CLOUD COMPUTING PRACTICAL 3

IDENTITY ACCESS MANAGEMENT (IAM)

NAME: KHUSHI

ROLL NO.: A073

Write-up:

Users and Groups

In cloud environments, Users and Groups are essential components in managing and organizing access control.

- Users represent individual identities that require access to resources. They can be employees, contractors, or applications that need permissions to operate in the system. Each user is given a unique identity within the organization, allowing for customized access and permissions.

- Groups are collections of users with similar access needs. Rather than assigning permissions to each user individually, administrators can create groups and assign specific permissions to the group, simplifying management. For example, a "Developers" group might be given permission to deploy applications, while a "Support" group could be restricted to viewing logs and system statuses.

Together, Users and Groups allow administrators to streamline access control policies, manage permissions more efficiently, and ensure that only authorized individuals have access to specific resources.

IAM (Identity and Access Management)

IAM (Identity and Access Management) is a critical framework in cloud security that enables organizations to define, manage, and control user access to resources. IAM provides a centralized way to create and manage identities, roles, and policies that specify what level of access each user or application has to resources.

The key functions of IAM include:

- Authentication: Verifying that users are who they claim to be, typically via passwords, multi-factor authentication, or single sign-on (SSO).

- Authorization: Granting the correct level of access to authenticated users based on their roles and policies.

- User Management: Creating, modifying, and deleting user accounts as employees join, leave, or change roles within the organization.

- Policy Management: Defining permissions and rules that control what resources users or groups can access and what actions they can perform.

IAM plays a crucial role in maintaining security and compliance, helping organizations avoid unauthorized access and safeguard sensitive data.

Role of IAM

The Role of IAM extends beyond just assigning access; it serves as the foundation of security and governance within an organization. IAM's responsibilities are essential for:

1. Enhancing Security: By ensuring that only authorized individuals or systems can access specific resources, IAM reduces the risk of unauthorized access or data breaches.

2. Maintaining Compliance: Many industries require strict access control for regulatory compliance. IAM provides the necessary tools to meet these standards, often with detailed logging and auditing capabilities.

3. Improving Operational Efficiency: IAM simplifies access management by using roles and groups, reducing the administrative workload associated with granting and revoking access.

4. Supporting Scalability: As organizations grow, IAM makes it easier to manage thousands of users and their permissions across various systems, applications, and resources.

IAM is essential in cloud environments, where resources are highly distributed and continuously scaled, making access control crucial for effective governance and security.

This overview highlights how IAM, along with user and group management, provides a structured approach to managing permissions and protecting sensitive data within an organization.