UNIT-4: CLOUD SECURITY AND PRIVACY

Introduction to Cloud Security

Cloud security refers to the set of policies, controls, procedures, and technologies designed to protect data, applications, and infrastructure in cloud environments. As organizations increasingly adopt cloud computing, securing cloud resources becomes critical to prevent unauthorized access, data breaches, and cyber threats.

Key Aspects of Cloud Security

Data Security – Protecting data from unauthorized access, loss, and corruption.

Identity and Access Management (IAM) – Ensuring that only authorized users have access to cloud resources.

Network Security – Implementing firewalls, intrusion detection, and encryption techniques.

Compliance and Legal Issues – Adhering to regulatory frameworks.

Cloud Governance – Defining policies for security management and risk mitigation.

Incident Response – Developing strategies to handle security breaches and threats effectively.

Threats in Cloud Computing

Cloud environments are prone to various security threats due to their shared resources and internet-based accessibility. Some common threats include:

1. Data Breaches

- Unauthorized access to sensitive data stored in the cloud.
- Can result from weak authentication, insider threats, or poor encryption.

2. Data Loss

- Data corruption or unintentional deletion due to system failures or cyberattacks.
- Lack of proper backup mechanisms exacerbates the problem.

3. Insider Threats

- Employees or service providers misusing access rights to compromise data.
- Hard to detect due to the legitimate access privileges of insiders.

4. Denial of Service (DoS) Attacks

- Attackers overwhelm cloud resources, making them unavailable to users.
- Disrupts business operations and leads to financial losses.

5. Account Hijacking

- Cybercriminals gain control of user credentials through phishing or credential stuffing.
- Can lead to unauthorized access to critical cloud services.

6. Insecure APIs

- Poorly secured cloud APIs can expose data and services to cyber threats.
- Attackers exploit vulnerabilities to manipulate cloud applications.

7. Malware and Ransomware Attacks

- Malware infections can compromise cloud workloads.
- Ransomware can encrypt user data and demand ransom for access.

Vulnerabilities in Cloud Computing

Cloud systems have inherent vulnerabilities that can be exploited by attackers. Some key vulnerabilities include:

1. Misconfigured Cloud Settings

- Incorrect access controls or permissions can expose data to unauthorized users.
- Default security settings might not provide adequate protection.

2. Lack of Encryption

- Unencrypted data transmission and storage increase the risk of data interception.
- Weak encryption algorithms can be broken by attackers.

3. Multi-Tenancy Risks

- Cloud providers host multiple clients on shared infrastructure.
- A vulnerability in one tenant's application can affect others.

4. Insufficient Identity and Access Management

- Weak password policies and lack of multi-factor authentication (MFA) increase risks.
- Unauthorized users can exploit weak IAM controls to gain access.

5. Shadow IT

- Unauthorized use of cloud services without IT department knowledge.
- Can lead to unmonitored security risks and compliance violations.

6. Inadequate Security Patching

- Failure to update cloud services with the latest security patches.
- Leaves systems vulnerable to known exploits.

Data Protection Techniques

1. Encryption

- Before transferring data to cloud storage, it has to be transformed or encoded. Cloud security service providers typically provide customers with various encryption methods.
- A comprehensive cloud data protection platform should include strong access controls and key management features that let businesses use encryption practically and affordably.

2. Authentication and identity security

- An identity check is necessary to ensure the person is who they claim to be and that the information they provide is accurate before you can trust them. Authentication is based on data that can only be produced by one, specific individual.
- This can include personal information, such as their full name, social security number, or license number. Physical identification techniques are also frequently used to authenticate someone’s identity, including fingerprint scanning or facial recognition.

3. Safe deletion techniques

- Your personal and professional information may be vulnerable if data on devices and in the cloud is not properly deleted.
- Choosing how long old data should be preserved and when it should be removed is the first step in managing and truly eliminating “deleted” data. As such, your company should determine:

How long data should be stored for regulatory purposes

- The length of time stakeholders should have immediate access to data. For example, someone from HR may upload employee contact information that is only available to an executive for a day

4. Managing access control

- Access control is a technique for ensuring users have the right level of access to corporate data—and that they are who they say they are. It involves selectively limiting access to information through a combination of authentication and authorization. As outlined above, authentication ensures the person is who they say they are, while authorization centers around making sure they have the right to use certain areas of your cloud network.

An adequate access control system can:

- Be seamlessly transferred into virtual environments like private clouds
- Work seamlessly with an organization's cloud assets and applications

5. Backing up data

- Organizations must configure each system that uses cloud security services to perform automatic backups at least once a week. This is especially true for systems that store data used in day-to-day operations. The software, operating system, and data on each workstation should all be backed up.
- Another general rule is to perform periodic backups according to regulatory compliance standards. For example, under the Health Insurance Portability and Accountability Act (HIPAA), hospitals must perform backups every day.

What Is Identity and Access Management(IAM)?

- 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)

- Users
- Roles
- Groups
- Policies
- With these new applications being created over the cloud, mobile and on-premise can hold sensitive and regulated information. It's no longer acceptable and feasible to just create an Identity server and provide access based on the requests.
- In current times an organization should be able to track the flow of information and provide least privileged access as and when required, obviously with a large workforce and new applications being added every day it becomes quite difficult to do the same.
- So organizations specifically concentrate on managing identity and its access with the help of a few IAM tools. It's quite obvious that it is very difficult for a single tool to manage everything but there are multiple IAM tools in the market that help the organizations with any of the few services given below.

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.

Example

With the aid of IAM users, we can accomplish our goal of giving a specific person access to every service available in the Amazon dashboard with only a limited set of permissions, such as read-only access. Let's say user-1 is a user that I want to have read-only access to the EC2 instance and no additional permissions, such as create, delete, or update. By creating an IAM user and attaching user-1 to that IAM user, we may allow the user access to the EC2 instance with the required permissions.

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.

Example

Consider two users named user-1 and user-2. If we want to grant user-1 specific permissions, such as the ability to delete, create, and update the auto-calling group only, and if we want to grant user-2 all the necessary permissions to maintain the auto-scaling group as well as the ability to maintain EC2,S3 we can create groups and add this user to them. If a new user is added, we can add that user to the required group with the necessary permissions.

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.

Example

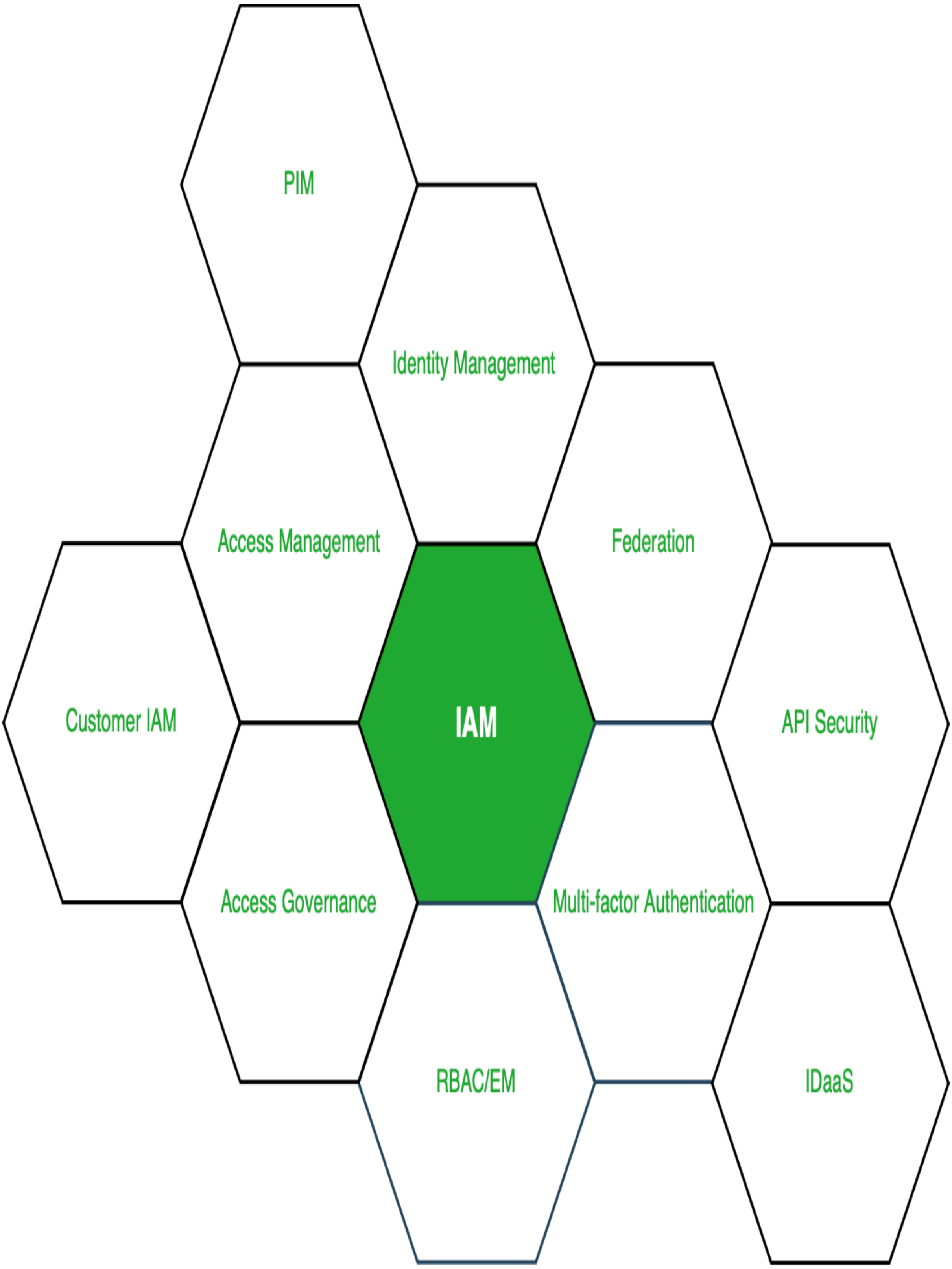
Consider Amazon EKS. In order to maintain an autoscaling group, AWS eks needs access to EC2 instances. Since we can't attach policies directly to the eks in this situation, we must build a role and then attach the necessary policies to that specific role and attach that particular role to EKS.

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.

Access Management For AWS Resources Identity Management

- Access management
- Federation
- RBAC/EM
- Multi-Factor authentication
- Access governance
- Customer IAM
- API Security
- IDaaS – Identity as a service
- Granular permissions
- Privileged Identity management – PIM (PAM or PIM is the same)



Services under IAM