UNIT 4

Cloud Security

As security is a major concern in cloud implementation, so an organization have to plan for security based on some factors like below represents the three main factors on which planning of cloud security depends.

- Resources that can be moved to the cloud and test its sensitivity risk are picked.
- The type of cloud is to be considered.
- The risk in the deployment of the cloud depends on the types of cloud and service models.

Types of Cloud Computing Security Controls :

There are 4 types of cloud computing security controls i.e.

1. Deterrent Controls : Deterrent controls are designed to block nefarious attacks on a cloud system. These come in handy when there are insider attackers.
2. Preventive Controls : Preventive controls make the system resilient to attacks by eliminating vulnerabilities in it.
3. Detective Controls : It identifies and reacts to security threats and control. Some examples of detective control software are Intrusion detection software and network security monitoring tools.
4. Corrective Controls : In the event of a security attack these controls are activated. They limit the damage caused by the attack.

Importance of cloud security :

For the organizations making their transition to cloud, cloud security is an essential factor while choosing a cloud provider. The attacks are getting stronger day by day and so the security needs to keep up with it. For this purpose it is essential to pick a cloud provider who offers the best security and is customized with the organization's infrastructure. Cloud security has a lot of benefits –

1. Centralized security : Centralized security results in centralizing protection. As managing all the devices and endpoints is not an easy task cloud security helps in doing so. This results in enhancing traffic analysis and web filtering which means less policy and software updates.
2. Reduced costs : Investing in cloud computing and cloud security results in less expenditure in hardware and also less manpower in administration
3. Reduced Administration : It makes it easier to administer the organization and does not have manual security configuration and constant security updates.
4. Reliability : These are very reliable and the cloud can be accessed from anywhere with any device with proper authorization.

When we are thinking about cloud security it includes various types of security like access control for authorized access, network segmentation for maintaining isolated data, encryption for encoded data transfer, vulnerability check for patching vulnerable areas, security monitoring for keeping eye on various security attacks and disaster recovery for backup and recovery during data loss.

There are different types of security techniques which are implemented to make the cloud computing system more secure such as SSL (Secure Socket Layer) Encryption, Multi Tenancy based Access Control, Intrusion Detection System, firewalls, penetration testing, tokenization, VPN (Virtual Private Networks), and avoiding public internet connections and many more techniques.

But the thing is not so simple how we think, even implementation of number of security techniques there is always security issues are involved for the cloud system. As cloud system is managed and accessed over internet so a lot of challenges arises during maintaining a secure cloud. Some cloud security challenges are

1. Control over cloud data
2. Misconfiguration
3. Ever changing workload
4. Access Management
5. Disaster recovery

Vulnerabilty Assesment Tools in Cloud:

Vulnerability assessment tools play a crucial role in identifying and mitigating security risks in cloud environments. Here are some popular vulnerability assessment tools specifically designed for cloud environments:

Nessus:

- Description: Nessus is a widely used vulnerability scanner that can be employed to assess cloud environments. It supports various cloud platforms, including AWS and Azure.
- Features: Vulnerability scanning, configuration assessment, compliance checking.

Qualys Cloud Platform:

- Description: Qualys provides a cloud-based security and compliance platform that includes vulnerability management capabilities. It supports multiple cloud providers.
- Features: Asset discovery, vulnerability assessment, compliance checks.

OpenVAS:

- Description: OpenVAS (Open Vulnerability Assessment System) is an open-source vulnerability scanner that can be utilized for cloud environments. It is often used in conjunction with other tools for comprehensive security assessments.
- Features: Network scanning, vulnerability scanning, and management.

AWS Inspector:

- Description: Amazon Inspector is an AWS service designed to assess applications for vulnerabilities and compliance issues on the AWS platform.
- Features: Agent-based assessments, predefined rules packages, and integration with other AWS services.

Azure Security Center:

- Description: Azure Security Center is a native Microsoft Azure service that provides advanced threat protection across hybrid cloud workloads. It includes vulnerability assessment capabilities.
- Features: Continuous monitoring, threat detection, and vulnerability assessment.

Tenable.io:

- Description: Tenable.io is a cloud-based vulnerability management platform that supports various cloud environments, including AWS and Azure.
- Features: Asset tracking, vulnerability detection, and compliance checks.

Privacy and Security in Cloud

The rapid development of the cloud has led to more flexibility, cost-cutting, and scalability of products but also faces an enormous amount of privacy and security challenges. Since it is a relatively new concept and is evolving day by day, there are undiscovered security issues that creep up and need to be taken care of as soon as discovered. Here we discuss the top 7 privacy challenges encountered in cloud computing:

1. Data Confidentiality Issues

Confidentiality of the user's data is an important issue to be considered when externalizing and outsourcing extremely delicate and sensitive data to the cloud service provider. Personal data should be made unreachable to users who do not have proper authorization to access it and one way of making sure that confidentiality is by the usage of severe access control policies and regulations. The lack of trust between the users and cloud service providers or the cloud database service provider regarding the data is a major security concern and holds back a lot of people from using cloud services.

2. Data Loss Issues

Data loss or data theft is one of the major security challenges that the cloud providers face. If a cloud vendor has reported data loss or data theft of critical or sensitive material data in the past, more than sixty percent of the users would decline to use the cloud services provided by the vendor. Outages of the cloud services are very frequently visible even from firms such as Dropbox, Microsoft, Amazon, etc., which in turn results in an absence of trust in these services during a critical time. Also, it is quite easy for an attacker to gain access to multiple storage units even if a single one is compromised.

3. Geographical Data Storage Issues

Since the cloud infrastructure is distributed across different geographical locations spread throughout the world, it is often possible that the user's data is stored in a location that is out of the legal jurisdiction which leads to the user's concerns about the legal accessibility of local law enforcement and regulations on data that is stored out of their region. Moreover, the user fears that local laws can be violated due to the dynamic nature of the cloud makes it very difficult to delegate a specific server that is to be used for trans-border data transmission.

4. Multi-Tenancy Security Issues

Multi-tenancy is a paradigm that follows the concept of sharing computational resources, data storage, applications, and services among different tenants. This is then hosted by the same logical or physical platform at the cloud service provider's premises. While following this approach, the provider can maximize profits but puts the customer at a risk. Attackers can take undue advantage of the multi-residence opportunities and can launch various attacks against their co-tenants which can result in several privacy challenges.

5. Transparency Issues

In cloud computing security, transparency means the willingness of a cloud service provider to reveal different details and characteristics on its security preparedness. Some of these details compromise policies and regulations on security, privacy, and service level. In addition to the willingness and disposition, when calculating transparency, it is important to notice how reachable the security readiness data and information actually are. It will not matter the extent to which the security facts about an organization are at hand if they are not presented in an organized and easily understandable way for cloud service users and auditors, the transparency of the organization can then also be rated relatively small.

6. Hypervisor Related Issues

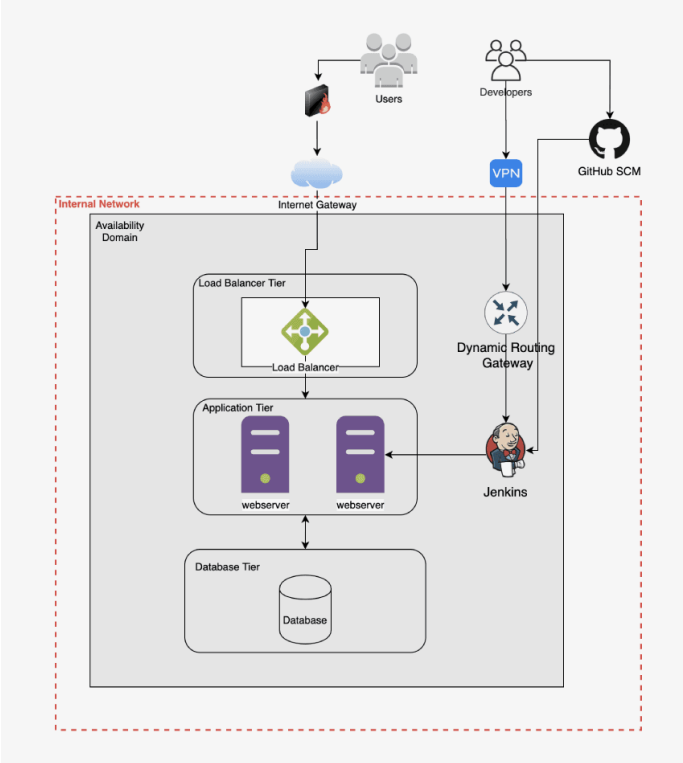
Virtualization means the logical abstraction of computing resources from physical restrictions and constraints. But this poses new challenges for factors like user authentication, accounting, and authorization. The hypervisor manages multiple Virtual Machines and therefore becomes the target of adversaries. Different from the physical devices that are independent of one another, Virtual Machines in the cloud usually reside in a single physical device that is managed by the same hypervisor.

7. Managerial Issues

There are not only technical aspects of cloud privacy challenges but also non-technical and managerial ones. Even on implementing a technical solution to a problem or a product and not managing it properly is eventually bound to introduce vulnerabilities. Some examples are lack of control, security and privacy management for virtualization, developing comprehensive service level agreements, going through cloud service vendors and user negotiations, etc.

Cloud Security Architecture

An improved security software's platform, services, technology, network, and best practices make up its security architecture, often referred to as a cloud computing security architecture. A cloud security architecture offers an oral and video model to describe how to customize and safeguard cloud-based activities, including things like identity management, techniques and limits to safeguard applications and data, methodologies for gaining and maintaining awareness into adherence, threat body position, and general stability, processes for incorporating security principles into the creation and operation of cloud services, regulations and democratic accountability.



A cloud computing security architecture comprises three fundamental features: confidentiality, integrity, and availability. An awareness of each feature will guide your attempts to design a better, safe cloud implementation.

1. Confidentiality

The ability to maintain information hidden and inaccessible from those who shouldn't have exposure to it, such as attackers or employees within an organization without the necessary access level, is known as confidentiality. Security and trustworthiness are additional examples of confidentiality, or when a company promises to handle consumer data confidently.

2. Integrity

Integrity means that the services and processes are precisely what you anticipate and behave exactly how you anticipate. Losses may result if a system or program has been exploited to generate an unknown, unanticipated, or false output.

3. Availability

The third capability, availability, is typically given the least thought by cloud architects. The term "availability" refers to DoS assaults. Perhaps an attacker can't access your data or alter it. However, if an attacker manages to render systems inaccessible to you or your clients, you will be unable to do operations that are crucial to running your company.

Elements of Cloud Security Architecture

Several crucial components should be present in a cloud computing security architecture:

1. Protection at Every Layer
2. Integrated Component Management
3. Redundant and robust design
4. Scalability and Elasticity
5. Storage That Is Appropriate for Deployments
6. Notifications & Alerts
7. Automation, Standardization, and Centralization

Principles of Cloud Security Architecture

The following essential tenets should serve as the foundation of any well-designed security architecture design in cloud computing:

- Identification: Understanding the people, resources, business climate, regulations, risks, security, and risk management techniques (business and supply chain) present inside your cloud environment.
- Security Controls: Describes the guidelines and regulations applied to individuals, information, and equipment to monitor the entire security posture.
- Security by Design: Outlines the security baseline's control roles, security configurations, and automation. Often standardized and repeatable for deployment across typical use cases, with security requirements, and in audit needs.

- Compliance: Ensures that standards and regulatory obligations are satisfied by integrating regulatory and industry standards into the architecture.
- Perimeter Security: Protects and encrypts traffic entering and leaving an organization's cloud-based resources, such as the points at which the corporate network connects to the public Internet.
- Segmentation: The design is divided into isolated component pieces to avoid lateral movement in the event of a breach. Frequently incorporates the "least privilege" concepts.
- User Identity and Access Management: Ensures awareness, control, and visibility over each user (including individuals, machines, and systems) who access business resources. Permits access, permissions, and protocol enforcement.
- Data encryption: ensures data is encrypted while it is in motion and moving between internal and outside cloud contact points to reduce the impact of breaches.
- Automation enables quick threat detection, security and configuration upgrades, and provisioning.
- Logging and monitoring: Ensures compliance, insight into processes, and understanding of dangers by monitoring (often automatically) all activity on connected devices and cloud-based services.
- Visibility: Incorporates tools and procedures to preserve visibility across a company's many cloud installations.
- Design Flexibility: Ensure the architecture is flexible enough to expand and incorporate new parts and solutions without compromising intrinsic security.

Identity Management

Identity and Access Management (IAM) is a combination of policies and technologies that allows organizations to identify users and provide the right form of access as and when required. There has been a burst in the market with new applications, and the requirement for an organization to use these applications has increased drastically. The services and resources you want to access can be specified in IAM. IAM doesn’t provide any replica or backup. IAM can be used for many purposes such as, if one want’s to control access of individual and group access for your AWS resources. With IAM policies, managing permissions to your workforce and systems to ensure least-privilege permissions becomes easier. The AWS IAM is a global service.

Components of Identity and Access Management (IAM)

1. Users
2. Roles
3. Groups
4. Policies

IAM Identities Classified As

- IAM Users
- IAM Groups
- IAM Roles

Root user

The root user will automatically be created and granted unrestricted rights. We can create an admin user with fewer powers to control the entire Amazon account.

IAM Users

We can utilize IAM users to access the AWS Console and their administrative permissions differ from those of the Root user and if we can keep track of their login information.

IAM Groups

A group is a collection of users, and a single person can be a member of several groups. With the aid of groups, we can manage permissions for many users quickly and efficiently.

IAM Roles

While policies cannot be directly given to any of the services accessible through the Amazon dashboard, IAM roles are similar to IAM users in that they may be assumed by anybody who requires them. By using roles, we can provide AWS Services access rights to other AWS Services.

IAM Policies

IAM Policies can manage access for AWS by attaching them to the IAM Identities or resources IAM policies defines permissions of AWS identities and AWS resources when a user or any resource makes a request to AWS will validate these policies and confirms whether the request to be allowed or to be denied. AWS policies are stored in the form of Jason format the number of policies to be attached to particular IAM identities depends upon no.of permissions required for one IAM identity. IAM identity can have multiple policies attached to them.

Use cases Identity and Access Management(IAM)

1. Resource Access Control: Identity and access management (IAM) will allows you to manage the permissions to the resources in the AWS cloud like users who can access particular serivce to which extent and also instead of mantaing the permissions individually you can manage the permissions to group of users at a time.
2. Managing permissions: For example you want to assign an permission to the user that he/her can only perform restart the instance task on AWS EC2 instance then you can do using AWS IAM.

3. Implemneting role-based access control(RBAC): Identity and Access Management(IAM) will helps you to manage the permissions based on roles Roles will helps to assign the the permissions to the resourcesw in the AWS like which resources can access the another resource according to the requirement.
4. Enabling single sign-on (SSO): Identity and Access Management will helps you to maintain the same password and user name which will reduce the effort of remembering the different password.

IAM Features

1. Shared Access to your Account: A team working on a project can easily share resources with the help of the shared access feature.
2. Free of cost: IAM feature of the AWS account is free to use & charges are added only when you access other Amazon web services using IAM users.
3. Have Centralized control over your AWS account: Any new creation of users, groups, or any form of cancellation that takes place in the AWS account is controlled by you, and you have control over what & how data can be accessed by the user.
4. Grant permission to the user: As the root account holds administrative rights, the user will be granted permission to access certain services by IAM.
5. Multifactor Authentication: Additional layer of security is implemented on your account by a third party, a six-digit number that you have to put along with your password when you log into your accounts.

Access Control In Cloud

Access control is a crucial aspect of cloud computing security, as it involves managing and regulating access to resources, data, and services in cloud environments. Effective access control ensures that only authorized users or systems can interact with specific resources, helping to prevent unauthorized access, data breaches, and other security incidents.

Automation Security

Automation is a key component of cloud computing, allowing organizations to streamline processes, enhance efficiency, and achieve scalability. However, the automation of tasks and workflows in the cloud introduces security considerations that need to be addressed to mitigate potential risks. Here are some important aspects to consider regarding automation security in cloud computing:

Infrastructure as Code (IaC) Security:

- Secure Coding Practices: Apply secure coding practices when developing Infrastructure as Code (IaC) scripts to create and manage cloud resources. This helps prevent vulnerabilities in the code.
- Code Reviews and Testing: Conduct regular code reviews and automated testing of IaC scripts to identify and remediate security issues before deployment.

Configuration Management:

- Baseline Security Configurations: Establish baseline security configurations for cloud resources to ensure that automated provisioning adheres to security best practices.
- Continuous Monitoring: Implement continuous monitoring to detect and remediate any deviations from the established security baselines.

Secrets Management:

- Secure Storage: Ensure that sensitive information such as API keys, passwords, and encryption keys are securely stored and managed. Avoid hardcoding secrets in scripts or configuration files.
- Use of Key Vaults: Leverage key vaults or secret management services provided by the cloud platform to securely store and retrieve secrets.

Access Control and Identity Management:

- Least Privilege Principle: Apply the principle of least privilege to automation scripts and tools. Ensure that they only have the minimum permissions required to perform their tasks.
- Identity and Access Management (IAM): Integrate automation tools with IAM services to manage authentication and authorization securely.

Secure APIs and Integration:

- API Security: Ensure that APIs used for automation are secured with proper authentication and authorization mechanisms.
- Secure Communication: Implement secure communication protocols, such as HTTPS, to protect data transmitted between automation tools and cloud services.

Patch Management and Updates:

- Automation for Patching: Automate the patching and updating of software and dependencies to reduce the risk of vulnerabilities. Regularly update automation tools themselves.
- Test Environments: Test updates in non-production environments before applying them to production systems.

Virtual Machine Security

The administrator must set up a program or application that prevents virtual machines from consuming additional resources without permission. Additionally, a lightweight process that gathers logs from the VMs and monitors them in real-time to repair any VM tampering must operate on a Virtual Machine. Best security procedures must be used to harden the guest OS and any running applications. These procedures include setting up firewalls, host intrusion prevention systems (HIPS), anti-virus and anti-spyware programmers, online application protection, and log monitoring in guest operating systems.

Guest Image Security

A policy to control the creation, use, storage, and deletion of images must be in place for organizations that use virtualization. To find viruses, worms, spyware, and rootkits that hide from security software running in a guest OS, image files must be analyzed.

Benefits of Virtualized Security

- Virtualized security is now practically required to meet the intricate security requirements of a virtualized network, and it is also more adaptable and effective than traditional physical security.
- Cost-Effectiveness: Cloud computing's virtual machine security enables businesses to keep their networks secure without having to significantly raise their expenditures on pricey proprietary hardware. Usage-based pricing for cloud-based virtualized security services can result in significant savings for businesses that manage their resources effectively.
- Flexibility: It is essential in a virtualized environment that security operations can follow workloads wherever they go. A company is able to profit fully from virtualization while simultaneously maintaining data security thanks to the protection it offers across various data centers, in multi-cloud, and hybrid-cloud environments.
- Operational Efficiency: Virtualized security can be deployed more quickly and easily than hardware-based security because it doesn't require IT, teams, to set up and configure several hardware appliances. Instead, they may quickly scale security systems by setting them up using centralized software. Security-related duties can be automated when security technology is used, which frees up more time for IT employees.
- Regulatory Compliance: Virtual machine security in cloud computing is a requirement for enterprises that need to maintain regulatory compliance because traditional hardware-based security is static and unable to keep up with the demands of a virtualized network.

Virtualization Machine Security Challenges

- As we previously covered, buffer overflows are a common component of classical network attacks. Trojan horses, worms, spyware, rootkits, and DoS attacks are examples of malware.
- In a cloud context, more recent assaults might be caused via VM rootkits, hypervisor malware, or guest hopping and hijacking. Man-in-the-middle attacks against VM migrations are another form of attack. Typically, passwords or sensitive information are stolen during passive attacks. Active attacks could alter the kernel's data structures, seriously harming cloud servers.
- HIDS or NIDS are both types of IDSs. To supervise and check the execution of code, use programmed shepherding. The RIO dynamic optimization infrastructure, the v Safe and v Shield tools from VMware, security compliance for hypervisors, and Intel vPro technology are some further protective solutions.

Four Steps to ensure VM Security in Cloud Computing

Protect Hosted Elements by Segregation

To secure virtual machines in cloud computing, the first step is to segregate the newly hosted components. Let's take an example where three features that are now running on an edge device may be placed in the cloud either as part of a private subnetwork that is invisible or as part of the service data plane, with addresses that are accessible to network users.

All Components are Tested and Reviewed

Before allowing virtual features and functions to be implemented, you must confirm that they comply with security standards as step two of cloud-virtual security. Virtual networking is subject to outside attacks, which can be dangerous, but insider attacks can be disastrous. When a feature with a backdoor security flaw is added to a service, it becomes a part of the infrastructure of the service and is far more likely to have unprotected attack paths to other infrastructure pieces.

Separate Management APIs to Protect the Network

The third step is to isolate service from infrastructure management and orchestration. Because they are created to regulate features, functions, and service behaviors, management APIs will always pose a significant risk. All such APIs should be protected, but the ones that keep an eye on infrastructure components that service users should never access must also be protected.

Keep Connections Secure and Separate

The fourth and last aspect of cloud virtual network security is to make sure that connections between tenants or services do not cross over into virtual networks. Virtual Networking is a fantastic approach to building quick connections to scaled or redeployed features, but each time a modification is made to the virtual network, it's possible that an accidental connection will be made between two distinct services, tenants, or feature/function deployments. A data plane leak, a link between the actual user networks, or a management or control leak could result from this, allowing one user to affect the service provided to another.