Unit V

Security in Cloud Computing

Course Objective5:
To study risk management in cloud computing

Points to cover:

- **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.

Part I: **Risks in Cloud Computing**

- Risk Management
- Enterprise-Wide Risk Management
- Types of Risks in Cloud Computing.

Reference Material:

Srinivasan, J. Suresh, “Cloud Computing: A Practical Approach for Learning and Implementation”,
Chap 18, pg 225 - 234

Part II: **Data Security in Cloud**

- Security Issues
- Challenges, advantages, Disadvantages
- Cloud Digital persona and Data security
- Content Level Security.

Reference Material:

Srinivasan, J. Suresh, “Cloud Computing: A Practical Approach for Learning and Implementation”,

Chap 19, pg 237 - 243

Part III: **Cloud Security Services**

- Confidentiality, Integrity and Availability
- Security Authorization Challenges in the Cloud
- Secure Cloud Software Requirements
- Secure Cloud Software Testing.

Reference Material:

Srinivasan, J. Suresh, “Cloud Computing: A Practical Approach for Learning and Implementation”,
Chap 20, pg 245 - 250

Cloud Computing

- The most widely used computing paradigm
- Brought the change in information and communications technology industry
- ***How??***
- Modifying the means by which software programs and hardware are trusted and purchased
- Successful due to the key capabilities such as:
  (i) all computing needs are suggested as a service,
  (ii) the proficiency in dynamically providing computational resources
- two types of cloud providers:
  1. Cloud Service Providers (CSP) or either SaaS or PaaS providers.
  2. Cloud Infrastructure Providers (CIP) or IaaS providers.

Result….

- Some new risks have appeared
- Cloud community: to recognize cloud-specific risks and re-evaluate accepted ones.
- Cloud services not just providers, should be the subject of risk administration and assessment.
- Risks in cloud environments should be advised at :
  - Service,
  - Data,
  - Infrastructure layers
- Sometimes, status of risk will alter considerably with the type of cloud architecture.
- It is likely for cloud clients to move some risks to external cloud providers.

- The most significant risks presented by cloud computing are:
  - SLAs violations,
  - proficiency to sufficiently consider risks of a cloud provider,
  - blame to defend sensitive data,
  - virtualization related risks,
  - reduction of direct command of assets and software programs,
  - compliance risks and decreased reliability since service providers may proceed out of business.

- On the contrary, there are some customary risks that should be re-evaluated.
  - For example, the risk of **network breach** is now more critical for cloud organizations since they are completely based on the network.
- Other risks, for example, **natural disasters**, should be advised specially for double-checking high-availability of cloud services.
- Cloud computing requires that businesses, the users of IT services, can purchase their IT associated services as a service.
- ***Instead of buying servers*** for interior or external services, or ***buying software programs licenses***, the organization can purchase them ***as a service***.
- **Hosting services** : authorizing us **to aim more on the enterprise** rather on the IT infrastructure.

Example

- A large-scale vendor is trading their items through a web portal.
- They require access to servers and infrastructure to support the large-scale peaks in demand, but most of the time they can manage with lesser capacity.
- They start wondering if they really have to own numerous infrastructures which are not completely utilized most of the time.
- With a hosting service, the large-scale vendor could purchase the required infrastructure as a service, pay a monthly or annual charge and worry less about their infrastructure.
- They would purchase precisely the capacity they require, as they require it at peak times.
- With cloud computing, they would pay for a top quality service based on the usage.

Levels in cloud computing

- There are some identified levels in cloud computing.
- The vendors in these levels have very distinct service offerings and functioning models.
- Some vendors focus on construction and sustaining a huge data centre, while other focus on constructing a user-friendly and feature-rich application.
- The levels, from bottom to top, are:

1. infrastructure,
2. storage,
3. platform,
4. application,
5. services and
6. client.

Levels in cloud computing

1. ***Infrastructure:***

- At the base is the infrastructure of the service or the platform virtualization.
- Users get the server environment as they want.
- The basic scheme
- Clients need to handle the server, all software programs installed and maintained on their own.

Levels in cloud computing

2. ***Storage:***

- With the storage level, one can get a database or something similar and pay per gigabyte per month.
- A storage level is nothing new or exceptional, except for the full stack of services.
- Options for storage.
- Examples : relational databases, Google's BigTable and Amazon's SimpleDB.

Levels in cloud computing

3. ***Platform:***

- The platform level has solution stacks, for example, Ruby on Rails, LAMP or Python Django.
- A start-up organization need not deal with the setting up of server programs, or upgrade their versions, because that comes with the service.
- They can aim on evolving and trading their application.

Levels in cloud computing

4. Application:

- The application level comprises applications that are suggested as services.
- The most well-known demonstrations:

  Salesforce.com and Google Docs
- Number of genuine applications that can be bought as services.

Levels in cloud computing

5. Services:

- The services level comprises interoperable machine-to-machine procedures over the network.
- The most common example : web services.
- Other examples:
  - payments schemes: PayPal
  - mapping services such as Google Maps and Yahoo Maps.

Levels in cloud computing

6. Client:

- At the highest of the stack is the consumer level
- Comprises the users of the cloud systems.
- Clients : desktop users and mobile users (Symbian, Android, iPhone).
- There are possibilities for vendors to exit and adapt new services, and for clients to find new services and applications to solve their problems.

five security concerns

- Although cloud computing can offer small enterprises important cost-saving advantages, namely, pay-as-you-go access to complicated programs and massive hardware, the service does come with certain security risks.
- While evaluating the promise of cloud-based service providers, one should hold following top five security concerns in mind:
- 1. Secure data transfer
- 2. Secure programs interfaces
- 3. Secure retained data
- 4. User access to control
- 5. Data separation

Cloud Computing Risks

- **Risk #1—*The solution may not meet its economic objectives:***
- Do the short-run and long-run ROI work.
- The key components to address when considering cloud ROI risk : **utilization, speed, scale and quality**.
- These components are constructed into most ROI forms and sway the headline numbers for buying into income, cost and time to return.

Cloud Computing Risks

- **Risk #2**—*The solution may not work in the context of the client enterprise's association and culture:*
- The best way to address is having a clear vision and direction for enterprise transformation, which involves top-level support.
- This should encompass
  - **the establishment of a clear roadmap** for procurement or implementation of cloud services and
  - **applications** that use them and coordination of stakeholders and
  - **competing schemes** to get agreement for storage, computing, mesh and applications to bypass islands of demand usage.

Cloud Computing Risks

- ***Risk #3—The solution may be tough to evolve due to the adversity of incorporating the cloud services involved:***
- There is a risk which will not be probable to include in cloud services with the current system and with each other.
- The service integration risk can be considered by contemplating interface alteration cost, proficiency to change the existing system and available skills.

Cloud Computing Risks

- ***Risk #4—A catastrophe may occur from which the solution will not recover:***
- As part of a risk investigation, it should recognize the unplanned activities that could damage and assess their probabilities and impacts.
- One may also wish to make general provision for unpredicted activities that disturb the cloud services that use or impair the data.

Cloud Computing Risks

- ***Risk #5—System value may be insufficient, in order that it does not meet the users' needs:***
- The value of an external service can be considered utilizing the identical components as for the value of the solution.
- In addition, look at the track records of suppliers very carefully.

Cloud Computing Risks

- ***Risk #6 —There may be an existing need for service orientation:***
- Not having full-fledged SOA isn’t inevitably strategic in itself when opting for cloud.
- But the incompetence to lead methods from present interfaces and inherent applications to more agile cloud services could actually mess up things.
- Finally it will make cloud more costly than leaving things as it is.

RISK MANAGEMENT

- A significant part of business planning
- To reduce or eliminate the risk of certain types of events or having an impact on the business.
- A method to recognize, consider and prioritize risks of different types
- Once the risks are recognized, the risk supervisor will consider a design to minimize or eliminate the effect of conflicting events.
- Several risk administration measures, including those evolved by the
  - Project Management Institute,
  - International Organization for Standardization (ISO),
  - National Institute of Science and Technology and
  - societies

- There are numerous distinct kinds of risks that risk management designs can mitigate.
- Common risks encompass risks such as **disasters** in the workplace or blazes, tornadoes, earthquakes and other **natural disasters**.
- It can also involve **legal risks** like deception, robbery and harassment lawsuits.
- Risks can also concern to the organizational practices, doubt in economic markets, flops in tasks, borrowing risks, or the security and storage of data and records.

Risk Management in Cloud Computing

- Google, Microsoft, IBM and all other renowned and unidentified cloud providers offer an array of foremost cost saving options to the customary data centre and IT department.
- 45% of IT professionals believe the risks overshadow the advantages and only 10% of those reviewed said they would prefer doing objective critical applications to the cloud.

- ISACA’s statistics and other commercial data around cloud adoption show that cloud computing is a mainstream alternative but decisively not the prime choice.
  - **Information Systems Audit and Control Association**
- While some organizations have effectively shifted part or all of their data assets into some pattern of cloud computing infrastructure, the majority are not left with much choice.

- Cloud computing is somewhat new in its present pattern, it is best directed to reduce intermediate risk enterprise areas.
- Don’t hesitate to inquire and if need be, enlist an unaligned consulting business to direct through the process.
- Selecting a cloud provider needs far more diligence than usual IT procurement.
- For this purpose, there is no clear cut template for success.
- The outcomes can be excellent if the risks are well managed.

ENTERPRISE WIDE RISK MANAGEMENT

- What is Risk Management?
- The Risk Management Process

Risk….

- Risk can be characterized as ‘the possibility of loss or twisted unsafe component or component, or an exposure to hazard or danger.
- It is very tough to consider any enterprise function, method, or undertaking that will not take advantage by methodically considering the risks that can have a contradictory influence on an enterprise’s competitiveness and profitability.
- Effectively organizing or commanding the origin of risk can have an effect in market authority: robust development, premium supply charges and investor confidence.

What is Risk Management?

- The practice followed to prevent as many errors as possible and planning fee procedures for the rest.
- Risk management is technical and set about considering the untainted risks faced by users and businesses.
- A risk supervisor is generally a highly trained person who makes risk management his/her full time job or the responsibilities may be dispersed within a risk management department.

- Risk management is not just buying protection for a company.
- It also considers both insurable and uninsurable risks and an alternative method.
- The focus of risk administration is to reduce the cost of managing risk by adapting the most suitable means.
- Insurance thus occurs to be one of the many advances for minimizing untainted risks the firm faces.
- When the risk manager's function embraces untainted risk avoidance they spend their time in analyzing the following:

  ● Hazards, for example, blaze, tornado or hurricanes, robbery, piracy, vandalism and crime.

  ● Internal procedure exposures initiated by security and security practices, workers' reimbursement and worker dishonesty

The Risk Management Process

- Risk management process includes,

  (i) determination of objectives,

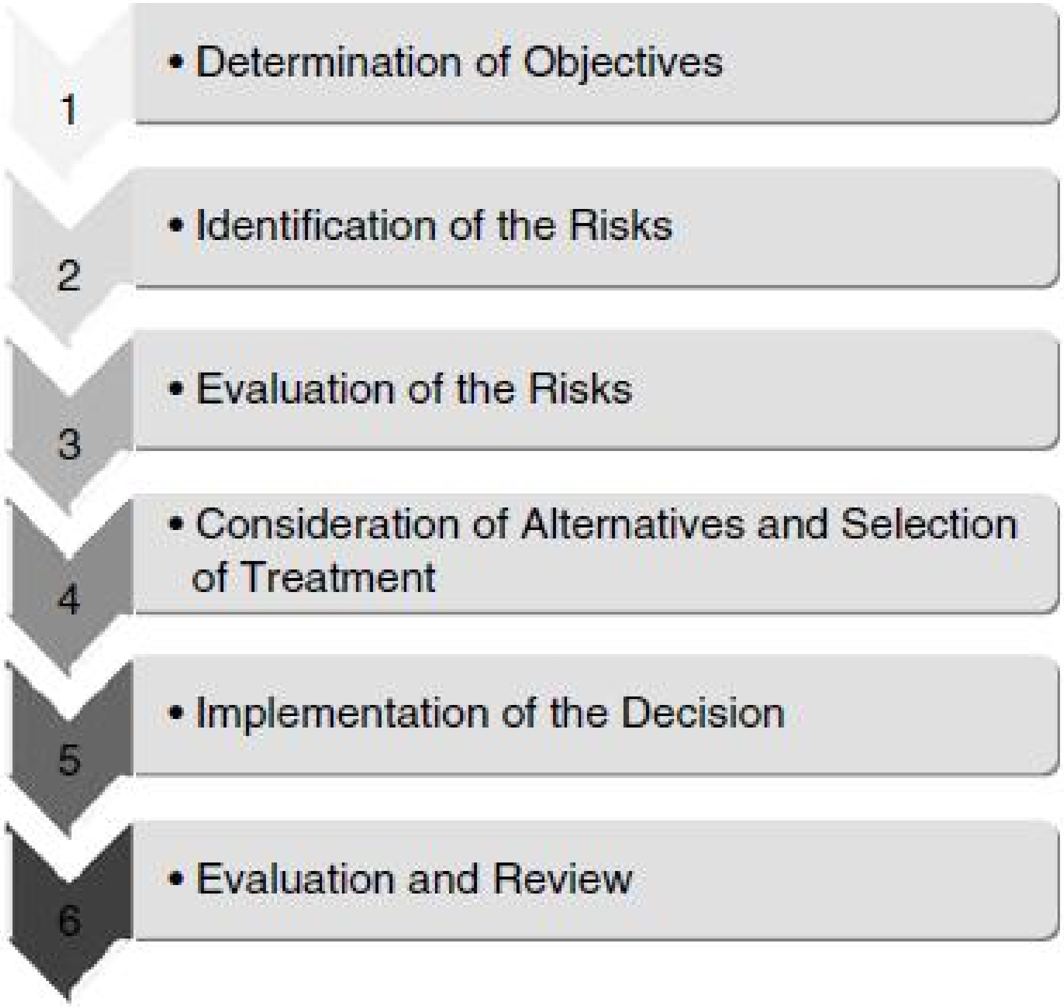
  (ii) identification of the risks,

  (iii) evaluation of the risks,

  (iv) consideration of alternatives and selection of risk treatment,

  (v) implement of the decision and

  (vi) evaluation and review.



1. • Determination of Objectives
2. • Identification of the Risks
3. • Evaluation of the Risks
4. • Consideration of Alternatives and Selection of Treatment
5. • Implementation of the Decision
6. • Evaluation and Review

Figure 18.1 Six-step Risk Administration Process

Diagram : the methods in risk management

- The method comprises of six steps which either an expert or non-professional risk supervisor can chart to an organizations enterprise conclusions and business goals

Step 1

- Determination of the objectives of the risk administration program, concluding accurately what the association anticipates its risk administration program to do.
- One prime target of the risk administration effort is **to maintain the functioning effectiveness of the organization.**
- The second target is the humanitarian aim of **defending workers from misfortunes that might outcome in death or grave injury**.

Step 2

- The identification of the risks involves somebody being cognizant of the risks.
- The next tools or methods supply awareness:
  - Risk analysis questionnaires
  - Exposure checklists
  - Insurance policy checklists
  - Flowcharts
  - Analysis of financial statements
  - Other internal records
  - Inspections
  - Interviews

Step 3

- Once the risks are recognized, the risk supervisor should evaluate the risks.
- Evaluation entails assessing the promise dimensions of the reduction and the likelihood that it is probable to occur.
- The evaluation needs grading of main concerns as **critical risks, significant or insignificant risks**.

Step 4

- Consideration of options and assortment of the risk remedy device, examines diverse advances utilized to deal with risks and the assortment of the method that should be utilized for each one.

Step 5

- Risk financing means encompass risk-keeping and risk moving or risk shifting.
- Risk remedy apparatus are utilized in concluding which method to use to deal with a granted risk, the risk supervisor considers the dimensions of the promise decrease, its likelihood and the assets that would be accessible to meet the loss if it should occur.

Step 6

- The last step, evaluation and reconsider are absolutely crucial to the program for two reasons.
- Within the risk administration method the enterprise environment alterations, new risks originate and old ones disappear.
- Techniques befitting last year may have become obsolete this year and so constant attention to risk is required.

Enterprise Risk Management (ERM)

- ERM in enterprise includes the procedures and methods utilized by organizations to organize risks and grab possibilities associated to the accomplishment of their objectives.
- ERM presents a structure for risk administration, which normally engages recognizing specific events or reducing components applicable to the organization’s objectives (risks and opportunities), considering them in times of prospect and magnitude of influence, working out for a solution and supervising progress.
- By recognizing and proactively speaking to risks and possibilities, enterprises defend and conceive worth for their stakeholders, encompassing proprietors, workers, clients, controllers and society in general.

Part I: **Risks in Cloud Computing**

- ✓ Risk Management
- ✓ Enterprise-Wide Risk Management

- Types of Risks in Cloud Computing.

Reference Material:

Srinivasan, J. Suresh, “Cloud Computing: A Practical Approach for Learning and Implementation”,
Chap 18, pg 225 - 234

Types of Risks in CC

(i) misuse and illicit use of cloud computing,
(ii) insecure interfaces and APIs,
(iii) vicious insiders,
(iv) issues-related technology sharing,
(v) data loss or leakage,
(vi) hijacking (account/service) and
(vii) unknown risk profile.

Risk in CC

Threat #1—Misuse and illicit use of cloud computing:

- Unlegislated individuals may take advantage of the befitting registration, straightforward methods and somewhat anonymous access to cloud services to launch diverse attacks.
- Examples of such attacks include:
  - password and key breaking,
  - DDOS,
  - malicious data hosting,
  - commencing dynamic strike points,
  - botnet command/control and
  - CAPTCHA-solving farms.
- Targets are IaaS, PaaS.

Threat #2—Insecure interfaces and APIs:

- Customers organize and combine with cloud services through interfaces or APIs.
- Providers should double-check that security is incorporated into their service forms, while users should be cognizant of security risks in the use, implementation, and administration and monitoring of such services.
- API dependencies, logging capabilities, inflexible access to controls, anonymous access, reusable passwords, clear-text authentication, transmission of content and improper authorizations are the example of such risks.
- Targets are IaaS, PaaS, SaaS.

Threat #3—Vicious insiders:

- Vicious insiders represent a larger risk in a cloud computing environment, since clients manage not have a clear outlook of provider principles and procedures.
- Vicious insiders can gain unauthorized access into organizations and their assets.
- Some risks encompass impairment, economic influence and decrease of productivity.
- Targets are IaaS, PaaS, SaaS.

Threat #4—Issues-related technology sharing:

- IaaS is based on distributed infrastructure, which is often not conceived to accommodate a multi-tenant architecture.
- Overlooked flaws have authorized visitors to gain unauthorized rights and/or leverage on the platform.
- Targets are IaaS

Threat #5—Data loss or leakage:

- Compromised data may encompass

  (i) deleted or changed data without producing a backup,

  (ii) unlinking a record,

  (iii) decrease of an encoding key and

  (iv) unauthorized access to perceptive data.

- The likelihood of data compromise considerably rises in cloud computing, due to the architecture and operations.
- Examples of data loss/ leakage include:

  (i) insufficient authentication,

  (ii) authorization,

  (iii) review (AAA) controls,

  (iv) inconsistent encryption,

  (v) inconsistent programs keys,

  (vi) operational flops,

  (vii) disposal challenges,

  (viii) risk of association,

  (xi) jurisdiction/political issues,

  (x) persistence and trials,

  (xi) data centre reliability and catastrophe recovery.

- Targets are IaaS, PaaS, SaaS.

Threat #6—Hijacking (Account/Service):

- Account or service hijacking is generally carried out with pilfered credentials.
- Such attacks encompass phishing, deception and exploitation of programs vulnerabilities. Using pilfered credentials, attackers can access critical localities of cloud computing services and compromise the confidentiality, integrity and accessibility (CIA) of such services.
- Examples of such attacks include eavesdropping on transactions/sensitive undertakings, manipulation of data, coming back with falsified data, redirection to illegitimate sites.
- Targets are IaaS, PaaS, SaaS.

Threat #7—Unknown Risk Profile:

- Cloud services signify that organizations are less engaged with hardware and software ownership and maintenance.
- Although this boasts important benefits, organizations should be cognizant that matters like internal security systems, security compliance, configuration hardening, patching, auditing and logging may be overlooked.
- Targets are IaaS, SaaS, PaaS.

Part I: **Risks in Cloud Computing**

- ✓ Risk Management
- ✓ Enterprise-Wide Risk Management
- ✓ Types of Risks in Cloud Computing.

Reference Material:

Srinivasan, J. Suresh, “Cloud Computing: A Practical Approach for Learning and Implementation”,
Chap 18, pg 225 - 234

Part II: **Data Security in Cloud**

- Security Issues
- Challenges, advantages, Disadvantages
- Cloud Digital persona and Data security
- Content Level Security.

Reference Material:

Srinivasan, J. Suresh, “Cloud Computing: A Practical Approach for Learning and Implementation”,
Chap 19, pg 237 - 243

Internal Security Risks

- **Malicious Insiders:** Employees or contractors with authorized access to cloud resources who intentionally misuse or compromise data.
- **Data Breaches:** Unauthorized access to sensitive data, potentially caused by weak security measures, misconfigurations, or insider threats.
- **Misconfiguration:** Incorrectly configured cloud environments leading to vulnerabilities and potential breaches.
- **Insecure APIs:** Unprotected APIs can be exploited by attackers to gain access to cloud resources and data.
- **Account Hijacking:** Unauthorized access to user accounts through stolen credentials or phishing attacks.

Internal Security Risks (1)

- **Human Error:** Mistakes in security protocols or procedures can lead to vulnerabilities.
- **Lack of Visibility:** Difficulty in monitoring and controlling cloud resources, making it harder to detect and prevent security incidents.
- **Shadow IT:** Unapproved cloud services used by employees can create security gaps and vulnerabilities.
- **Inadequate Identity and Access Management (IAM):** Weak or poorly implemented IAM practices can lead to unauthorized access.
- **Data Loss:** Data can be lost or corrupted due to system failures, human error, or malicious attacks.
- **Malware Injection:** Malicious software can be injected into cloud environments, potentially compromising data and systems.

External Security Risks

1. **Cyberattacks:** Malicious actors attempting to exploit vulnerabilities in cloud infrastructure or applications.
2. **Data Breaches:** Unauthorized access to sensitive data, potentially caused by weak security measures, misconfigurations, or insider threats.
3. **Denial-of-Service (DoS) Attacks:** Overwhelming cloud infrastructure with traffic, making it unavailable to legitimate users.
4. **Insecure Interfaces:** Unprotected APIs or web interfaces can be exploited by attackers to gain access to cloud resources and data.
5. **Account Hijacking:** Unauthorized access to user accounts through stolen credentials or phishing attacks.

External Security Risks

6. **Phishing:** Deceptive emails or websites designed to trick users into revealing sensitive information.
7. **Ransomware:** Malicious software that encrypts data and demands a ransom for its release.
8. **Shared Infrastructure Vulnerabilities:** Security vulnerabilities in the shared infrastructure of cloud providers can affect multiple customers.
9. **Data Leakage:** Sensitive data can be leaked or exposed due to security flaws or breaches.
10. **Compliance Issues:** Failure to comply with industry regulations or standards can lead to security risks and penalties.

- Cloud computing has flexibility, as it outsources the services. This property adds risks, because of malicious intents who can make the unauthorized persons to login into the system.
- Cloud computing technologies can be utilized as a platform for commencing attacks, hosting spam/malware, programs exploits, and for numerous other unethical reasons.
- Cloud computing architecture presents larger trials in commanding and mitigating risks due to its exclusive structure and operational attributes.

In cloud computing,

- Internal Security Risks stem from within an organization, like malicious insiders or misconfigurations
- External Security Risks originate from outside, such as cyber attacks or data breaches.

Data to be protected…how?

- **The levels of security of any data** should be considered as concentrated levels of progressively omnipresent security, which are broken down into components to display the expanding granularity of this pervasiveness:
  - *Level 1: Transmission of the document utilizing encryption protocols*
  - *Level 2: Access control to the document itself, but without encryption of the content*
  - *Level 3: Access control (including encryption of the content of a data object)*
  - *Level 4: Access control (including encryption of the content of a data object) also encompassing privileged administration choices*

- Many organizations use one time sign-in method to make things simpler and regulate client authentication over a collection of applications.
- Force.com carries two single sign-on options:

1. Federated authentication
2. Delegated authentication

1. Federated authentication:

- Uses benchmark protocols to broadcast between the organization and the Force.com platform for authentication purposes.
- The organization configures the platform to use SAML (Security Assertion Markup Language).

2. Delegated authentication

- Enables an organization to incorporate Force.com cloud applications with an alternative authentication procedure, for example, an LDAP (Lightweight Directory Access Protocol) service or authentication utilizing a token rather than a password.
- The delegated administration can be set up to validate users in three distinct combinations:

(i) Password validation: Username and password are validated contrary to the delegated administration rather than of the interior Salesforce password store.

(ii) Token validation: Users should first authenticate to their enterprise and the enterprise in turn should conceive a Salesforce by dispatching (via HTTP POST) the username and a token to Salesforce for validation by the delegated authority.

(iii) Hybrid model: While accessing the Salesforce website, users are required to use token validation, but they are permitted to validate using password validation on a consumer application.

Authentication Mechanisms in Cloud Services

- Federated authentication streamlines access using standard protocols.
- Delegated authentication allows integration with existing enterprise authentication systems.
- Security profiles and sharing rules enhance control over user access to data.

- Two prime mechanisms for client access to assets on the Force.com platform are: **client profiles and sharing rules.**

1. **User profiles**: Users access is controlled by an organization by customizing user profiles. Among users, organizations can control users by using field-level security.

2. **Sharing rules**: Sharing rules permit for exceptions to organization-wide default settings. It encourages the users to access the records that they don't own. Sharing rules can be based on the record or on standards in the record.

CONTENT LEVEL SECURITY (CLS)

- Content level application of data security authorizes you to double-check that all four levels can be contacted by a single architecture, rather than of multiple models of operations which can cause interoperability and can add extra components of human mistake, foremost to reduce of security.

CLS (1)

- CLS was evolved to meet the marketplace demand and driven by the demands of purchaser institutions.
- Content level security offers organizations to organize data and content at the organizational level, other than at the institutional level.
- CLS presents the expertise to view, edit and delete data based on client functions and permissions for both application-level security and content-level security.
- The new functionality presents users with content that is applicable to them, decreasing the need for applications to run on multiple servers and permitting applications to assist different organizations inside the institution.

CLS (2)

- The CLS solution can be rolled out over an unlimited number of distinct partitions and agencies, with each organization sustaining a concentrated outlook over all of its pertinent functions.
- Other advantages include increased usability aimed at content, new functionality that advances effectiveness and decreases mistakes and reduction in overhead cost with unlimited number of permitted users.

Note….

- Security, availability and reliability are the foremost value concerns of cloud service users.
- Key security benefits of a cloud computing environment are (i) data centralization, (ii) incident response, (iii) forensic image verification time and (iv) logging.
- Key security issues are (i) investigation, (ii) data segregation, (iii) long-term viability, (iv) compromised servers, (v) regulatory compliance, (vi) recovery.

- Cloud computing boasts private and organization a much more unsolidified and opens way of broadcasting information.
- Cloud computing is a platform for conceiving the digital matching of this unsolidified, human to-human data flow, which is a sure thing that internal computing systems have not yet achieved.
- In the context of computing, the terms security, privacy and trust may seem one and same but have distinct meanings.
- CLS evolved to meet the marketplace demands and propelled by the wishes of customer institutions.
- Content level security endows organizations to organize data and content at the organizational level, rather than at the institutional level.

Part III: **Cloud Security Services**

- Confidentiality, Integrity and Availability
- Security Authorization Challenges in the Cloud
- Secure Cloud Software Requirements
- Secure Cloud Software Testing.

Reference Material:

Srinivasan, J. Suresh, “Cloud Computing: A Practical Approach for Learning and Implementation”,
Chap 20, pg 245 - 250

- Confidentiality, integrity, and availability (CIA) are the three core principles of information security, forming the basis for protecting data and systems, ensuring that information is kept private, accurate, and accessible when needed.

CIA….

Confidentiality:

- This principle focuses on restricting access to information to only authorized individuals or systems. It ensures that sensitive data remains private and is not disclosed to unauthorized parties.

Integrity:

- Integrity ensures that data is accurate, complete, and consistent throughout its lifecycle. It means that data has not been altered, corrupted, or destroyed without authorization.

Availability:

- Availability ensures that authorized users can access information and resources when they need it. This includes ensuring that systems and networks are operational and accessible, and that data can be retrieved quickly and reliably.

Data Confidentiality

- Confidentiality refers to limiting data access only to authorized users, and stopping access to unauthorized ones.
- Underpinning the aim of confidentiality are authentication procedures like user-IDs and passwords that exclusively recognize a data system's users and supporting procedures that restrict each recognized user's get access to the data system's resources.
- Confidentiality is associated to the broader notion of data privacy limiting access to individual's information.

- Following are some confidentiality topics that double-check an agreeable level of information is imparted upon employees of the organization.
- Access control
- Passwords
- Biometrics
- Encryption
- Privacy
- Ethics

- Access control: Access control is the means utilized for controlling which assets a client can get access to and the jobs which can be presented with the accessed resources.
- Passwords: Passwords are a basic component of network security. An intruder in the organization’s confidential locality may check under keyboards and in drawers to find passwords that may have been in written down and then use it to gain access to personal information. Password protection can be augmented by added security systems such smart cards and biometric identification systems.

- Biometrics: Biometric expertise can recognize persons based on the individual characteristics like human body parts. The prime biometric technologies in use are retina scanning, facial recognition, voice recognition and fingerprint scanning. A sample is submitted by a client demanding to get access in evaluating with database for a match to get access per missions. Biometric data is tough to replicate and when utilized in conjunction with other access procedures, for example, passwords and badges make a very good protecting as against unauthorized access to organizational resources.

- Encryption: Encryption is any method that converts readable (plain text) data into mystery cipher (cipher text) to avert unauthorized access of information which is used in Internet transactions, e-mail and wireless networking. An encryption algorithm is a mathematical technique which changes the data to unreadable data by unauthorized parties. Encryption is the basis of protecting systems, communications schemes and online transactions. Employees should utilize encryption when likely to double-check its security.

- Privacy: Privacy is the upkeep of confidential or individual data from being viewed by unauthorized parties and the command over its assemblage, usage and distribution. The privacy and confidentiality can be utilized interchangeably.
- Ethics: Employees should be granted clear direction by principle, on what the organization considers agreeable conduct and should furthermore be acquainted with the methods in location for clarification of ethical anxieties and for revelation of unethical activities.

Data Integrity

- Data integrity is characterized as safeguarding the correctness and completeness of data and processing procedures from intentional, unauthorized or unintentional changes.
- Maintaining data integrity is absolutely crucial to the privacy, security and reliability of enterprise data.
- Integrity of data can be compromised by malicious users, hackers, programs mistakes, computer virus, hardware constituent flops and by human mistake while moving data.
- Mitigating data integrity risk can be there for fast recovery of data. Employees can mitigate risk by normal data backups and off-site protected storage of backup, supervising integrity devices and encryption.
- Integrity means trustworthiness of data resources.

Data Availability

- Availability means, availability of data resources.
  - A data system that is not accessible when required is not good.
  - It may be calculated on how reliant the institute has become on carrying out a computer and communications infrastructure.
  - Almost all premier organizations are highly reliant on functioning data systems.
  - Availability, like other facets of security, may be solely influenced by technical matters such as natural phenomena or human causes.
  - While the relation risks affiliated with these classes count on the specific context, the general is that humans are the weakest link.
- Availability is double-checking that the authorized users have access to data and affiliated assets when required.
  - This can be carried out by utilizing data backup, catastrophe recovery and enterprise continuity/recovery plans.
  - Employees should have knowledge about their responsibilities as it concerns data backups, catastrophe recovery and enterprise continuity.

Data Backup Plan

- Data backups are an absolutely crucial part of data security and an organization should be adept to refurbish data in the happening of data corruption or hardware failure.
- Backups should be completed on a normal basis and the frequency depends upon how much data an organization is agreeable to lose in the event of loss.
- Backups should also be occasionally refurbished to check systems that should double-check that the method are functioning correctly inside the particular time limit before the requirement for the backup really arises.

Disaster Recovery Plan (DRP)

- A DRP is a design that is utilized to retrieve rapidly after a catastrophe with a smallest of influence to the organization.
- DR designing should be part of the primary stage of applying IT systems.
- DR designs are evolved in answering to risk evaluations and conceived to mitigate those risks. Risk evaluations work out the frequency and span of promise disasters.
- This will permit an organization to conclude which technologies to apply to accomplish a befitting grade of recovery.

Security Issues and Challenges

- IaaS, PaaS and SaaS : general forms of cloud computing.
- Each of these forms has different influences on application security, whereas in a normal situation where an application is deployed in a cloud, two general security studies occur:
  - How is data protected?
  - How is code protected?
- Cloud computing environment is usually presumed to be economical as well as provides higher service quality.
- Security, availability and reliability are the foremost values of cloud service users.

Security Advantages in Cloud Environments

- Current cloud service providers function as very large systems.
- They have complicated methods and professional staff for sustaining their systems, which small enterprises may not have control over.
- As an outcome, there are numerous direct and indirect security benefits for the cloud users.
- Some of the key security benefits of a cloud computing environment are :

Security Advantages in Cloud Environments

1. **Data centralization**: In a cloud atmosphere, the service provider takes responsibility of storage and small organizations need not spend more money for personal storage devices. Also, cloud-based storage provides a method to centralize the data much faster and probably with low cost.
2. **Incident response**: IaaS providers contribute dedicated legal server which can be used on demand. Whenever there is a violation of the security policy, the server can be intimated through online.
3. When there is a review, a backup of the environment can be effortlessly made and put up on the cloud without affecting the usual course of business.

Security Advantages in Cloud Environments

4. **Forensic image verification time**: Some cloud storage implementations reveal a crypto graphic ascertain addition or hash. For example, MD5 hash function is developed automati cally by Amazon S3 during object storage. Therefore in principle, the time to develop MD5 checkups utilizing external devices is eliminated.
5. Logging: In a usual computing paradigm by and large, logging is regular feature. In gen eral, insuffi cient computer disk space is assigned that makes logging either non-existent or minimal. However, in a cloud, storage requirement for benchmark logs is mechanically solved.

Security Disadvantages in Cloud Environments

- In spite of security features, cloud computing adds some key security issues.
- Some of these key security challenges are summarized as follows:

Security Disadvantages in Cloud Environments

- Investigation: Investigating an illegal undertaking may be unrealistic in cloud environments. Cloud services are particularly hard to enquire, because data for multiple clients may be co-located and may also be dispersed over multiple datacentres. Users have little information about the mesh topology of the inherent environment. Service provider may also enforce limits on the network security of the users.
- Data segregation: Data in the cloud is normally in a distributed simultaneously with data from other customers. Encryption will not be presumed as the single solution for data seg regation issues. Some clients may not desire to encrypt data because there may be a case when encryption misleads can decimate the data.
- Long-term viability: Service providers should double-check the data security in altering enterprise positions, such as mergers and acquisitions. Customers should double-check data accessibility in these situations. Service provider should furthermore confirm data security in contradictory situations such as extended outage, etc.

Security Disadvantages in Cloud Environments

- Compromised servers: In a cloud computing environment, users do not even have an alter native of utilizing personal acquisition toolkit. In a situation where a server is compromised, they require to shut their servers down until they get a backup of the data. This will further create source accessibility concerns.
- Regulatory compliance: Traditional service providers are exempted from outside audits and security certifications. If a cloud service provider does not adhere to these security audits, then it directs to a conspicuous decline in clientele trust.
- Recovery: Cloud service providers should double-check the data security in natural and man-made disasters. Generally, data is duplicated over multiple sites. However, in the case of any such redundant happenings, provider should do an absolute and fast restoration.