Unit 5: Cloud security

Cloud Security Issues

Cloud Security

- Cloud security, also known as cloud computing security, consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data, and infrastructure.
- These security measures are configured to protect cloud data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices.
- From authenticating access to filtering traffic, cloud security can be configured to the exact needs of the business.
- Rules can be configured and managed in one place, administration overheads are reduced and IT teams empowered to focus on other areas of the business.
- The way cloud security is delivered will depend on the individual cloud provider or the cloud security solutions in place. However, implementation of cloud security processes should be a joint responsibility between the business owner and solution provider.

Why is Cloud Security important?

To Achieve CIA

- Confidentiality
- Integrity
- Availability

Unit 5: Cloud security

Cloud Security Benefits:

- **Centralized Security**: Cloud-based business networks consist of numerous devices and endpoints that can be difficult to manage. Managing these entities centrally **enhances traffic analysis** and **web filtering**, streamlines the monitoring of network events and results in fewer software and policy updates. Disaster recovery plans can also be implemented and actioned easily when they are managed in one place.
- **Reduced Costs**: It eliminates the need to invest in dedicated hardware. Not only does this reduce capital expenditure, but it also reduces administrative overheads and delivers proactive security features that offer protection 24/7 with little or no human intervention.
- **Reduced Administration**: Pre-configured security configurations and almost constant security updates. These tasks can have a massive drain on resources.
- **Reliability: U**sers can safely access data and applications within the cloud no matter where they are or what device they are using.

Cloud Security Issues

- Specific security problems and risks in cloud environments.
- Existing threats and vulnerabilities .

  - **Data Breaches** – Hackers or mistakes can expose sensitive data like personal info and financial details.
  - **Weak Access Control** – Poor password management and access rules allow hackers to steal or change data.

- **Insecure APIs** – Weak security in cloud interfaces lets attackers break in and exploit services.
- **Software Vulnerabilities** – Bugs in cloud systems let hackers steal data or disrupt services.
- **Account Hijacking** – If attackers steal login details, they can misuse cloud services.
- **Insider Threats** – Employees or admins may leak or misuse company data.
- **Advanced Attacks (APTs)** – Hidden cyber threats slowly steal data without being noticed.
- **Data Loss** – Accidents or disasters can delete cloud data permanently without backups.
- **Lack of Planning** – Poor cloud security planning can expose companies to cyber risks.
- **Misuse of Cloud Services** – Criminals can abuse weak cloud security for fraud or cyberattacks.
- **Denial of Service(Dos)**
- **Shared Technology Vulnerability**
-

Cloud Security Challenges

- Difficulties faced in securing cloud systems effectively.
- Problems in implementing security solutions (e.g., compliance, misconfigurations).

Unit 5: Cloud security

- Challenges are the gap between theory and practice. It’s great to know you need a cloud security strategy. But where do you start? How do you tackle cultural change? What are the daily practical steps to make it happen?

Some security challenges are

1. Lack of Cloud Security and Skills
2. Identity and Access Management
3. Shadow IT
4. Cloud Compliance
5. Data Encryption

1. Lack of cloud security strategy and skills

- Traditional data center security models are not suitable for the cloud. Administrators must learn new strategies and skills specific to cloud computing.
- Cloud may give organizations agility, but it can also open up vulnerabilities for organizations that lack the internal knowledge and skills to understand security challenges in the cloud effectively. Poor planning can manifest itself in misunderstanding the implications of the shared responsibility model, which lays out the security duties of the cloud provider and the user. This misunderstanding could lead to the exploitation of unintentional security holes.

2. Identity and access management

- Identity and Access Management (IAM) is essential. While this may seem obvious, the challenge lies in the details.
- It's a difficult task to create the necessary roles and permissions for an enterprise of thousands of employees. There are three steps to a holistic IAM strategy: role design, privileged access management, and implementation.
- Next, a strategy for privileged access management (PAM) outlines which roles require more protection due to their privileges. Tightly control who has access to privileged credentials and rotate them regularly.
- Finally, it's time to implement the designed roles within the cloud provider's IAM service.

3. Shadow IT

- Shadow IT refers to the use of information technology systems, devices, software, or applications by individuals or departments within an organization without the approval or knowledge of the IT department

- Shadow IT creates security risks because it bypasses standard IT rules. Employees use cloud services without approval, making it hard to track and secure. For example, developers may set up cloud resources quickly, but these may have weak security, default passwords, or misconfigurations.

4. Cloud compliance

- Organizations must follow rules like PCI DSS and HIPAA to protect sensitive data, such as credit card details and medical records. To stay compliant, they restrict user access and control what users can do. Without proper access controls, it becomes hard to track and secure network access.

5. Data Encryption

- Implementing a cloud computing strategy means placing critical data in the hands of a third party, so ensuring the data remains secure both at rest (data residing on storage media) as well as when in transit.
- Data should always be encrypted, and only authorized people should manage the encryption keys. To keep cloud data private, the client should control and manage their own encryption keys.

Cloud Security Risks

You cannot completely eliminate risk; you can only manage it. Knowing common risks ahead of time will prepare you to deal with them within your environment.

Some Cloud security risks are:

1. The effect on a company's return on investment(ROI)
2. Lack of control over performance
3. Insufficient Data Encryption
4. Theft or loss of intellectual property

5. Compliance violations
6. Malware attacks

## other from security issues

Managing Cloud Security

The following steps will aid business decision-makers and enterprise IT managers to analyze cloud security of company data: -

1. **Ensure governance and compliance is effective**
    - Establish privacy and compliance policies to protect their assets.
    - Create a framework of governance that establishes authority and a chain of responsibility in the organization.
    - A well-defined set of policies clearly describes the responsibilities and roles of each employee. It should also define how they interact and pass information.
2. **Auditing**
    - Every system in an organization requires a regular audit that firms keep their IT systems in check in case of malware and phishing attacks.
    - An IT system audit must also check the compliance of IT system vendors and data in the cloud servers.

3. **Manage identities, people and roles**
    - Employees from the cloud service provider will inevitably have access to our firm’s applications and data.

- Ensure that the cloud service provider has sufficient policies to govern who has access to sensitive data and software.
- Provide the customer the privilege to manage and assign authorization for the users.

4. **Enforcing privacy policies**
    - Privacy and protection of personal and sensitive information are crucial to any organization's success.
    - Personal data held by an organization could face bugs or security negligence.
    - If a provider is not offering adequate security measures, the firm should consider seeking a different cloud service provider or not uploading sensitive information on the cloud.

5. **Assess security vulnerabilities for cloud applications**
    - Assessing security vulnerabilities for cloud applications involves identifying and evaluating potential risks that could compromise the integrity, confidentiality, and availability of the application and its data.

6. **Cloud networks security**
    - Audits of the cloud networks should be able to establish malicious traffic that can be detected and blocked. However, the cloud service providers have no way of knowing which network traffic its users plan to send or receive.
    - Organizations must then work together with their service providers to establish safety measures.

7. **Evaluating physical infrastructure and security controls**

Unit 5: Cloud security

- The security of the physical infrastructure of an IT system determines its vulnerability at the onset of a malicious attack.
- The provider must assure its users that appropriate measures are in place. Facilities and infrastructure should be stored in secure locations and backed up to protect against external threats.

- It is becoming more critical to maintain privacy and security with more data and software being migrated to the cloud.
- The IT groups must consider the cloud security risks and implement solutions to ensure the security of client data stored and processed in the cloud.

Unit 5: Cloud security

Software-as-a-Service (SaaS) Security

What is SaaS Security?

SaaS Security focuses on protecting user privacy and corporate data in cloud applications that users subscribe to. These applications store sensitive information and are accessible from almost any device, which can increase the risk of privacy breaches.

Software-as-a-Service (SaaS) Security Issues

- Future cloud computing models will likely combine SaaS, utility computing, and Web 2.0 technologies to better meet customer needs.
- The shift to cloud computing is introducing new technologies, business models, and security challenges that need to be addressed.
- SaaS will continue to be the leading cloud service model, requiring strong security measures and oversight.
- Companies or users must carefully check vendors' data security policies before using their services to ensure they don't risk losing or being unable to access their data.

Seven security issues which one should discuss with a cloud-computing vendor:

1. Privileged user access—Inquire about who has specialized access to data, and about the hiring and management of such administrators.

2. Regulatory compliance—Make sure that the vendor is willing to undergo external audits and/or security certifications.

3. Data location—Does the provider allow for any control over the location of data?

4. Data segregation—Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals.

5. Recovery—Find out what will happen to data in the case of a disaster. Do they offer complete restoration? If so, how long would that take?

6. Investigative support—Does the vendor have the ability to investigate any inappropriate or illegal activity?

7. Long-term viability—What will happen to data if the company goes out of business? How will data be returned, and in what format?

To address the security issues listed above along with others mentioned earlier in the topic, SaaS providers will need to incorporate and enhance security practices used by the managed service providers and develop new ones as the cloud computing environment evolves

The Baseline Security Practices for the SaaS Environment

Key aspects of SaaS security include:

1. Data Encryption: Encrypting sensitive data both at rest (stored data) and in transit (data being transferred) ensures that even if data is intercepted, it remains unreadable.
2. Access Control: Strong authentication and authorization mechanisms, including multi-factor authentication (MFA), ensure only authorized users can access the application and its data.

3. Data Privacy: Protecting user privacy by ensuring that only authorized individuals have access to personal or sensitive data, and that data is handled according to privacy regulations (e.g., GDPR, HIPAA).
4. Vendor Security Practices: SaaS providers should have robust security protocols, including regular security audits, vulnerability assessments, and secure coding practices. Companies should also evaluate the security measures of SaaS vendors before adopting their services.
5. Compliance: SaaS applications must comply with relevant regulations and standards (e.g., GDPR, PCI DSS) to ensure data protection and avoid legal penalties.
6. Incident Response and Monitoring: Continuous monitoring of SaaS applications for unusual activity, as well as having an effective incident response plan, ensures quick action in case of a security breach.
7. Backup and Recovery: Implementing a reliable backup and disaster recovery strategy helps ensure that data can be restored in case of a breach, loss, or system failure.
8. Shared Responsibility Model: In a SaaS environment, security responsibilities are typically shared between the service provider and the customer. Understanding and managing this shared responsibility is crucial for protecting the application and data.

Unit 5: Cloud security

Security Monitoring and Incident Response

Cloud security monitoring is a part of cloud security management. It works as various automations, continuously scanning virtual and physical servers looking for threats and vulnerabilities. This assures network administrators that the security is under control and the sensitive data is kept safe.

In most cases, cloud service providers offer built-in cloud security monitoring tools as part of the package. The cloud hosting infrastructure often already comes equipped with monitoring tools. In cases when it does not, or the client wants additional reassurance, there's always a possibility to turn to third-party providers.

The tools aggregate data from various sources like servers, instances, and containers. It's up to the cloud monitoring solution to correlate and analyze the collected data. This is where Security Information and Event Management (SIEM) systems become crucial.

Monitoring actions include:

- Identifying the source of the breach.
- Implementing security measures to prevent similar incidents from occurring in the future.
- Notifying affected parties and providing them with guidance on protecting their data.
- Assessing the extent of the damage and determining the necessary steps to recover.
- Taking legal action against the responsible parties, if applicable.

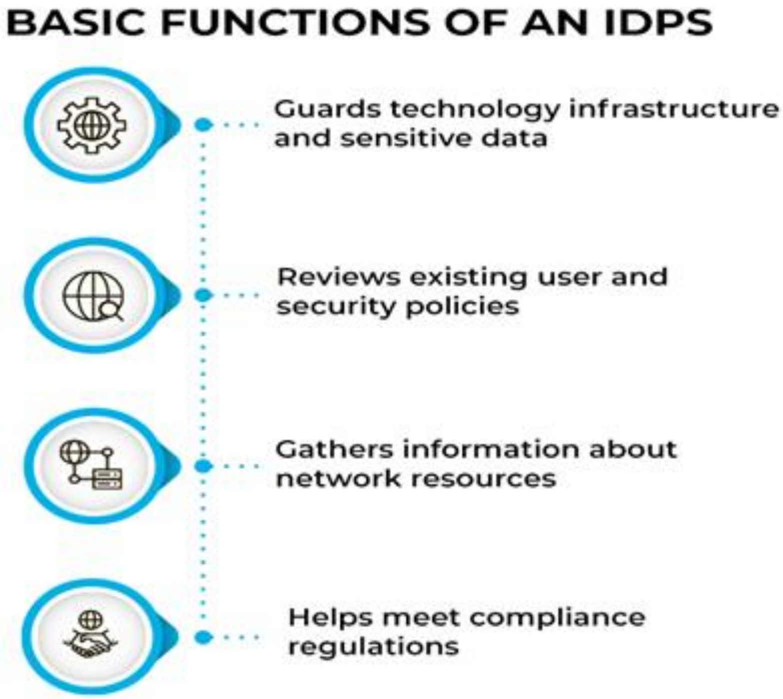
- Developing a plan to restore data and systems to their pre-breach state.

Incident Response

- Incident response is an organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident).
  - The goal is to handle the situation in a way that limits damage and reduces recovery time and costs. An incident response plan includes a policy that defines, in specific terms, what constitutes an incident and provides a step-by-step process that should be followed when an incident occurs. An organization's incident response is conducted by the computer incident response team, a carefully selected group that, in addition to security and general IT staff, may include representatives from legal, human resources, and public relations departments.

Intrusion Detection and Prevention System

An intrusion detection and prevention system (IDPS) monitors a network for possible threats to alert the administrator, thereby preventing potential attacks.


BASIC FUNCTIONS OF AN IDPS
Guards technology infrastructure and sensitive data
Reviews existing user and security policies
Gathers information about network resources
Helps meet compliance regulations

Security Architecture Design

- Security architecture is a key part of a product or system's overall design, providing guidance during development.
- A security framework should include processes like authentication, access control, data protection, security management, and compliance.
- A security architecture document should outline security and privacy principles to support business goals.
- Proper documentation is needed for asset protection, system access, network security, application development, business continuity, and compliance.
- A well-defined security architecture helps engineers and IT teams design, build, and test secure applications and systems.

Unit 5: Cloud security

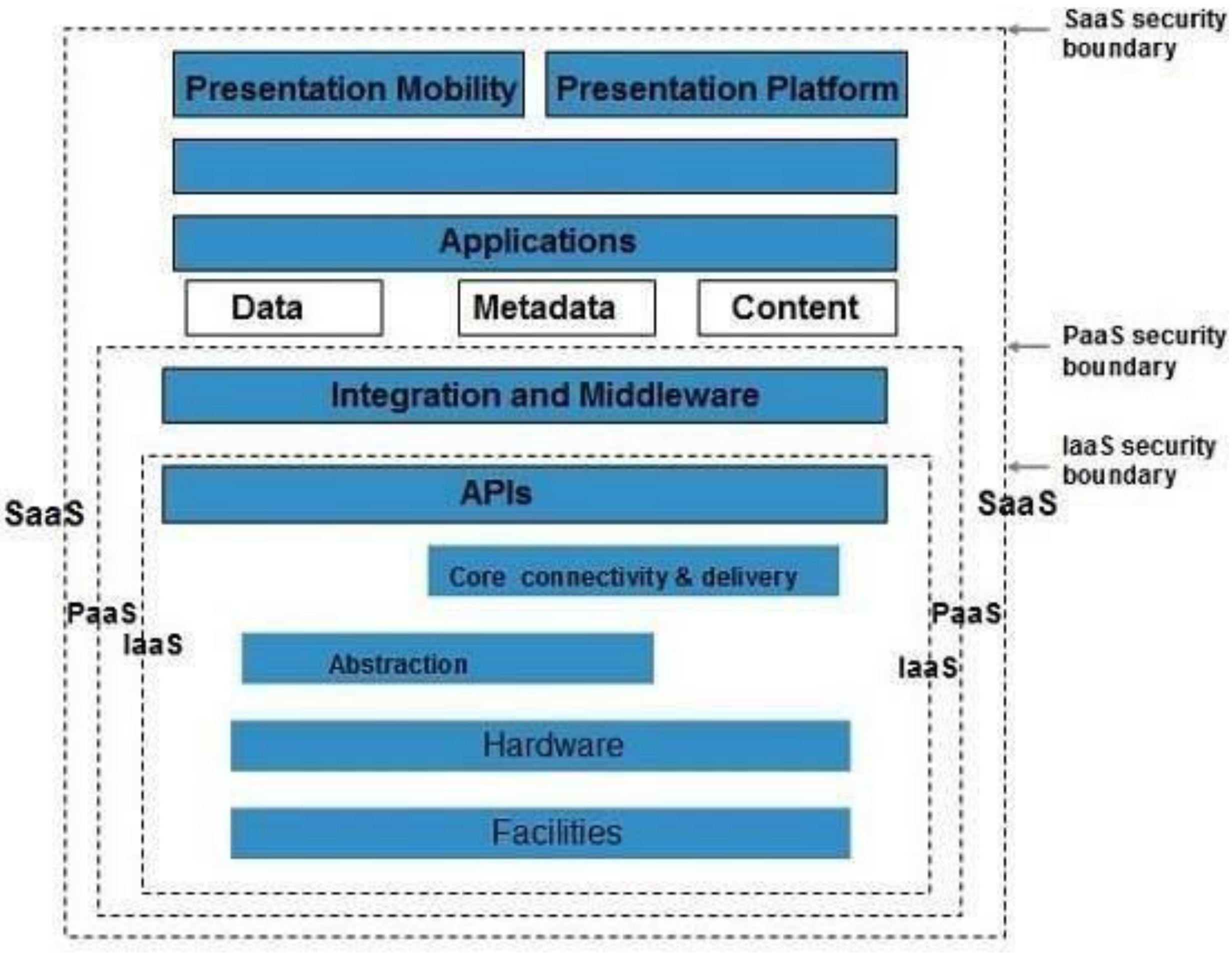
When designing cloud security architecture, the following key elements should be included:

1. Security at Every Layer: Ensure protection at all levels of the system.
2. Centralized Management: Manage all components from one place.
3. Redundancy & Resilience: Design the system to be fault-tolerant and reliable.
4. Elasticity & Scalability: Allow the system to grow or shrink based on needs.
5. Proper Storage: Choose the right storage solutions for your deployment.
6. Alerts & Notifications: Set up systems to notify you of security issues.
7. Centralization, Standardization & Automation: Centralize, standardize, and automate processes for efficiency and consistency.

Security Boundaries

- A particular service model defines the boundary between the responsibilities of service provider and customer.

- **Cloud Security Alliance (CSA)** stack model defines the boundaries between each service model and shows how different functional units relate to each other.



CSA Model:

- IaaS is the most basic service, followed by PaaS and SaaS as the next levels.
- As you move up, each service inherits the capabilities and security concerns of the lower-level service.
- IaaS provides the infrastructure, PaaS provides the platform for development, and SaaS provides the operating environment.

- IaaS has the least integrated functionality and security, while SaaS has the most.
- This model shows where the cloud provider’s responsibilities end and the customer’s responsibilities begin.
- Any security measures below this boundary must be implemented and maintained by the customer.

When designing a cloud architecture, it is essential to consider the security implications. Security measures must be taken to protect data, applications, and systems from unauthorized access and malicious activity.

###In summary

To ensure the security of a cloud architecture, it is essential to:

- Implement authentication and authorization protocols to control access to resources.
- Utilize encryption to protect data in transit and at rest.
- Monitor and log activities to detect suspicious behavior.
- Deploy security patches and updates regularly.
- Establish a secure backup and recovery plan.
- Utilize firewalls and other security tools to protect against external threats.
- Educate users on security best practices.

Unit 5: Cloud security

Data and application Security

Data Privacy and Security in Cloud Computing

Cloud computing has changed how organizations handle IT, making them more flexible, cost-efficient, and able to offer new services. It can be implemented in different ways and combined with other technologies.

Keeping control over data is crucial for cloud success. In the past, organizations stored data on their own servers, but now, with virtualization and cloud services, data is often stored on external infrastructure managed by third parties.

Some of the points to keep data private and secure in cloud infrastructure are as below:

1. Avoid storing sensitive information in the cloud.
2. Read the user agreement to find out how the cloud service storage works.
3. Password sensitivity
4. Encrypt the data
5. Use Encrypted cloud services

Unit 5: Cloud security

Who is responsible for Cloud Data Security?

To ensure sensitive information remains secure, it is crucial to understand the shared responsibility of cloud data security between Cloud Service Providers (CSPs) and customers.

Cloud Service Provider (CSP) Responsibilities

CSPs play a vital role in maintaining the overall infrastructure supporting their services. Their primary responsibilities include:

- **Physical security:** Ensuring data centers housing servers and other hardware components are protected from unauthorized access, theft, or damage.
- **Network security:** Implementing measures like firewalls and intrusion detection systems to defend against external threats targeting network resources.
- **Patching vulnerabilities:** Regularly updating software applications with patches provided by vendors to address known vulnerabilities.
- **Data encryption at rest:** Encrypting stored data using industry-standard algorithms like AES-256 to prevent unauthorized access when it’s not being actively used or processed by an application.

Customer Responsibilities

The user or organization using cloud services also has several key responsibilities related to ensuring proper protection of their sensitive information within these environments. These include:

- **Data classification:** Determining which types of information should be considered confidential or restricted based on factors such as legal requirements, business needs, and risk assessments.
- **Data encryption in transit:** Ensuring that any transmission of sensitive information over networks is encrypted using protocols like TLS or HTTPS to prevent unauthorized interception.
- **Identity and access management (IAM):** Establishing strong authentication and authorization controls for users accessing cloud resources, such as multi-factor authentication (MFA) and role-based access control (RBAC).
- **Data loss prevention:** Implementing policies and tools designed to detect potential data breaches in real-time, such as monitoring user activity for unusual patterns of behavior that could indicate a security incident.
- **Secure configuration:** Ensuring cloud systems and applications are securely configured, for example by configuring access permissions and ensuring only authorized administrators have access to sensitive functions.

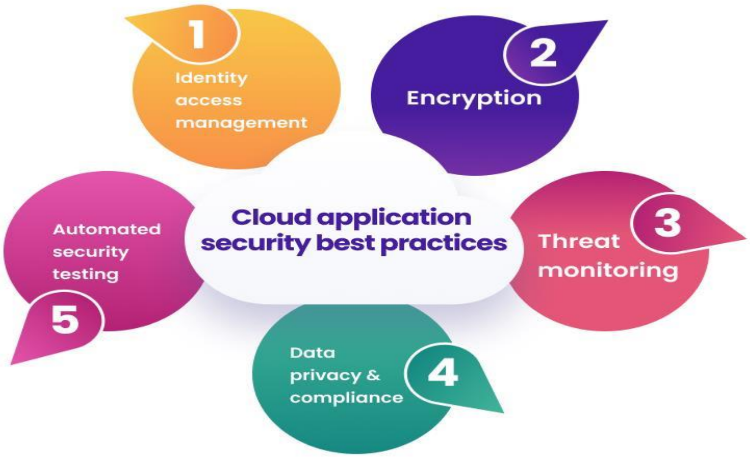
Application Security

- Application security is crucial for the success of a SaaS company.
- It involves defining security requirements, reviewing test results, and following secure coding practices.
- Security and development teams work together on security processes, training, testing tools, and guidelines.

- While engineers focus on application security and infrastructure, the security team provides key security requirements.
- External testers conduct penetration tests and source code reviews to ensure security and reassure customers.

Some of the things that we should consider while moving to cloud application are:

a. Risks associated with cloud application
b. The fact that someone is managing and controlling our critical application
c. The perimeter of cloud is different and multitenant
d. Application should be protected with industry standard firewall and security products e. Insecure Interfaces and Application Program Interface (API's)
e. Denial of Service (DOS) attack


1
Identity access management
2
Encryption
Cloud application security best practices
3
Threat monitoring
Automated security testing
5
Data privacy & compliance
4

Unit 5: Cloud security

1. **Identity Access Management:** IAM ensures every user is authenticated and can only access authorized data and application functionality. A holistic approach to IAM can protect cloud applications and improve the overall security posture of an organization.
2. **Encryption:** Implementing encryption in the right areas optimizes application performance while protecting sensitive data. In general, the three types of data encryption to consider are encryption in transit, encryption at rest, and encryption in use.
   a. Encryption in transit protects data as it's transmitted between cloud systems or to end-users. This includes encrypting communication between two services, whether they're internal or external, so that data cannot be intercepted by unauthorized third parties.
   b. Encryption at rest ensures data cannot be read by unauthorized users while it is stored in the cloud. This can include multiple layers of encryption at the hardware, file, and database levels to fully protect sensitive application data from data breaches.
   c. Encryption in use is aimed at protecting data that is currently being processed, which is often the most vulnerable data state. Keeping data in use safe involves limiting access beforehand using IAM, role-based access control, digital rights protection, and more.
3. **Threat monitoring:** After applications are deployed to the cloud, it's crucial to continuously monitor for cyber threats in real-time. Since the application security threat landscape is constantly evolving, leveraging threat intelligence data is crucial for staying ahead of malicious actors. This enables development

teams to find and remediate cloud application security threats before they impact end-users.

4. **Data privacy & compliance:** Along with application security, data privacy, and compliance are crucial for protecting end-users of cloud native applications. It includes careful vetting of open source components, data encryption, access controls, and other cloud security controls can also help protect the privacy of application users.
5. **Automated security testing:** A key part of DevSecOps is integrating automated security testing directly into the development process. By automatically scanning for vulnerabilities throughout the continuous integration and continuous delivery (CI/CD) process, development teams can ensure every new software build is secure before deploying to the cloud. This includes not only the code and open source libraries that applications rely on, but the container images and infrastructure configurations they're using for cloud deployments.

Unit 5: Cloud security

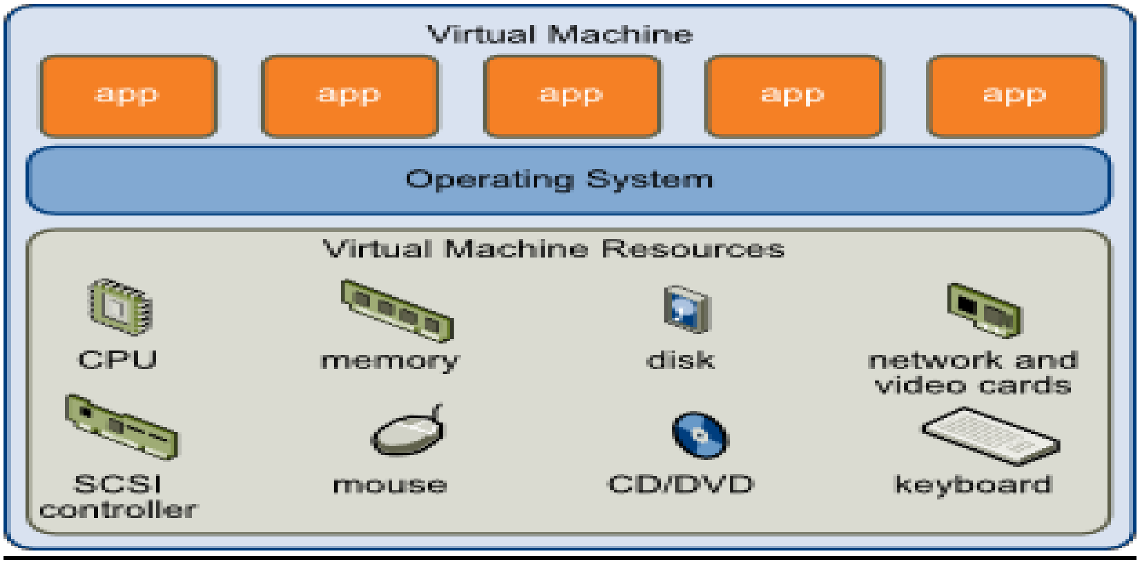
Virtual Machine Security

Virtualized Security

It is also known as “security virtualization,” describes security solutions that are software-based and created to operate in a virtualized IT environment. This is distinct from conventional hardware-based network security, which is static and is supported by equipment like conventional switches, routers, and firewalls.

Virtualized security is flexible and adaptive, in contrast to hardware-based security. It can be deployed anywhere on the network and is frequently cloud-based so it is not bound to a specific device.

Virtual Machine



- Virtual machines are the containers in which applications and guest operating systems run.

- By design, all VMware virtual machines are isolated from one another. This isolation enables multiple virtual machines to run securely while sharing hardware and ensures both their ability to access hardware and their uninterrupted performance.
- Although virtual machines share physical resources such as CPU, memory, and I/O devices, a guest operating system on an individual virtual machine cannot detect any device other than the virtual devices made available to it.

Virtual Machine Isolation

- In cloud computing, physical servers are divided into multiple virtual machines (VMs) running on a shared infrastructure.
- Security teams apply traditional data center security measures to protect VMs and guide users on migrating them safely to the cloud.
- Security tools like **firewalls, intrusion detection, integrity monitoring, and log inspection** can be installed as software on VMs to enhance protection, ensure compliance, and secure cloud-based resources.
- A **bidirectional stateful firewall** should be used to manage security policies, ensuring VMs remain isolated and aware of their network location.
- Integrity monitoring and log inspection software must be set up at the VM level to track security threats.
- Network traffic between VMs on the same physical server must be monitored to prevent undetected cyberattacks.

- **Network virtualization** should provide a suitable network interface for each VM, where switching and routing are efficiently managed by the network hardware.

Legal issues and Aspects

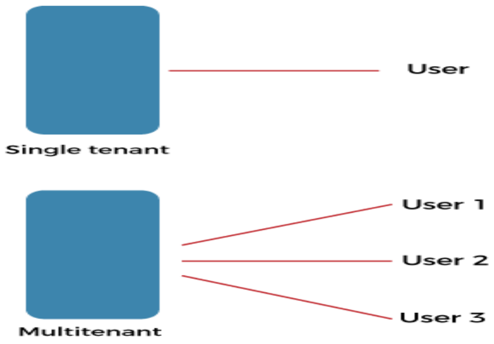
Legal issues and aspects in cloud computing refer to the legal challenges and concerns that arise when using cloud services for storing, processing, and managing data. Some key legal issues include:

1. **Data Privacy and Security**: Cloud providers must comply with laws that protect personal and sensitive data. Users need to ensure that the cloud services they use follow strict security protocols to prevent unauthorized access or data breaches.
2. **Data Ownership**: Determining who owns the data stored in the cloud can be complex. Often, users retain ownership, but the terms of service from the cloud provider may grant them certain rights over the data.
3. **Compliance and Regulations**: Different regions have different laws, such as the GDPR in Europe or HIPAA in the United States, which regulate how personal data is handled. Businesses using cloud services must ensure they comply with these regulations.
4. **Contractual Agreements**: Cloud service providers and users must have clear contracts that define responsibilities, liabilities, and service-level agreements (SLAs). These agreements should address issues like uptime, performance, and data protection.

5. **Cross-Border Data Transfer**: Cloud computing often involves storing data in multiple locations worldwide. This raises legal questions about where data is stored and whether it complies with local laws, particularly regarding privacy and data protection.
6. **Intellectual Property**: Cloud users and providers must address intellectual property concerns, especially when sharing or hosting software or other proprietary content on the cloud.

Multitenancy in Cloud computing

- Multitenancy is a type of software architecture where a single software instance can serve multiple distinct user groups. It means that multiple customers of cloud vendors are using the same computing resources. As they are sharing the same computing resources but the data of each Cloud customer is kept separate and secure. It is a very important concept of Cloud Computing.
- Multitenancy is also a shared host where the same resources are divided among different customers in cloud computing.



Advantages of Multitenancy:

- The use of Available resources is maximized by sharing resources.
- Customer's Cost of Physical Hardware System is reduced, and it reduces the usage of physical devices and thus power consumption and cooling cost savings.
- Save Vendor's cost as it becomes difficult for a cloud vendor to provide separate Physical Services to each individual.

Disadvantages of Multitenancy:

- Data is stored in third-party services, which reduces our data security and puts it into vulnerable conditions.

- Unauthorized access will cause damage to data.

Assignments

1. Why it is important to assess the concept of recovery time objective in disaster recovery? How disaster recovery is done in cloud infrastructure?
2. Why intrusion detection systems are implemented in cloud networks? How anamoly based intrusion detection system differs from signature based?