**AMAZON WEB SERVICES.**

Amazon web services provides a secure virtual platform were users can successfully deploy their applications.

Amazon provides a high-level protection of data with little to no cost.

AWS have a number services that help users secure their account and application. They include:

- IAM

- Key management system

- Cognito

- Web access firewall

One of them is the IAM (Identity and Access Management), it is widely used.

What is IAM?

The IAM is use to create and manage users, groups, set password policies, enable MFA and give permissions.

The IAM allows you to manage your AWS services and resources in a more secured manner. You can create groups and assign users to them. You can give certain permissions to the users/group, this helps to limit who have access to your AWS resources and also limit how it’s being used

Why even use IAM?

//Make sure to change tone//

Before AWS or IAM, companies share password in an insecure manner. They do this through text, call or even through handwritten note. Using these means a hacker can easily access the password and carry out its malicious intent.

We can see why advent of AWS and IAM, has helped mitigate these security issues.

IAM Workflow.

How does the IAM work?

1. A principal is an entity that can perform actions on an AWS service. A user, group, roles, applications can be a principal
2. Authentication is the process of confirming the credentials or access keys of a principal trying to access an AWS service.
3. Request: This is the process whereby a principal sends a request to AWS specifying an action and which resource/service should perform it.
4. Authorization: By default, a principal cannot access any resource. IAM allows a request to be resolved only it is allowed by a matching policy
5. Actions are used to create, edit, view or delete a resource.
6. Resources: Actions are performed on resources.

Components

The components of IAM are as follows:

1. Users – An IAM user is an identity with an associated credentials and permissions attached to it. A user can an individual or an application. By default a new user is not associated to any service or permissions. An organization can safely secure it data and operations by creating a user for each employee.
2. Groups – A collection of users in IAM is a group. If a permission is applied to a group, our users in that group can also access the permission. This helps to reduce administrator burden.
3. Policies – Policies are used to set permissions and control access to AWS services and resources. A policy would contain:

- Who can access a given resource.

- What actions can be performed.

- When a resource can be accessed.

There are different types of policies:

- Managed policies: These types are default policies that can be

attached to an AWS account.

- Inline policies; These policies are created by the user, and can be embedded into a single entity.

4) Role: An IAM role is a set of permission that define what actions are allowed or denied.

Features of IAM.

1. Shared access to the AWS account. The main feature of IAM is that it allows you to create separate usernames and password for the user and delegate certain roles and resources to them,
2. Granular permissions: this help to enforce a set of rules, on what a user can do and can’t do.
3. Multi Factor Authentication: This add additional layer of security to your AWS account. It helps to ensure that your account can only accessed with a certain device.
4. Identity federation: This enables IAM to trust a particular authentication method.
5. Free to use: There is little to no charge when using IAM and its services.
6. Password Policy: This helps to enforce a certain password rules. Where users are forced to enter strong passwords, change passwords after some weeks/months.