# UNIT - V

# 5 Security in Cloud Computing

## Syllabus

***Risks in Cloud Computing :*** *Risk Management, Enterprise-Wide Risk Management, Types of Risks in Cloud Computing.* ***Data Security in Cloud :*** *Security Issues, Challenges, advantages, Disadvantages, Cloud Digital persona and Data security, Content Level Security.*
***Cloud Security Services :*** *Confidentiality, Integrity and Availability, Security Authorization Challenges in the Cloud, Secure Cloud Software Requirements, Secure Cloud Software Testing.*

## Contents

## 5.1 Risks in Cloud Computing

- Cloud security is the protection of data stored online via cloud computing platforms from theft, leakage, and deletion. Methods of providing cloud security include firewalls, penetration testing, tokenization, Virtual Private Networks (VPN), and avoiding public internet connections.
- Cloud security refers to an array of policies, technological procedures, services, and solutions designed to support safe functionality when building, deploying, and managing cloud-based applications and associated data.
- Cloud security is designed to protect the following, regardless of your responsibilities :
  a) **Physical networks -** Routers, electrical power, cabling, climate controls, etc.
  b) **Data storage -** Hard drives, etc.
  c) **Data servers -** Core network computing hardware and software
  d) **Computer virtualization frameworks -** Virtual machine software, host machines, and guest machines
  e) **Operating Systems (OS) -** Software that houses
  f) **Middleware -** Application Programming Interface (API) management,
  g) **Runtime environments -** Execution and upkeep of a running program
  h) **Data -** All the information stored, modified, and accessed
  i) **Applications -** Traditional software services (email, tax software, productivity suites, etc.)
  j) **End-user hardware -** Computers, mobile devices, Internet of Things (IoT) devices, etc.
- Cloud computing security addresses both physical and logical security issues across all the different service models of software, platform and infrastructure. It also addresses how these services are delivered in the Public, Private, Hybrid and Community delivery models.

### 5.1.1 Risk Management

- Risk management is the process that allows business managers to balance operational and economic costs of protective measures and achieve gains in mission capability by protecting business processes that support the business objectives or mission of the enterprise.
- Risk management is the total process used to identify, control and minimize the impact of uncertain events. The objective of the risk management program is to

reduce the risk of performing some activity or function to an acceptable level and obtain senior management approval.

- Threat is a potential cause of an incident that may result in harm to a system or organization.
- Vulnerability is a weakness of an asset (resource) or a group of assets that can be exploited by one or more threats.
- Risk is potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability.
- Risk control is an important part of risk management. It involves determining what to do with uncontrolled risks.
- Some questions to ask when selecting a risk control strategy are, "What is an acceptable level of risk ?" and "What should I do about the risks ?"
- Risk control is often achieved by applying safeguards. Safeguard is anything that removes a vulnerability or protects against one or more specific threats.
- Security risk analysis, otherwise known as risk assessment, is fundamental to the security of any organization. It is essential in ensuring that controls and expenditure are fully commensurate with the risks to which the organization is exposed.
- However, many conventional methods for performing security risk analysis are becoming more and more untenable in terms of usability, flexibility and critically... in terms of what they produce for the user.
- Security in any system should be commensurate with its risks. However, the process to determine which security controls are appropriate and cost effective, is quite often a complex and sometimes a subjective matter. One of the prime functions of security risk analysis is to put this process onto a more objective basis.
- There are a number of distinct approaches to risk analysis. However, these essentially break down into two types : Quantitative and qualitative.

## 5.2 Enterprise-wide Risk Management

- Enterprise Risk Management (ERM) is the overall management of risk for an organization. As with governance, the contract defines the roles and responsibilities for risk management between a cloud provider and a cloud customer. And, as with governance, you can never outsource your overall responsibility and accountability for risk management to an external provider.
- Risk management in cloud is based on the shared responsibilities model.

- Risk management process is as follows :
  1. Define objective
  2. Identify risk
  3. Evaluate risk
  4. Options and assortment of risk
  5. Decision about implementation
  6. Evolution and review
- Fig. 5.2.1 shows six step risk administration process.

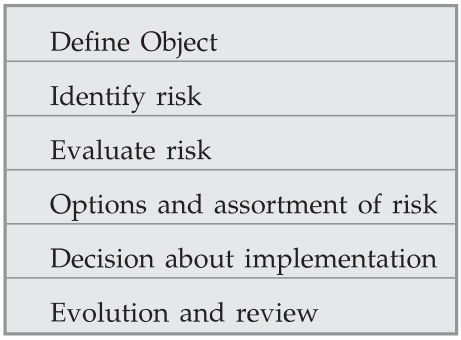


**Fig. 5.2.1 Six step risk administration process**

| Parameters | Remarks |
|---|---|
| Define object | • Administration program |
| Identify risk | • Checklist, flowchart |
| | • Inspections |
| | • Internal records |
| Evaluate risk | • Significant or insignificant risk |
| Options and assortment of risk | • How to deal with risk |
| Decision about implementation | • Methods |
| | • Risks remedy |
| Evolution and review | • Risk administration |

## 5.3 Types of Risks in Cloud Computing

- Risks in cloud computing is divided into internal and external.
- Loss of data : Data stored on cloud servers can be lost through a natural disaster, malicious attacks, or a data wipe by the service provider.

- Increased customer agitation : A growing number of cloud service critics are keen to see which service providers have weak security protocols and encourage customers to avoid them.
- Attacks to deny service to legitimate users.
- Shared vulnerabilities : Cloud security is the responsibility of all concerned parties in a business agreement.
- Contract breaches with clients and/or business partners : Contracts restrict how business partners or clients use data and also who has the authorization to access it.
- Malware attacks : Cloud services can be a vector for data exfiltration.
- Compliance violations : Organizations can quickly go into a state of non-compliance, which puts them in the risk of serious repercussions
- top threats identified by Cloud Security Alliance (CSA) of cloud computing are as follows :
  1. Insecure Interfaces and APIs : Cloud Computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration and monitoring are all performed using these interfaces.
- Remediation : Analyze the security model of cloud provider interfaces.
  2. Malicious insiders : The threat of a malicious insider is well-known to most organizations. This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure.
- Remediation : Determine security breach notification processes.
  3. Shared technology issues : IaaS vendors deliver their services in a scalable way by sharing infrastructure.
- Remediation : Implement security best practices for installation/configuration. Monitor environment for unauthorized changes/activity.
  4. Data loss or leakage : There are many ways to compromise data. Deletion or alteration of records without a backup of the original content is an obvious example. Unlinking a record from a larger context may render it unrecoverable, as can storage on unreliable media. Loss of an encoding key may result in effective destruction.
- Remediation : Implement strong API access control. Encrypt and protect integrity of data in transit.

5. Account or service hijacking : Attack methods such as phishing, fraud and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks.

- Remediation : Prohibit the sharing of account credentials between users and services. Leverage strong two-factor authentication techniques where possible. Employ proactive monitoring to detect unauthorized activity.

## 5.4 Data Security in Cloud : Security Issues and Challenges

**SPPU : March-20**

- Cloud computing security challenges fall into three broad categories :
  1. **Data protection :** Securing your data both at rest and in transit
  2. **User authentication :** Limiting access to data and monitoring who accesses the data
  3. **Disaster and data breach :** Contingency planning
- Data protection : Data needs to be encrypted at all times, with clearly defined roles when it comes to who will be managing the encryption keys.
- User authentication : Data resting in the cloud needs to be accessible only by those authorized to do so, making it critical to both restrict and monitor who will be accessing the company's data through the cloud. In order to ensure the integrity of user authentication, companies need to be able to view data access logs and audit trails to verify that only authorized users are accessing the data.
- Contingency planning : With the cloud serving as a single centralized repository for a company's mission-critical data, the risks of having that data compromised due to a data breach or temporarily made unavailable due to a natural disaster are real concerns.
- **Security challenges for cloud service customers :**
  1. **Ambiguity in responsibility :** A CSC uses services based on different service categories as well as different deployment models. If the responsibilities are not clearly defined in any of these cases then it may result in inconsistency or may leave an open gate for attacks.
  2. **Loss of trust :** Because of the abstraction of the security implementation details between a CSC and a CSP, it is difficult for a CSC to get details of the security mechanisms that the CSP has implemented to keep the cloud data secure.
  3. **Loss of governance :** When the CSC uses cloud services, it has to move its data onto the cloud and has to provide certain privileges to the CSP for handling the data in the cloud. This may result in misconfiguration or an attack due to the abstraction of the CSP's cloud practices and due to the privileges that need to be given to the CSP.

4. **Loss of privacy :** CSC's privacy may be violated due to leakage of private information while the CSP is processing CSC's private data or using the private information for a purpose that the CSP and CSC haven't agreed upon.
5. **Cloud service provider lock-in :** This issue arises if a CSP doesn't abide by the standard functions or frameworks of cloud computing and hence makes it difficult for a CSC using its services to migrate to any other CSP. The use of non-standard functions and cloud framework makes the CSP non-inter-operable with other CSPs and also leaves CSC open to security attacks.
6. **Misappropriation of intellectual property :** A CSC may face this challenge due to the possibility that a CSC's data on the cloud might leak to third parties that are using the same CSP for their cloud services. This leakage may violate the CSC's copyrights and may result in the disclosure of CSC's private data.
7. **Loss of software integrity :** A CSC encounters this challenge due to the fact that its software is running in the cloud once it is given to the CSP. It is possible that this software might be tampered with or might be affected while the software is running in the CSP and is not in CSC's control, resulting in CSC's loss over its software.

### 5.4.1 Advantages

- **Data centralization :** service provider takes responsibility of storage and small organization need not spend more money for personal storage device.
- **Incident response :** IaaS providers contribute dedicated legal server which can be used on demand.
- Forensic image verification time.
- **Logging :** storage requirement for benchmark logs is mechanically solved.

### 5.4.2 Disadvantages

- Loss of control : The enterprise's loss of control in enhancing the network's security is the most significant disadvantage of cloud computing security. The responsibility of securing the network is shared between the Cloud Service Provider (CSP) and the enterprise.
- Reduced visibility and control : when migrating to a cloud based computing model, organizations will lose a degree of visibility and control, with some responsibility for policies and infrastructure moving to the cloud provider.
- Unsecure API and interfaces.
- Data segregation

**Review Question**

1. *What are the security challenges in cloud computing ?*

**SPPU : March-20, In Sem, Marks 5**

## 5.5 Content Level Security

- Content-based security is a departure from traditional enterprise content management security measures that focus on restricting access to a static repository or network, or on securing specific devices or applications.
- Specific content-based security features include restricting who can open, email, print or edit a piece of content and placing a time limit on how long a user can access a given piece of content. Content can expire from a given repository and no longer be viewable by anyone.
- Content-based security enables custodians of enterprise information to define and control the scope of actions available for users handling content (such as business records or documents), regardless of the physical location of the content in question. This can be useful for organizations that extensively use cloud computing and enterprise mobility technologies that take company information outside the enterprise firewall.

## 5.6 Cloud Security Services

- The basic security services for information security include assurance of data confidentiality, integrity and availability.
- Fig. 5.6.1 shows organization of data security and privacy in cloud computing.

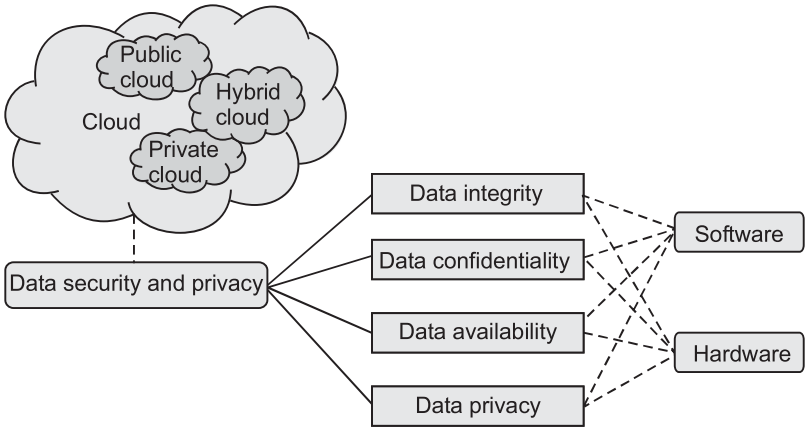


**Fig. 5.6.1**

**1. Confidentiality :**

- Confidentiality refers to limiting information access. Sensitive information should be kept secret from individuals who are not authorized to see the information. In cloud environments, confidentiality primarily pertains to restricting access to data in transit and storage.
- Data confidentiality is important for users to store their private or confidential data in the cloud. Authentication and access control strategies are used to ensure data confidentiality.
- The data confidentiality, authentication and access control issues in cloud computing could be addressed by increasing the cloud reliability and trustworthiness.
- Because the users do not trust the cloud providers and cloud storage service providers are virtually impossible to eliminate potential insider threat, it is very dangerous for users to store their sensitive data in cloud storage directly.
- Simple encryption is faced with the key management problem and cannot support complex requirements such as query, parallel modification and fine-grained authorization.

**2. Integrity :**

- This service protects data from malicious modification. When having outsource their data to remote cloud servers, cloud users must have a way to check whether or not their data at rest or in transit are intact. Such a security service would be of the core value to cloud users.
- Integrity can extend to how data is stored, processed and retrieved by cloud services and cloud-based IT resources.
- Data integrity in the cloud system means preserving information integrity. The data should not be lost or modified by unauthorized users.
- Data integrity in the cloud system means preserving information integrity. The data should not be lost or modified by unauthorized users.
- Data integrity is the basis to provide cloud computing service such as SaaS, PaaS and IaaS.
- Besides data storage of large-scaled data, cloud computing environment usually provides data processing service. Data integrity can be obtained by techniques such as RAID-like strategies and digital signature.

**3. Availability :**

- This service assures that data stored in the cloud are available on each user retrieval request. This service is particularly important for data at rest in cloud servers and related to the fulfillment of service level agreement.

- Data availability means the following : When accidents such as hard disk damage, IDC fire, and network failures occur, the extent that user's data can be used or recovered and how the users verify their data by techniques rather than depending on the credit guarantee by the cloud service provider alone.
- The cloud service provider should ensure the data security, particularly data confidentiality and integrity. The cloud provider should share all such concerns with the client and build trust relationship in this connection. The cloud vendor should provide guarantees of data safety and explain jurisdiction of local laws to the clients.
- Disaster recovery plan is a plan designed to recover all the vital business processes during a disaster with in a limited amount of time. This plan has all the procedures required to handle the emergency situations.
- A disaster recovery process should have provable recovery capability, and hence it provides the most efficient method to be adopted immediately after a disaster occurs.

## 5.7 Security Authorization Challenges in the Cloud

- Authorization is the function of specifying access rights/privileges to resources related to information security and computer security in general and to access control in particular.
- Authorization determines what the user can access and what he cannot access

**1. Auditing :**

- Cloud security audit can help by assessing and prioritizing risks, evaluating current controls, identifying the gaps in existing cloud security strategy and programs and making recommendations tied to business priorities.
- Functions performed by IT auditors :
  a. Backup controls
  b. Data center security
  c. System development standards
  d. System and transaction controls
  e. Contingency plan.

**2. Accountability :**

- This is the process that keeps track of a user's activity while attached to a system; the trail included the amount of time attached, the resources accessed, and how much data transferred.

- Accounting data is used for trending, detecting breaches and forensic investigating. Keeping track of users and their activities serves many purposes.
- For example, tracing back to events leading up to a cyber security incident can prove very valuable to a forensics analysis and investigation case.

## 5.8 Secure Cloud Software Requirements

- Requirements of secure cloud software are as follows :
  1. **Secure Development Practices :** It includes data handling, code practices, language options, input validation and content injection, physical security of the system.
  2. **Approaches to cloud software requirements engineering :** A resource perspective on cloud software security requirements, goal-oriented software security requirements and monitoring internal and external requirements.
  3. **Cloud security policy implementation and decomposition :** Includes implementation issues, decomposing critical security issues into secure cloud software requirements (Confidentiality, Integrity, Availability, Authentication and Identification, Authorization, Auditing).

## 5.9 Secure Cloud Software Testing

- Cloud testing, also called cloud-based testing, is the assessment of a Web application's performance, reliability, scalability and security in a third-party's cloud computing environment.
- Compared to a traditional on-premises environment, cloud testing offers users pay-per-use pricing, flexibility and reduced time-to-market.
- The test processes and technologies used to perform functional testing against cloud-based applications are not significantly different than traditional in-house applications, but awareness of the non-functional risks around the cloud is critical to success.
- For example, if testing involves production data, then appropriate security and data integrity processes and procedures need to be in place and validated before functional testing can begin.
- In the cloud environment, any application can be subjected to the following types of testing :
  1. Functional testing to ensure that software meets functional requirements
  2. Non-functional testing to ensure the quality of service
  3. Ability testing to show whether users will receive application services from the cloud environment on-demand

- Functional testing : Functional software testing checks all the features and functions of software and its interaction with hardware. For conducting functional testing, testers can use such tools as Rapise, Sauce Labs and TimeShiftX
- Non-functional testing : Non-functional testing is also known as performance testing, as it allows you to check the non-functional aspects of software like its performance, usability, and reliability. For conducting this type of testing, you can use cloud-based tools such as CloudTest, AppPerfect, CloudTestGo and AppLoader
- Ability testing : Ability testing is necessary to verify whether users really receive application services on demand.
- Cloud testing focuses on the core components like
  1. **Application :** It covers testing of functions, end-to-end business workflows, data security, browser compatibility, etc.
  2. **Network :** It includes testing various network bandwidths, protocols and successful transfer of data through networks.
  3. **Infrastructure :** It covers disaster recovery test, backups, secure connection and storage policies. The infrastructure needs to be validated for regulatory compliances.

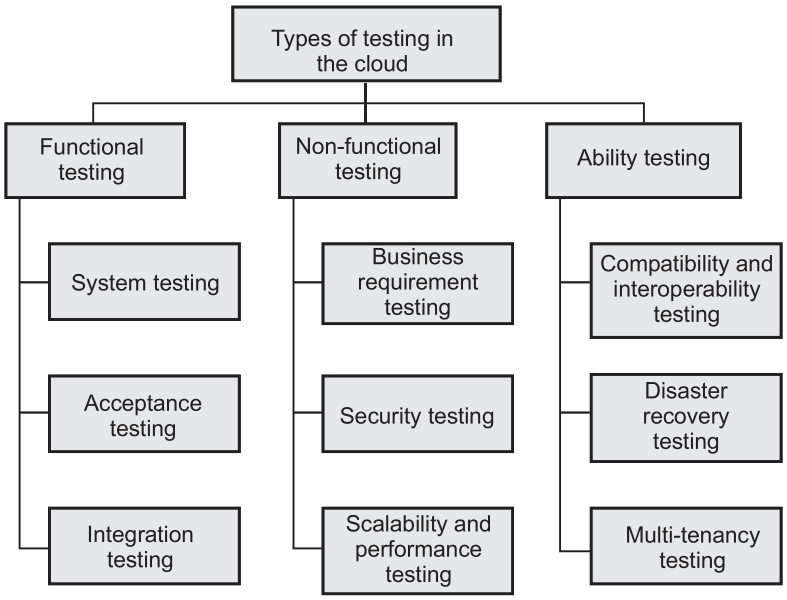


**Fig. 5.9.1**

### 5.9.1 Type of Testing in Cloud

- The whole cloud testing is segmented into four main categories,
  a) **Testing of the whole cloud :** The cloud is viewed as a whole entity and based on its features testing is carried out. Cloud and SaaS vendors, as well as end users, are interested in carrying out this type of testing
  b) **Testing within a cloud :** By checking each of its internal features, testing is carried out. Only cloud vendors can perform this type of testing
  c) **Testing across cloud :** Testing is carried out on different types of cloud-like private, public and hybrid clouds
  d) **SaaS testing in cloud :** Functional and non-functional testing is carried out on the basis of application requirements

### 5.9.2 Benefit of Cloud-based Testing

- In contrast to traditional software testing, cloud-based testing has several unique advantages :
- Scalability : Cloud computing allows testers to increase or decrease computing resources according to their needs.
- Cost-cutting : In cloud computing, you pay only for those resources that you use.
- Timesaving : With cloud-based testing, an application can be simultaneously run on different hardware so testers can spend more time fixing defects.
- Easily customizable : By using cloud-based tools and services, testers can easily emulate an end-user-centric environment with minimum cost and time.
- Properly configured test environment : It usually takes much time to properly set up a test environment on multiple devices.
- Ensure comprehensive testing : In order to conduct comprehensive testing, the test team needs to run an application on all possible devices that support different platforms, operating systems and browsers.
- Faster testing : Cloud-based testing tools ensure automated testing, which greatly reduces the time to market for software.
- Constant availability : Software testing in the cloud is available to testers at any time.

## 5.10 Multiple Choice Questions

**Q.1** _____ ensures that information is not changed or altered in transit.

a Integrity
b Authentication
c Confidentiality
d Availability

**Q.2** _____ prevents either sender or receiver from denying a transmitted message.

a Integrity
b Nonrepudiation
c Confidentiality
d Availability

**Q.3** _____ management is the total process used to identify, control, and minimize the impact of uncertain events.

a Software
b Hardware
c Risk
d All of these

**Q.4** The responsibility of securing the network is shared between the _____ and the enterprise.

a network user
b cloud service provider
c middle service provider
d all of these

**Q.5** A security _____ is a statement produced by the senior management of an organization.

a mechanism
b policy
c method
d all of these

**Answer Keys for Multiple Choice Questions :**

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Q.1** | a | **Q.2** | b | **Q.3** | c | **Q.4** | b | **Q.5** | b |

❑❑❑

# Unit - VI

# 6 Advanced Techniques in Cloud Computing

## *Syllabus*

*Future Trends in cloud Computing, Mobile Cloud,* ***Automatic Cloud Computing :*** *Comet Cloud.* ***Multimedia Cloud :*** *IPTV, Energy Aware Cloud Computing, Jungle Computing, Distributed Cloud Computing Vs Edge Computing, Containers, Docker, and Kubernetes, Introduction to DevOps.* ***IOT and Cloud Convergence :*** *The Cloud and IoT in your Home, The IOT and cloud in your Automobile, PERSONAL : IoT in Healthcare.*

## *Contents*