious. Many such error cause program malfunction but do not lead to more serious vulnerabilities. However, a few classes of error plagued programmer and security professional for decades. The vast amount of data hosted by cloud service provider (CSP) makes them susceptible to the risk of data breaches. While cloud providers take responsibility for their services, the customers or businesses are also responsible for protecting their own data.

Multifactor authentication and encryption are two of the security measures that ensure protection against data breaches.[4][5]

Inadequate Identity and Access Management

Attacks and security breaches can also result from non-usage of multifactor authentication, lack of ongoing automated rotation of cryptographic keys and certificates, as well as weak password usage.

- Centralized management creates a single centralized target.
- Improper management of network/application
- Insufficient process automation
- Failing to plan for scalability.

The authentication system should support the enforcement of policies for strong password usage and organization-defined rotation period, in case of legacy systems that involve the usage of passwords alone.

Insecure APIs

The Application Programming Interfaces (APIs) in the cloud computing is responsible for the provisioning, management and monitoring of cloud services, their security is of prime importance. In The interfaces must be designed to prevent any malicious efforts pertaining to authentication, access control, encryption and activity monitoring.

API attack pattern

- Denial of Service
- Access Violation
- Abuse of functionality

System Vulnerabilities

Attackers can infiltrate and take control of the systems in addition to disrupting the service operations, utilizing the system vulnerabilities or exploitable bugs.

To reduce the security gaps and mitigate the damage caused by system vulnerabilities, installation of security patches or upgrades, regular vulnerability scanning and following up on reported system threats are mandatory.

Following are the example of cloud vulnerabilities.

- Misconfigured Cloud Storage
- Insecure API
- Loss or Theft of Intellectual Property
- Compliance Violation and Regulatory Actions
- Loss of Control over End –User Actions
- Poor Access Management
- Contractual Breaches with Customers or Business Partners

Account or Service Hijacking

Cloud account hijacking is a process in which an individual or organization's cloud account is stolen or hijacked by an attacker. Account hijacking is a common identity theft scheme. Service hijacking includes attack methods such as phishing, fraud and exploitation and tempering of data. software vulnerabilities that enable attackers to misuse the account access, steal data, impact cloud services and systems, and damage the overall reputation.

Wherever possible, organizations should avoids the sharing of account credentials among users and apply strong two-factor authentication techniques.

Malicious Insider Threats

The threat caused by insiders or a person who is a insider with malicious intent, who might be system administrators having access to critical systems and sensitive information, can have a tremendous impact on a company's security.

There are many reasons an insider can be or become malicious including revenge, coercion, ideology, financial gain etc. Malicious insider can be employee, former employee or Business associates etc.

To control this, the CSP needs to ensure effective policies, segregation of duties and proper logging, auditing and monitoring of administrators' activities. Following are some points prevent malicious insider threat. [11][12]

- Require strong password
- Access control
- Auditing and Logging
- Deactivate Access
- Improve staff education

Advanced Persistent Threats (APTs)

An Advanced persistent threat is an attack in which an unauthorized user gains access to system or network and remains there for some time. Advanced Persistent Threats (APTs) steal data, information and Intellectual Property (IP) by infiltrating the IT systems of target companies. The common points of entry or cause for APTs are spear-

phishing, direct hacking systems and use of unsecured or third-party networks.

Though APTs are difficult to detect and eliminate, they can be restricted with proactive security measures.

Malware Injection

Cloud malware or malware in the cloud refers to the cyber-attack on cloud computing based system with a malicious code and service. Malware injection attacks are becoming a major security concern in cloud computing. These are malicious scripts or code that enable attackers to eavesdrop, steal data and compromise the integrity of sensitive information.

Types of malware attacks are:

- DDoS Attack
- Hypercall Attack
- Hypervisor DoS
- Hyperjacking
- Exploiting Live Migration

Data Loss

Data loss occur when valuable or sensitive information on a computer is compromised due to theft, human error, viruses or by a third party person etc. Data loss can also occur because of multiple reasons such as a catastrophe like fire or earthquake, or even accidental deletion by the CSP. To avert this, both the providers and the users need to ensure proper data backup measures and follow the best practices pertaining to disaster recovery and business continuity.

Data loss can be caused by external factors, such as power outage, theft, or a broad-based phishing attack.

Insufficient Due Diligence

Insufficient due diligence or lack of due diligence or the lack of knowledge in security is an existing problem. Organizations need to perform the necessary due diligence and develop a proper roadmap before adopting cloud technologies and selecting the cloud providers, failing which they might be exposed to several security risks.

Poor IP Protection

Safeguarding Intellectual Property (IP) demands the highest encryption and security protocols. When IP is created in the cloud environment, it becomes imperative & crucial to understand the laws of the land where IP sits. In cases of creation of IP, the terms of the contract should be clear on the ownership of IP. Go with a service provider that would ensure compliance with global regulations and would keep abreast with the evolving laws and policies. In addition to identification and classification of IP for determining potential security risks, vulnerability assessment and appropriate encryption must be carried out.

Abuse of Cloud Services

The criminals may use cloud computing to target their victims and use cloud service against them. The DDoS attacks, phishing attempts, email spam, digital currency "mining" are just example of misuse of cloud resources. Malicious attacks can also result from issues such as unsecured cloud service deployments, fraudulent account sign-ups and free cloud service trials. Large-scale automated click fraud, hosting of malicious or pirated content, launching distributed DoS attacks, email spam, and phishing campaigns are some of the examples of cloud-based resource misuse.

DoS Attacks

In cloud computing, a DoS attack can described as an attack designed to prevent some cloud computing service or resource from providing its normal services for a period of time. Denial-of-Service (DoS) attacks cause the consumption of disproportionately large amounts of system resources including memory, disk space, network bandwidth and processor power by the targeted cloud services, thereby preventing the users from accessing their data and applications.[9][10]

Generally, DoS attack comes in following categories:

- Bandwidth attack
- Connectivity attack
- Resource exhaustion
- Limitation exploitation
- Process disruption
- Data Corruption
- Physical Disruption

The Severity of DoS attack depends on the following issues:[10]

- Type of attack
- Type of protocol or event misused in the attack.
- Number of compromised attacking hosts.
- The amount of resources at victim's site.
- Topology and defense mechanism at victim site.
- Type of Cloud.

Vulnerabilities Caused by Shared Technology

The Cloud Computing runs software, software has vulnerabilities and adversaries try to exploit those vulnerabilities. Cloud Service Provider (CSPs) deliver scalable services by sharing infrastructure, applications and platforms without substantial alterations to the off-the-shelf hardware and software.

If the underlying components such as CPU caches and GPUs do not offer strong isolation properties for a multitenant architecture (IaaS), multi-customer applications (SaaS) or redeployable platforms (PaaS), it could lead to shared technology vulnerabilities.

Communication with CSPs

Cloud Computing for CSPs and other enterprises can be modeled around three common pillars, Software as a Service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS). Customers need to define the exact security requirements in the Service Level Agreements (SLAs) with CSPs. They can use the Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (CSA STAR) as a reference for understanding the security controls offered by CSPs. [11]

CSPs also need to provide details on how they protect multi-tenant boundaries and ensure PCI and Federal Information Security Management Act (FISMA) compliance.

IV SECURITY SOLUTION FOR CLOUD

Many organizations operate in multi-cloud environments, where they use IaaS, PaaS and SaaS from different vendors. Regardless of which cloud service model you are using, we encourage you to take a look at the following best practices oriented at increasing the security of your cloud infrastructure.

Implement stringent role-based access controls

Ensure that both users and developers are allowed to do only what's included in their job description and nothing more.

Manage inactive accounts

Always de provision inactive accounts and those belonging to former employees before hackers become interested in them. With services such as LinkedIn, it's easy to find out who has recently left your company. Remember to lock root account credentials as well to block unauthorized access to admin accounts.

How to Prevent Misconfigured Cloud Storage

To secure the misconfigured data, it is required to re verify cloud security configurations by setting up a dedicated cloud server. It can be safely stored by keeping data in storage without second thoughts regarding its safety.

Using specialized tools and cloud solutions, finding the security configurations. It can analyze the state of security configurations in an interval of time and identify the possible issues before anything happens.

How to Prevent Loss of Online Visibility

To secure the cloud data from the loss of online visibility, frequent backups are one of the most effective ways. Make a schedule for each backups and clear delineation of necessary data for backup, and unrequired data can be deleted. Using data loss prevention (DLP) software helps to detect and secure unauthorized access and backups.

Also, institution or companies encrypt their data and geo-diversify their backups to prevent essential data from loss or theft. Offline data backup creates problems with ransomware.

How to Prevent DoS Attack

To avoid DoS attacks, businesses use Intrusion Detection Systems. This system helps to identify peculiar traffic and provide an early warning as per the credentials and behavioral factors. It is also known as a cloud security break-in alarm.

Using firewall type traffic verification and inspection to check the source of incoming traffic or detect good or bad traffic. So that it can help to sort the data packets or traffic and delete the bad data packets or traffic. Also, blocking the Internet Protocol (IP) addresses that can cause an attack to the network helps to avoid a DoS attack.

How to Prevent Data Loss

To secure our data in the cloud from being lost, it is required to have frequent data backups. Using data loss protection software to automate the process of data recovery. Schedule the operation to clear unrequired data and take the timely backup of required data. Let's look at different ways how we can prevent data loss:

- Data Backup
- Protect Data from Power Surges
- Firewall and Antivirus
- Develop a Disaster Recovery Plan
- Work With IT Security Experts

VI. CONCLUSION

The cloud computing has great importance in the current decade. As the Cloud Computing offers different services such as IaaS, PaaS, and SaaS. The cloud virtualization allows sharing of resources and it represent the logical view of data representation. The Data Security in the cloud computing is a challenging task. Different security vulnerabilities and threats are discussed in the paper. The some of the basic security checks are authentication, access control, encryption etc. are been discussed. Some security issues related with cloud services are also been discussed. At the end few solutions techniques how to prevent such vulnerabilities and threats are suggested.

VI REFERENCES

[1] Peter Mell and Timothy Grance (September 2011). The NIST Definition of Cloud Computing (Technical report). National Institute of Standards and Technology: U.S. Department of Commerce. doi:10.6028/NIST.SP.800-145. Special publication 800-145.

[2] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing"[online] https://cloudsecurityalliance.org/csaguide.pdf (Accessed 26 December2013)

[3] D.Feng, et al. "Study on cloud computing security." *Journal of Software* 22.1 (2011): pp.71-83.

[4] Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., et al. (2014). Security and privacy for storage and computation in cloud computing. *Information Sciences*, *258*(0), 371-386.

[5] Boutaba, R., Zhang, Q., & Zhani, M. F. (n.d.). Virtual Machine Migration in Cloud Computing Environments. In Communication Infrastructures for Cloud Computing (pp. 383–408). IGI Global. https://doi.org/10.4018/978-1-4666-4522-6.ch017

[6] Harish C. Sharma, P. Semwal, "A Review of Load Balancing Algorithms in Cloud Computing", International Journal of Creative Research Thoughts, Vol. 9, Issue 3, pp. 2786-2791, Issn: 2320:2882

[7] Harish C. Sharma, M Bisht, "Best fit resource allocation in cloud computing", International Journal of Computer Science & Engineering, Vol. 7, Issue 3, Issn: 2347:2693, pp. 928-932

[8] V. Sharma, Harish C. Sharma, "A Review of cloud computing scheduling algorithms", International Journal of Innovative Science & Research Technology, Vol 6, Issue 12, Issn : 2456:2165, pp. 565-570

[9] M. Masdari, M Jalali, " A Survey and taxonomy of DoS attacks in cloud computing", Security Comm. Network 2016, 9: 3724-3751, doi: 10. 1002/sec.1539

[10] Hashizume, K., Rosado, D.G., Fernández-Medina, E. *et al.* An analysis of security issues for cloud computing. *J Internet Serv Appl* **4,** 5 (2013). https://doi.org/10.1186/1869-0238-4-5

[11] Hiral B. Patel, N.Kansara, "Cloud Computing Deployment Models: A Comparative Study", IJIRCST, Vol. 9, Issue 2, pp.45-50

[12] M. Farsi, M. Ali et at "Cloud computing and data security threats taxonomy: A review", Journal of Intelligent & Fuzzy Systems xx (20xx) x–xx DOI:10.3233/JIFS-179539