UNIT-III

Cloud Security Aspects

Cloud security fundamentals

Vulnerability assessment

- Vulnerability scanning or vulnerability assessment is a systematic process of finding **security loopholes** in any system addressing the potential vulnerabilities.
- The purpose of vulnerability assessments is to **prevent the possibility of unauthorized access to systems**.
- Vulnerability testing preserves the **confidentiality**, **integrity**, **and availability** of the system.
- The system refers to any **computers, networks, network devices, software, web application, cloud computing**, etc.

Types of Vulnerability Scanners

- Vulnerability scanners have their ways of doing jobs.
- We can classify the vulnerability scanners into four types based on how they operate.

Cloud-Based Vulnerability Scanners

- Used to find vulnerabilities within cloud-based systems such as web applications, WordPress, and Joomla.

Host-Based Vulnerability Scanners

- Used to find vulnerabilities on a single host or system such as an **individual computer** or a network device like a **switch or core-router**.

Network-Based Vulnerability Scanners

- Used to find vulnerabilities in an internal network by scanning for open ports.
- Services running on open ports determined whether vulnerabilities exist or not with the help of the tool.

Database-Based Vulnerability Scanners

- Used to find vulnerabilities in database management systems.
- Databases are the backbone of any system storing sensitive information.
- Vulnerability scanning is performed on database systems to prevent attacks like **SQL Injection**.

Vulnerability assessment tool for cloud

- Vulnerability assessment tools were devised to **detect security threats** of the system causing potential threats to the applications.
- These include web application scanners that are tested, and the gauge is known to attack patterns through simulation.
- **Protocol scanners** search and scan protocols, ports, and network services.

- The **goal** of the vulnerability assessment tool is to **prevent unsanctioned access to systems.**
- Vulnerability assessment tools help in maintaining **confidentiality, integrity, and availability of the system.**

Vulnerability assessment tools

Intruder:

- A **paid tool** for vulnerability assessment designed to assess **cloud-based storage**.
- Intruder software assesses the vulnerability instantly after it releases.
- An intruder has **automated scanning features** that persistently monitors for vulnerability, by providing **quality reports**.

Openscap:

- A structured assistance of tools that is useful in vulnerability **scanning, assessment, measurement, forming a security measure.**
- A community developed tool supporting **Linux platforms**.
- Openscap framework provides strength to the vulnerability assessment on **web applications, servers, databases, operating systems, networks, and virtual machines**.
- They also assess **risk** and **counteract threats**.

Open VAS:

- A robust vulnerability scanning tool supporting **large-scale** scans suited for organizations.
- This tool is beneficial in detecting vulnerabilities in the web application or web servers and **databases, operating systems, networks, and virtual machines.**
- Open VAS has **daily access** to updates widening the vulnerability detection coverage.
- It is useful in **risk assessment** recommending expedients for detecting vulnerabilities.

Nikto2:

- It is an **open-source** vulnerability scanning assessment software pivoting on **web application security**.
- Nikto2 can detect around **6700 malicious files** causing a threat to web servers disclosing obsolete servers.
- Nikto2 watches on server configuration issues by performing **web server scans within a short time**.
- Nikto2 does not have any expedients to vulnerabilities detected, and also **does not provide risk assessment features**.

Netsparker:

- A tool with web application vulnerability embedded with an automated **feature for detecting vulnerabilities**.
- This tool is proficient in assessing vulnerabilities in several **web-applications** within a specified time.

W3AF:

- An untethered and open-source tool also known as **web-application-attack and framework.**
- An **open-source assessment tool** for **web applications**.
- It forms a framework securing web applications by detecting and making use of the vulnerabilities.

Security and Privacy Issues in Cloud Computing

- Infrastructure Security
- Data Security and Storage
- Identity and Access Management (IAM)
- Privacy

The Network Level

- Ensuring confidentiality and integrity of your organization's data-in- transit to and from your public cloud provider
- Ensuring proper access control (authentication, authorization, and auditing) to whatever resources you are using at your public cloud provider
- Ensuring availability of the Internet-facing resources in a public cloud that are being used by your organization, or have been assigned to your organization by your public cloud providers
- Replacing the established model of network zones and tiers with domains

The Host Level

SaaS/PaaS

- Both the PaaS and SaaS platforms abstract and hide the host OS from end users
- Host security responsibilities are transferred to the CSP (Cloud Service Provider)
- You do not have to worry about protecting hosts
- However, as a customer, you still own the risk of managing information hosted in the cloud services.

Local Host Security

Are local host machines part of the cloud infrastructure?

- Outside the security perimeter
- While cloud consumers worry about the security on the cloud provider’s site, they may easily forget to harden their own machines.

The lack of security of local devices can

- Provide a way for malicious services on the cloud to attack local networks through these terminal devices
- Compromise the cloud and its resources for other users

With mobile devices, the threat may be even stronger

- Users misplace or have the device stolen from them
- Security mechanisms on handheld gadgets are often times insufficient compared to say, a desktop computer
- Provides a potential attacker an easy avenue into a cloud system.
- If a user relies mainly on a mobile device to access cloud data, the threat to availability is also increased as mobile devices malfunction or are lost

Devices that access the cloud should have

- Strong authentication mechanisms
- Tamper-resistant mechanisms
- Strong isolation between applications
- Methods to trust the OS
- Cryptographic functionality when traffic confidentiality is required

The Application Level

- DoS
- EDoS(Economic Denial of Sustainability)
- – An attack against the billing model that underlies the cost of providing a service with the goal of **bankrupting** the service itself.
- End user security
- Who is responsible for Web application security in the cloud?
- SaaS/PaaS/IaaS application security
- Customer-deployed application security

Data Security and Storage

Several aspects of data security, including:

Data-in-transit

- Confidentiality + integrity using secured protocol
- Confidentiality with non-secured protocol and **encryption**

Data-at-rest

- Generally, not encrypted , since data is mixed with other users' data
- Encryption if it is not associated with applications?

Why IAM(Identity and Access Management)?

- Organization's trust boundary will become dynamic and will move beyond the control and will extend into the service provider domain.
- Managing access for diverse user populations (employees, contractors, partners, etc.)

Increased demand for authentication

- personal, financial, medical data will now be hosted in the cloud
- S/W applications hosted in the cloud requires access control

Need for higher-assurance authentication

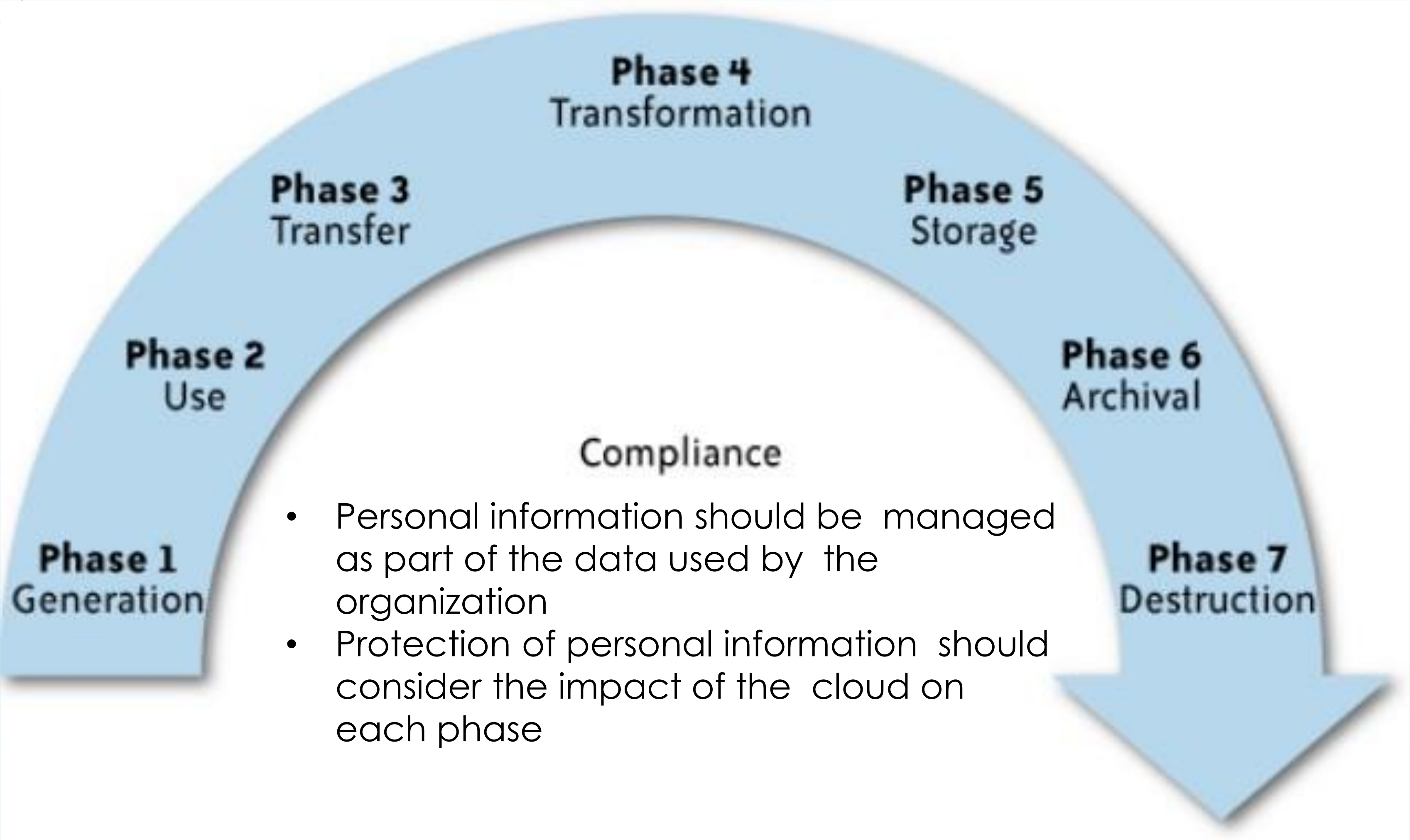
- authentication in the cloud may mean authentication outside F/W
- Limits of password authentication

Need for authentication from mobile devices

What is Privacy?

- The concept of privacy varies widely among (and sometimes within) countries and cultures.
- It is shaped by public expectations and legal interpretations.
- Privacy rights or obligations are related to the **collection**, **use**, **disclosure**, **storage, and destruction** of personal data.
- Privacy is about the **accountability** of organizations to data subjects, as well as the **transparency** to an organization’s practice around personal information.

What is the data life cycle?



Phase 1
Generation

Phase 2
Use

Phase 3
Transfer

Phase 4
Transformation

Phase 5
Storage

Phase 6
Archival

Phase 7
Destruction

Compliance

- Personal information should be managed as part of the data used by the organization
- Protection of personal information should consider the impact of the cloud on each phase

Trusted Cloud computing

- Cloud computing infrastructures enable companies to cut costs by outsourcing computations on-demand.
- However, clients of cloud computing services currently have no means of verifying the **confidentiality and integrity** of their data and computation.
- To address this problem the design of a trusted cloud computing platform (TCCP) was introduced.
- TCCP enables Infrastructure as a Service (IaaS) providers such as Amazon EC2 to provide a **closed box execution environment** that guarantees **confidential execution of guest virtual machines**.

- Moreover, it allows users to verify the IaaS provider and **determine whether or not the service is secure before they launch their virtual machines**.
- The goal of trusted cloud computing is to make the **computation of virtual machines confidential** which is deployed by the service provider.
- Customers can verify that the computation is confidential and prevent inspection of computation state at the service provider site
- It allows customers to verify that computation is secure and deployed with cooperation of the cloud provider

- Two components :
- **A trusted virtual machine monitor (TVMM)**
- **A trusted co-ordinator**.
- It helps to determine whether the service is secure before they launch their VM
- Hence, TCCP provides a closed box execution environment by extending the concept of trusted platform to an entire IAAS backend.

Secure Execution Environments and Communications

- Configuring computing platforms for secure execution is a complex task; and in many instances it is not performed properly because of the large number of parameters that are involved.
- This provides opportunities for **malware to exploit vulnerabilities**, such as **downloading code embedded in data** and having the code executed at a high privilege level.
- In cloud computing, the major burden of establishing a secure execution environment is **transferred from the client to the cloud provider**.
- However, protected data transfers must be established through **strong authentication mechanisms**, and the client must have practices in place to address the **privacy and confidentiality** of information that is exchanged with the cloud.

- In fact, the client's port to the cloud might provide an attack path if not properly provisioned with security measures.
- Therefore, the client needs assurance that computations and data exchanges are conducted in a secure environment.
- This assurance is affected by trust enabled by **cryptographic methods**.
- Also, research into areas such as compiler-based virtual machines promises a more secure execution environment for operating systems.

Microservice Architecture/Microservice

- We have been designing systems and applications for several years now and getting better at it day by day, but the tech world is all over microservices. Why?
- Because microservice architecture is a **service-oriented architecture** pattern that can **break up monolithic applications into smaller service units**.
- For business enhancement, many companies/industries have started using microservices.

Why are Microservices used?

- Microservices were used to overcome the challenges of monolithic.
- Monolithic architecture is similar to a big container wherein all the software components of an application are assembled and packaged.

Disadvantages of monolithic architecture:

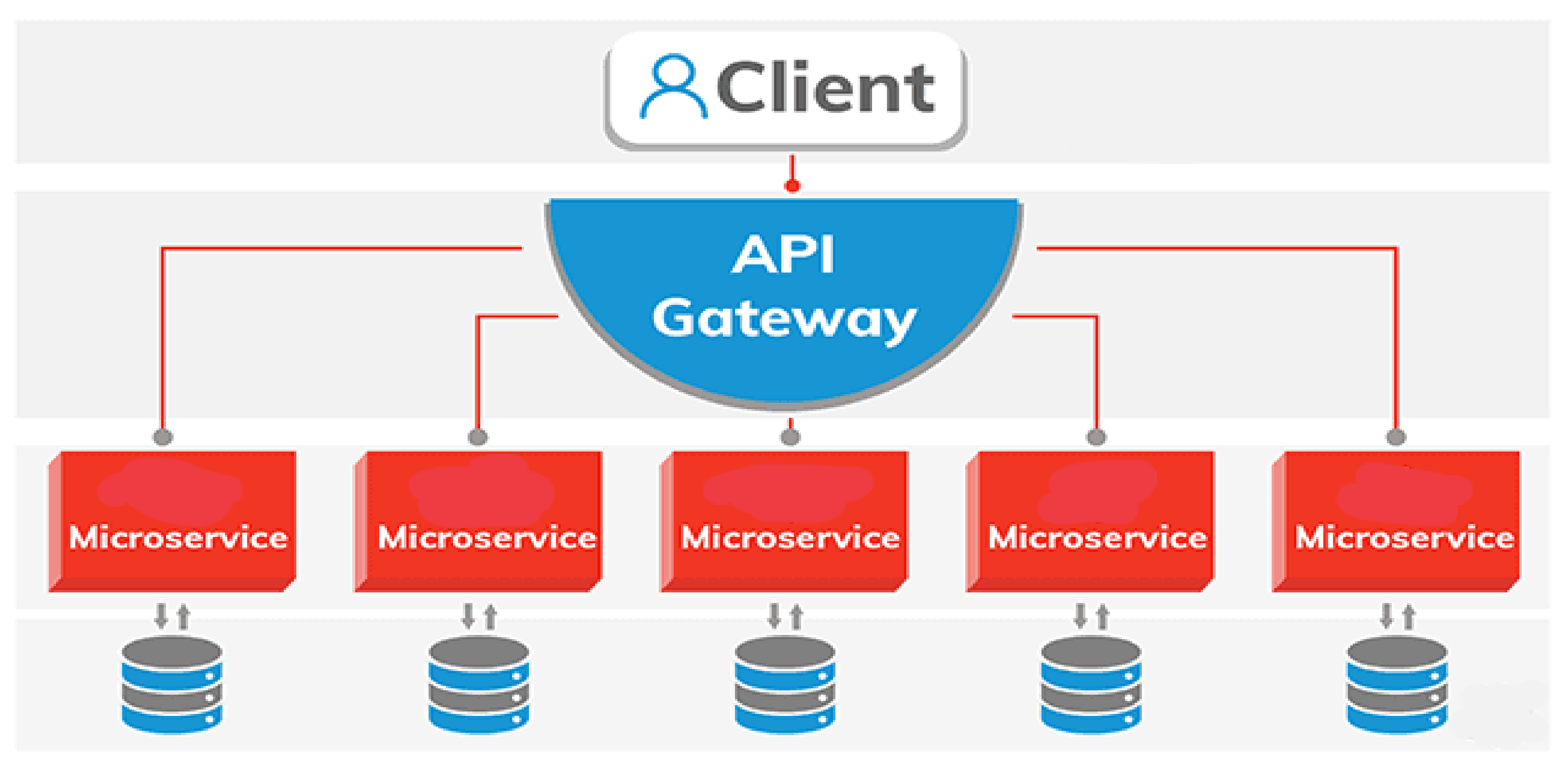
- **Inflexible:** Monolithic is inflexible, i.e. it cannot be built using **different technologies.**
- **Unreliable:** Monolithic is unreliable as it **depends on the entire system**, even if one component in the system does not work the entire system does not work.
- **Unscalable:** The application **needs to be updated every time**, which is unscalable.

- **Slow Development:** Every feature has to be **built one after the othe**r; this takes a lot of time.
- **Unfit for Complex Applications:** Monolithic architecture does not fit for complex applications due to its **slow development process, less flexibility**, etc.
- So these above disadvantages of monolithic architecture have led to the evolution of microservice.

What is Microservices?

- Microservices is also called **microservice architecture** which is an organizational approach to software development where software is composed of **small independent services** that communicate over APIs which are well-defined.
- Highly maintainable and testable
- Loosely coupled
- Independently deployable
- Organized around business capabilities
- Owned by a small team

How does Microservices Architecture work?



- The microservice architecture contains components depending on the business requirements.

- **API Gateway-** Clients need API Gateway as it is an entry point, which forwards the call to the specific services on the back end.
- Here API gateway helps in collecting the responses from different services and returns the response to the client.

- **Microservices-** As the name itself suggests that microservices are the services that help in dividing the service into small services that perform a certain business capability like user registration, current orders, or wish list.

- **Database-** Microservices can either share the same database or an independent database.
- **Inter-microservices communication-** REST or Messaging are the protocol to interact with each other.

Microservices Features

- **Decoupling:** Microservices systems are largely decoupled from within which can be **easily built, altered, and scaled**.
- **Componentization:** Microservices can be easily replaced and upgraded as independent components.
- **Business Capabilities:** Microservices focus on a single capability.
- **Autonomy:** Developers and teams can work independently without much dependency, thus increasing speed.
- **Continuous Delivery:** Microservices is here to update frequently, through systematic automation of software creation, testing, and approval.

- **Responsibility:** Microservices is responsible enough to focus on products.
- **Decentralized Governance:** Microservices do not have a standardized pattern that makes the developers have the freedom to choose **useful tools** to solve their problems.
- **Agility**: Microservice is known for **quick adaptation** of any new feature and even discard the feature.

Advantages of Microservices

- **Small in size:** Microservices is an implementation of SOA design pattern. Hence, it will be small in size and easy to maintain than any other monolithic application.
- **Focused:** Each microservice should be full stack in nature and designed to deliver only one business task which helps in focusing the deliverability.
- **Autonomous:** Microservice is an autonomous business unit of the entire application that makes the application more loosely coupled, which helps to reduce the maintenance cost.
- **Heterogeneity:** Microservice is a heterogeneous system that supports different technologies to communicate with each other, which helps the developers to use the correct technology at the correct place.

- **Ease of deployment:** Microservices is easy to deploy as the entire application is divided into small pieces of units; every component should be full stack in nature.

Disadvantages of Microservices

- **Distributed system:** We saw that microservice is heterogeneous, which requires a set of skilled professionals to support this big heterogeneous distributed software. Hence, this stands as the number one disadvantage of using microservice.
- **Cost:** Microservice requires different server spaces for different business tasks. Hence, it is costly!

Building Microservices architecture

- Microservices can be built on **different frameworks**. Here are the most popular ones:
- Spring Boot with Spring Cloud
- Vert.x
- Akka
- Quarkus
- Falcon
- Molecular

How to deploy microservices?

- Microservices can be deployed **on the cloud** to serve a lot of users from different locations.
- Microservices can be deployed **on containers,** to reduce the time taken to solve issues, time-to-market, etc…
- Microservices can be deployed **on PaaS** (Platform-as-a-Service).

What cloud provider to use?

- **AWS** cloud provider is suitable for almost any kind of technology.
- **An azure** cloud provider is suitable for the .NET stack, which mainly helps in data storage, and hosting solutions.
- **Google Cloud Platform** is suitable for AI & data analytics and has great support for Kubernetes.

Identity Management in Cloud Security

- Identity management (IM) is a term that refers to the information system being used within the enterprise.
- This represents the **systematic management of any single identity** and provides **authentication**, **privileges**, **authorization**, and **roles of the enterprise boundaries.**
- The primary purpose is to **upgrade security and productivity** by decreasing the total cost, repetitive tasks, and system downtime.
- Identity management in cloud computing covers all types of users who can work with defined devices under different circumstances.

- Various identity management (IM) services imply that wired and wireless user can support the directory integration.
- There are some additional **security services**, which are mentioned below:
- Access Control
- Password Manager
- Digital Identity Management
- Single Sign-On

Benefits of Identity Management in Cloud Security

- **Enhanced Network Abilities:** Identity management (IM) makes it simple in sharing the network capabilities with a complete grid of users who were connected with it.
- **Provides a secure collaboration:** SaaS protocol is designed and utilized as a hub for connecting with all virtual networks of suppliers, distributors, and trading partners.
- **Support On-demand improvement:** The problem that affects from churn protects organizations with a cloud-based solution. All experts can be able to provide 24*7 hours support and monitoring, whenever needed.

- **Increase Overall Productivity:** It is completely known that cloud-based services are configured and hosted by service providers. This may also get a little or zero hassle either for users or any other clients. As a result, many organizations can improve their overall productivity.
- **Centralized Management System:** Business users can be able to manage all services and programs at one place with the cloud-based services. Identity management can be done with one click on a single dashboard.

Virtualization Security

- Virtualization security is a broad concept that includes a number of different methods to evaluate, implement, monitor and manage security within a virtualization infrastructure / environment.

Typically, virtualization security may include processes such as:

- Implementation of **security controls and procedures** granularly at each virtual machine.

- Securing virtual machines, virtual network and other virtual appliance with attacks and vulnerabilities surfaced from the underlying physical device.

- Ensuring **control and authority over each virtual machine.**
- Creation and implementation of security policy across the infrastructure / environment

SECURITY CHALLENGES AND RISKS

User awareness:

- Cloud service users are the weakest point in any information security because cloud service providers do not check the surrounding of their customers. Suspicious user accounts can give attackers an opportunity to do any malicious work without being identified

Insecure APIs:

- A cloud-computing provider provides infrastructure, software, and platform services to the users and enables them to access the services through their interfaces. They designed their interfaces via the published application programming interfaces.
- APIs pose a variety of security issues such as improper authorizations, weak credentials, and clear-text during transmission may affect the availability and the security of the cloud services.

Lack of security policies:

- The organization defines security policies to determine how to protect its assets from any potential threats and how to deal with these situations when they occur.
- The security policies of the cloud service provider may be inadequate or incompatible with the security requirements of an organization.
- Lack of security policies may pose some vulnerabilities that lead to the insecure environment of VMs.

Incorrect VM isolation:

- The hypervisor is responsible for ensuring isolation between different VMs.
- The isolation between VMs prevents the VM from gets access to others' virtual disks, applications, or memory on the same host.
- Furthermore, isolation of VM limits the scope of the attack. It makes access resources, and sensitive data on the physical machine complicated.