## What are the Prerequisites to learn Cloud Computing?

So if you want to take cloud computing course, you wonder what prerequisites one needs. This is the question that bothers most of the IT professionals who want to delve into the world of cloud. There are also several myths surrounding the requirements to become a cloud computing professional. In this article, while taking you through the skills required to learn it, we will also attempt to bust the false assumptions about the same.

The term Cloud Computing is an umbrella term and encompasses many different concepts of Information Technology. It basically dwells around the areas of IT that involve software infrastructures, hardware infrastructures, virtualization technologies, data center facilities, and software engineering concepts.

In this article, we will emphasize on Infrastructure as a Service cloud providers such as  Amazon Web Services.

**Knowledge of Operating Systems**

As Amazon cloud is a broad area, it is essential to know the basic concepts related to Operating Systems, like Windows, Linux, etc. (e.g. how they work and operate at a high level).

Learning to use Linux operating system is essential as most organizations that work with web applications and scalable environments use Linux as their preferred Operating System. Linux is also the main choice for using an Infrastructure-as-a-Service (IaaS) platform i.e. the [AWS platform](https://aws.amazon.com/choosing-a-cloud-platform/). The best way to learn Linux is to start using it and going through the documentation and basic courses online.

**Knowledge of Virtualization**

Once you acquire a working knowledge of operating systems, the next thing to learn is Virtualization Technology. Virtualization plays a huge role in this.

Virtualization is a technique to the house and runs multiple operating systems (virtual machines) within a single physical machine. Each virtual machine has specific CPU, RAM, and disk space capacities and runs its own operating system.

Virtual machines share the same hardware and the same network equipment. They are just virtually separated from one another.

**Knowledge of Networking**

Networking is an essential element of Amazon cloud as all operations in a cloud platform involve networking. To start with, you should at least have the understanding of how IP addresses work and comprehend what public and private networks are.

Each cloud instance needs to be connected to the Internet. Mastering the concepts of networking can be a difficult task as it requires you to learn certain key skills that demand time to understand.

## Understanding of the Difference Between Public and Private Cloud Computing

To become an Amazon cloud professional, it is essential to understand the difference between [Public and Private Cloud Computing](http://www.onlinetech.com/resources/references/public-vs-private-cloud-computing).

**Public Cloud:**A publicly accessible cloud infrastructure that allows you to store data, virtual machines, and other cloud resources. Public clouds can be used with a pay per use approach. It is like renting an infrastructure for a specific period of time.

**Private Cloud:**It is similar to the public cloud in terms of services like flexibility and scalability and self-service, however, it is dedicated to a single enterprise and cannot be accessed publicly. In other words, it refers to an organization’s own private data center that has all the [advantages of Cloud Computing](https://www.springpeople.com/blog/google-cloud-computing-elements-features-benefits/) but everything is housed within the company’s own infrastructure which is managed privately.

**Coding skills (Good To Have):**Although it is not a prerequisite, it is good to have knowledge of coding as building applications for the cloud and deploying them into the AWS cloud requires programming knowledge.

However, it is not mandatory to have coding skills as most of the platforms like Amazon Web Services, contain API sets to automate all the operations and orchestrate all the resources with the organization software. Moreover, cloud computing has several facets spanning across different roles and can be grasped by non-programmers as well.

Now you know the basic requirements to [learn Cloud Computing](https://www.springpeople.com/blog/what-are-the-prerequisites-to-learn-cloud-computing-amazon-web-services/), let’s clarify the false assumptions now.

## Notions about learning Cloud Computing: Myths Busted

**Myth** – You should know coding to learn it.

**Fact**– To try your hands on, you can take cloud computing courses and begin using a public or private cloud computing service. You need not be a coder.

**Myth**– CC is a niche domain only meant for techies and developers.

**Fact**– Anyone can learn it. It is transforming the way companies conduct business and this involves all the internal stakeholders of the enterprise. Therefore, It is equally important to be learned by managers, marketing experts, system administrators, and developers. Yes, approaches and specific aspects will vary with different roles and responsibilities.

**Myth –** You should have previous IT experience to learn cloud computing.

**Fact –** It can be learned by anyone from scratch. The cloud infrastructure is used almost by everyone one in various ways. So, you need not to be a technical pro to grasp It.

With the growing buzz and exponential rise of cloud dependency, demand for cloud computing professionals is not going to decrease in the coming years. The best way to learn it is to enroll in [cloud computing courses](https://www.springpeople.com/cloud-computing-training-courses) and practice through hands-on labs. The lab sessions acquaint you with the actual AWS environment.

Now you know what you need to learn AWS cloud computing, kickstart your endeavor today. Let’s meet in the cloud!

What is Cloud Computing

The term cloud refers to a network or the internet. It is a technology that uses remote servers on the internet to store, manage, and access data online rather than local drives. The data can be anything such as files, images, documents, audio, video, and more.

There are the following operations that we can do using cloud computing:

* Developing new applications and services
* Storage, back up, and recovery of data
* Hosting blogs and websites
* Delivery of software on demand
* Analysis of data
* Streaming videos and audios

## Why Cloud Computing?

Small as well as large IT companies, follow the traditional methods to provide the IT infrastructure. That means **for any IT company, we need a Server Room that is the basic need of IT companies**.

In that server room, there should be a database server, mail server, networking, firewalls, routers, modem, switches, QPS (Query Per Second means how much queries or load will be handled by the server), configurable system, high net speed, and the maintenance engineers.

To establish such IT infrastructure, we need to spend lots of money. To overcome all these problems and to reduce the IT infrastructure cost, Cloud Computing comes into existence

# Cloud Computing Architecture

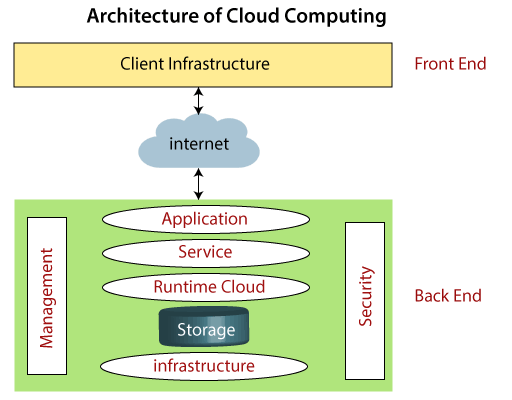
As we know, cloud computing technology is used by both small and large organizations to **store the information** in cloud and **access** it from anywhere at anytime using the internet connection.

Cloud computing architecture is a combination of **service-oriented architecture** and **event-driven architecture**.

Cloud computing architecture is divided into the following two parts -

* Front End
* Back End

The below diagram shows the architecture of cloud computing -



### Front End

The front end is used by the client. It contains client-side interfaces and applications that are required to access the cloud computing platforms. The front end includes web servers (including Chrome, Firefox, internet explorer, etc.), thin & fat clients, tablets, and mobile devices.

### Back End

The back end is used by the service provider. It manages all the resources that are required to provide cloud computing services. It includes a huge amount of data storage, security mechanism, virtual machines, deploying models, servers, traffic control mechanisms, etc.

#### Note: Both front end and back end are connected to others through a network, generally using the internet connection.

## Components of Cloud Computing Architecture

There are the following components of cloud computing architecture -

**1. Client Infrastructure**

Client Infrastructure is a Front end component. It provides GUI (Graphical User Interface)  to interact with the cloud.

**2. Application**

The application may be any software or platform that a client wants to access.

**3. Service**

A Cloud Services manages that which type of service you access according to the client’s requirement.

Cloud computing offers the following three type of services:

**i. Software as a Service (SaaS) –**It is also known as **cloud application services**. Mostly, SaaS applications run directly through the web browser means we do not require to download and install these applications. Some important example of SaaS is given below –

**Example:** Google Apps, Salesforce Dropbox, Slack, Hubspot, Cisco WebEx.

**ii. Platform as a Service (PaaS) –** It is also known as **cloud platform** **services**. It is quite similar to SaaS, but the difference is that PaaS provides a platform for software creation, but using SaaS, we can access software over the internet without the need of any platform.

**Example:** Windows Azure, Force.com, Magento Commerce Cloud, OpenShift.

**iii. Infrastructure as a Service (IaaS) –**It is also known as **cloud infrastructure services**. It is responsible for managing applications data, middleware, and runtime environments.

**Example:** Amazon Web Services (AWS) EC2, Google Compute Engine (GCE), Cisco Metapod.

**4. Runtime Cloud**

Runtime Cloud provides the **execution and runtime environment** to the virtual machines.

**5. Storage**

Storage is one of the most important components of cloud computing. It provides a huge amount of storage capacity in the cloud to store and manage data.

**6. Infrastructure**

It provides services on the **host level**, **application level**, and **network level**. Cloud infrastructure includes hardware and software components such as servers, storage, network devices, virtualization software, and other storage resources that are needed to support the cloud computing model.

**7. Management**

Management is used to manage components such as application, service, runtime cloud, storage, infrastructure, and other security issues in the backend and establish coordination between them.

**8. Security**

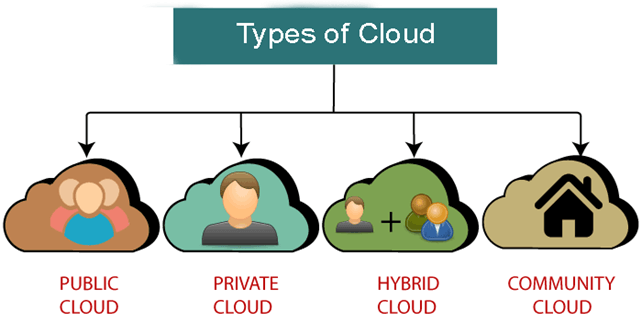
Security is an in-built back end component of cloud computing. It implements a security mechanism in the back end.

**9. Internet**

The Internet is medium through which front end and back end can interact and communicate with each other.

# Types of Cloud

There are the following 4 types of cloud that you can deploy according to the organization's needs-



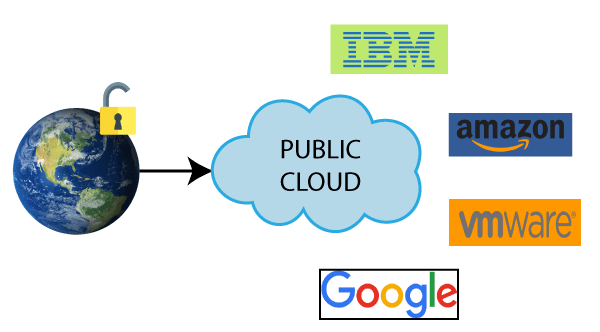
* [Public Cloud](https://www.javatpoint.com/types-of-cloud#Public)
* [Private Cloud](https://www.javatpoint.com/types-of-cloud#Private)
* [Hybrid Cloud](https://www.javatpoint.com/types-of-cloud#Hybrid)
* [Community Cloud](https://www.javatpoint.com/types-of-cloud#Community)

## Public Cloud

Public cloud is **open to all** to store and access information via the Internet using the pay-per-usage method.

In public cloud, computing resources are managed and operated by the Cloud Service Provider (CSP).

**Example:** Amazon elastic compute cloud (EC2), IBM SmartCloud Enterprise, Microsoft, Google App Engine, Windows Azure Services Platform.



### Advantages of Public Cloud

There are the following advantages of Public Cloud -

* Public cloud is owned at a lower cost than the private and hybrid cloud.
* Public cloud is maintained by the cloud service provider, so do not need to worry about the maintenance.
* Public cloud is easier to integrate. Hence it offers a better flexibility approach to consumers.
* Public cloud is location independent because its services are delivered through the internet.
* Public cloud is highly scalable as per the requirement of computing resources.
* It is accessible by the general public, so there is no limit to the number of users.

AD

### Disadvantages of Public Cloud

* Public Cloud is less secure because resources are shared publicly.
* Performance depends upon the high-speed internet network link to the cloud provider.
* The Client has no control of data.

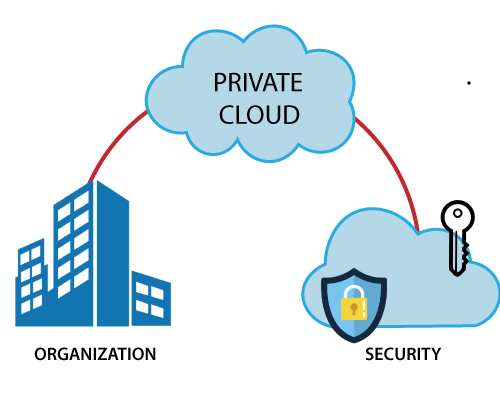
**To Read More** [**Click Here**](https://www.javatpoint.com/public-cloud)

## Private Cloud

Private cloud is also known as an **internal cloud** or **corporate cloud**. It is used by organizations to build and manage their own data centers internally or by the third party. It can be deployed using Opensource tools such as Openstack and Eucalyptus.

Based on the location and management, National Institute of Standards and Technology (NIST) divide private cloud into the following two parts-

* On-premise private cloud
* Outsourced private cloud



### Advantages of Private Cloud

There are the following advantages of the Private Cloud -

* Private cloud provides a high level of security and privacy to the users.
* Private cloud offers better performance with improved speed and space capacity.
* It allows the IT team to quickly allocate and deliver on-demand IT resources.
* The organization has full control over the cloud because it is managed by the organization itself. So, there is no need for the organization to depends on anybody.
* It is suitable for organizations that require a separate cloud for their personal use and data security is the first priority.

### Disadvantages of Private Cloud

* Skilled people are required to manage and operate cloud services.
* Private cloud is accessible within the organization, so the area of operations is limited.
* Private cloud is not suitable for organizations that have a high user base, and organizations that do not have the prebuilt infrastructure, sufficient manpower to maintain and manage the cloud.

**To Read More** [**Click Here**](https://www.javatpoint.com/private-cloud)

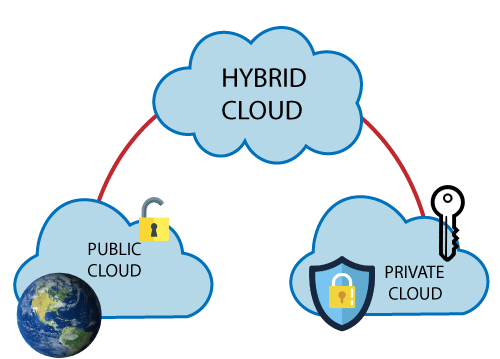
## Hybrid Cloud

Hybrid Cloud is a combination of the public cloud and the private cloud. we can say:

**Hybrid Cloud = Public Cloud + Private Cloud**

Hybrid cloud is partially secure because the services which are running on the public cloud can be accessed by anyone, while the services which are running on a private cloud can be accessed only by the organization's users.

**Example:** Google Application Suite (Gmail, Google Apps, and Google Drive), Office 365 (MS Office on the Web and One Drive), Amazon Web Services.



### Advantages of Hybrid Cloud

There are the following advantages of Hybrid Cloud -

* Hybrid cloud is suitable for organizations that require more security than the public cloud.
* Hybrid cloud helps you to deliver new products and services more quickly.
* Hybrid cloud provides an excellent way to reduce the risk.
* Hybrid cloud offers flexible resources because of the public cloud and secure resources because of the private cloud.

### Disadvantages of Hybrid Cloud

* In Hybrid Cloud, security feature is not as good as the private cloud.
* Managing a hybrid cloud is complex because it is difficult to manage more than one type of deployment model.
* In the hybrid cloud, the reliability of the services depends on cloud service providers.

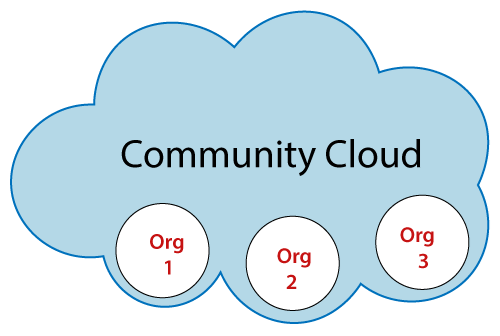
**To Read More** [**Click Here**](https://www.javatpoint.com/hybrid-cloud)

AD

## Community Cloud

Community cloud allows systems and services to be accessible by a group of several organizations to share the information between the organization and a specific community. It is owned, managed, and operated by one or more organizations in the community, a third party, or a combination of them.

**Example:** Health Care community cloud



### Advantages of Community Cloud

There are the following advantages of Community Cloud -

* Community cloud is cost-effective because the whole cloud is being shared by several organizations or communities.
* Community cloud is suitable for organizations that want to have a collaborative cloud with more security features than the public cloud.
* It provides better security than the public cloud.
* It provdes collaborative and distributive environment.
* Community cloud allows us to share cloud resources, infrastructure, and other capabilities among various organizations.

### Disadvantages of Community Cloud

* Community cloud is not a good choice for every organization.
* Security features are not as good as the private cloud.
* It is not suitable if there is no collaboration.
* The fixed amount of data storage and bandwidth is shared among all community members.

**To Read More** [**Click Here**](https://www.javatpoint.com/community-cloud)

## Difference between public cloud, private cloud, hybrid cloud, and community cloud -

The below table shows the difference between public cloud, private cloud, hybrid cloud, and community cloud.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Parameter** | **Public Cloud** | **Private Cloud** | **Hybrid Cloud** | **Community Cloud** |
| **Host** | Service provider | Enterprise (Third party) | Enterprise (Third party) | Community (Third party) |
| **Users** | General public | Selected users | Selected users | Community members |
| **Access** | Internet | Internet, VPN | Internet, VPN | Internet, VPN |
| **Owner** | Service provider | Enterprise | Enterprise | Community |

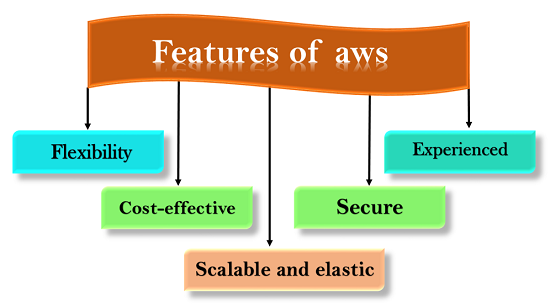
What is AWS?

* AWS stands for **Amazon Web Services**.
* The AWS service is provided by the Amazon that uses distributed IT infrastructure to provide different IT resources available on demand. It provides different services such as infrastructure as a service (IaaS), platform as a service (PaaS) and packaged software as a service (SaaS).
* Amazon launched AWS, a cloud computing platform to allow the different organizations to take advantage of reliable IT infrastructure.

Uses of AWS

* A small manufacturing organization uses their expertise to expand their business by leaving their IT management to the AWS.
* A large enterprise spread across the globe can utilize the AWS to deliver the training to the distributed workforce.
* An architecture consulting company can use AWS to get the high-compute rendering of construction prototype.
* A media company can use the AWS to provide different types of content such as ebox or audio files to the worldwide files.

# Features of AWS



The following are the features of AWS:

* Flexibility
* Cost-effective
* Scalable and elastic
* Secure
* Experienced

## 1) Flexibility

* The difference between AWS and traditional IT models is **flexibility**.
* The traditional models used to deliver IT solutions that require large investments in a new architecture, programming languages, and operating system. Although these investments are valuable, it takes time to adopt new technologies and can also slow down your business.
* The flexibility of AWS allows us to choose which programming models, languages, and operating systems are better suited for their project, so we do not have to learn new skills to adopt new technologies.
* Flexibility means that migrating legacy applications to the cloud is easy, and cost-effective. Instead of re-writing the applications to adopt new technologies, you just need to move the applications to the cloud and tap into advanced computing capabilities.
* Building applications in aws are like building applications using existing hardware resources.
* The larger organizations run in a hybrid mode, i.e., some pieces of the application run in their data center, and other portions of the application run in the cloud.
* The flexibility of aws is a great asset for organizations to deliver the product with updated technology in time, and overall enhancing the productivity.

AD

## 2) Cost-effective

* Cost is one of the most important factors that need to be considered in delivering IT solutions.
* For example, developing and deploying an application can incur a low cost, but after successful deployment, there is a need for hardware and bandwidth. Owing our own infrastructure can incur considerable costs, such as power, cooling, real estate, and staff.
* The cloud provides on-demand IT infrastructure that lets you consume the resources what you actually need. In aws, you are not limited to a set amount of resources such as storage, bandwidth or computing resources as it is very difficult to predict the requirements of every resource. Therefore, we can say that the cloud provides flexibility by maintaining the right balance of resources.
* AWS provides no upfront investment, long-term commitment, or minimum spend.
* You can scale up or scale down as the demand for resources increases or decreases respectively.
* An aws allows you to access the resources more instantly. It has the ability to respond the changes more quickly, and no matter whether the changes are large or small, means that we can take new opportunities to meet the business challenges that could increase the revenue, and reduce the cost.

## 3) Scalable and elastic

* In a traditional IT organization, scalability and elasticity were calculated with investment and infrastructure while in a cloud, scalability and elasticity provide savings and improved ROI (Return On Investment).
* Scalability in aws has the ability to scale the computing resources up or down when demand increases or decreases respectively.
* Elasticity in aws is defined as the distribution of incoming application traffic across multiple targets such as Amazon EC2 instances, containers, IP addresses, and Lambda functions.
* Elasticity load balancing and scalability automatically scale your AWS computing resources to meet unexpected demand and scale down automatically when demand decreases.
* The aws cloud is also useful for implementing short-term jobs, mission-critical jobs, and the jobs repeated at the regular intervals.

AD

## 4) Secure

* AWS provides a scalable cloud-computing platform that provides customers with end-to-end security and end-to-end privacy.
* AWS incorporates the security into its services, and documents to describe how to use the security features.
* AWS maintains confidentiality, integrity, and availability of your data which is the utmost importance of the aws.

**Physical security:** Amazon has many years of experience in designing, constructing, and operating large-scale data centers. An aws infrastructure is incorporated in AWS controlled data centers throughout the world. The data centers are physically secured to prevent unauthorized access.

**Secure services:** Each service provided by the AWS cloud is secure.

**Data privacy:** A personal and business data can be encrypted to maintain data privacy.

## 5) Experienced

* The AWS cloud provides levels of scale, security, reliability, and privacy.
* AWS has built an infrastructure based on lessons learned from over sixteen years of experience managing the multi-billion dollar Amazon.com business.
* Amazon continues to benefit its customers by enhancing their infrastructure capabilities.
* Nowadays, Amazon has become a global web platform that serves millions of customers, and AWS has been evolved since 2006, serving hundreds of thousands of customers worldwide.

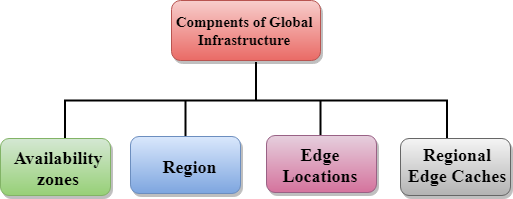
# AWS Global Infrastructure

* AWS is a cloud computing platform which is globally available.
* Global infrastructure is a region around the world in which AWS is based. Global infrastructure is a bunch of high-level IT services which is shown below:
* AWS is available in 19 regions, and 57 availability zones in December 2018 and 5 more regions 15 more availability zones for 2019.

The following are the components that make up the AWS infrastructure:

* Availability Zones
* Region
* Edge locations
* Regional Edge Caches

AD

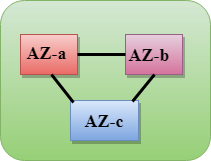


## Availability zone as a Data Center

* An availability zone is a facility that can be somewhere in a country or in a city. Inside this facility, i.e., Data Centre, we can have multiple servers, switches, load balancing, firewalls. The things which interact with the cloud sits inside the data centers.
* An availability zone can be a several data centers, but if they are close together, they are counted as 1 availability zone.

## Region

* A region is a geographical area. Each region consists of 2 more availability zones.
* A region is a collection of data centers which are completely isolated from other regions.
* A region consists of more than two availability zones connected to each other through links.



* Availability zones are connected through redundant and isolated metro fibers.

## Edge Locations

* Edge locations are the endpoints for AWS used for caching content.
* Edge locations consist of CloudFront, Amazon's Content Delivery Network (CDN).
* Edge locations are more than regions. Currently, there are over 150 edge locations.
* Edge location is not a region but a small location that AWS have. It is used for caching the content.
* Edge locations are mainly located in most of the major cities to distribute the content to end users with reduced latency.
* For example, some user accesses your website from Singapore; then this request would be redirected to the edge location closest to Singapore where cached data can be read.

AD

## Regional Edge Cache

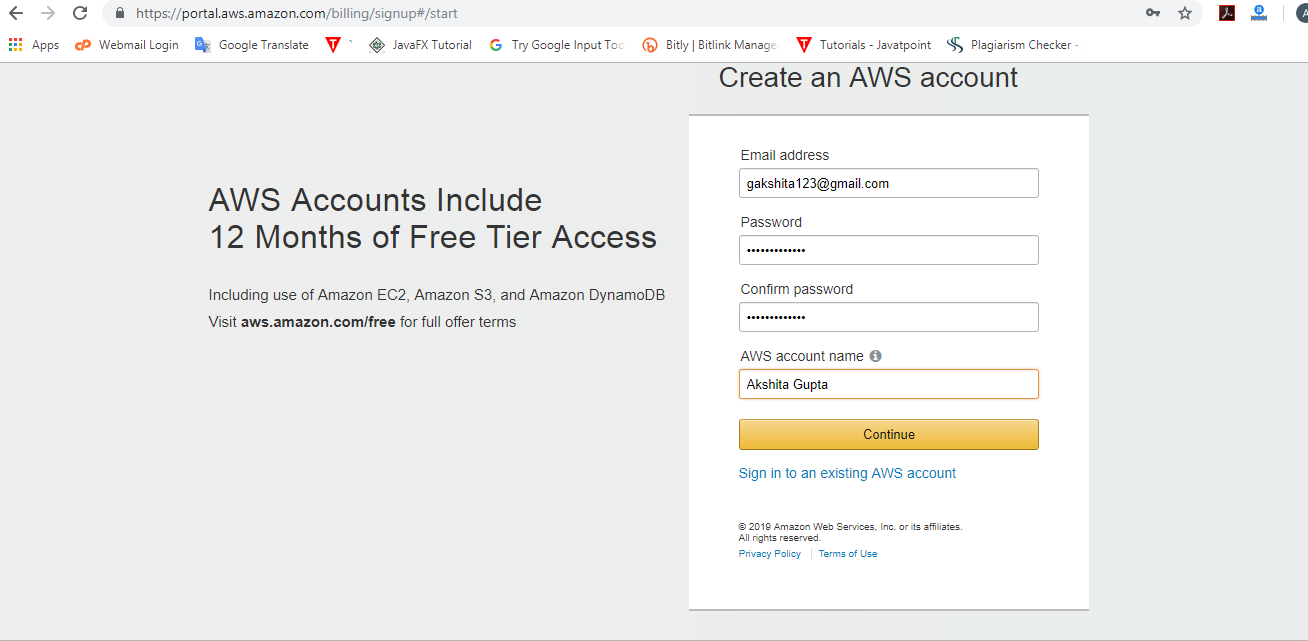
* AWS announced a new type of edge location in November 2016, known as a Regional Edge Cache.
* Regional Edge cache lies between CloudFront Origin servers and the edge locations.
* A regional edge cache has a large cache than an individual edge location.
* Data is removed from the cache at the edge location while the data is retained at the Regional Edge Caches.
* When the user requests the data, then data is no longer available at the edge location. Therefore, the edge location retrieves the cached data from the Regional edge cache instead of the Origin servers that have high latency.

# AWS Free Tier

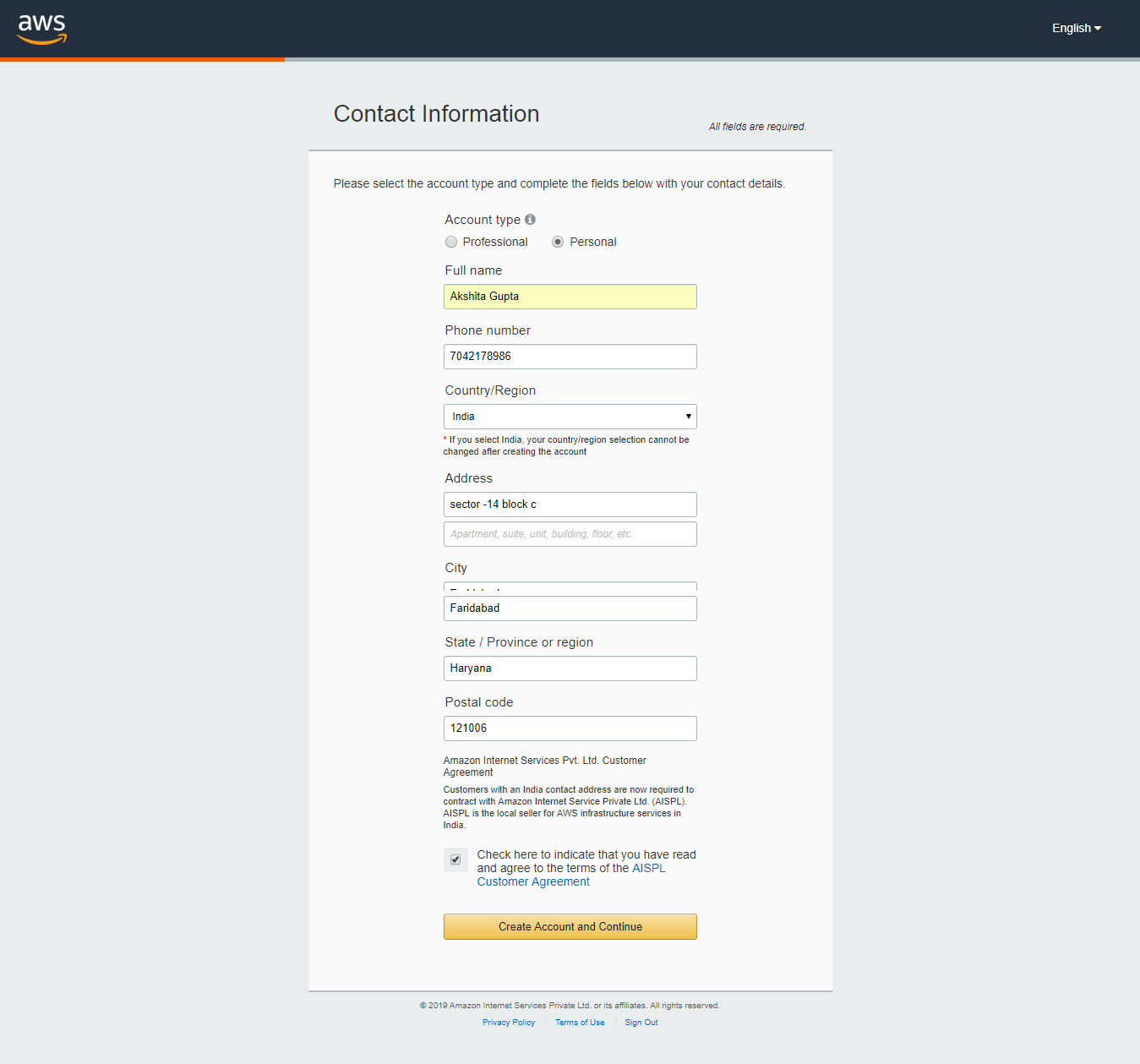
**How to SignUp to the AWS platform**

* Firstly visit the website [https://aws.amazon.com.](https://aws.amazon.com/)
* The following screen appears after opening the website, then click on the **Complete Sign Up** to create an account and fill the required details.
* The following screen appears after clicking on the **"Complete Sign Up"** button. If you are an already existing user of an AWS account, then enter the email address of your AWS account otherwise **"create an aws account"**.
* On clicking on the **"create an aws account"** button, the following screen appears that requires some fields to be filled by the user.
* On clicking on the **"create an aws account"** button, the following screen appears that requires some fields to be filled by the user.

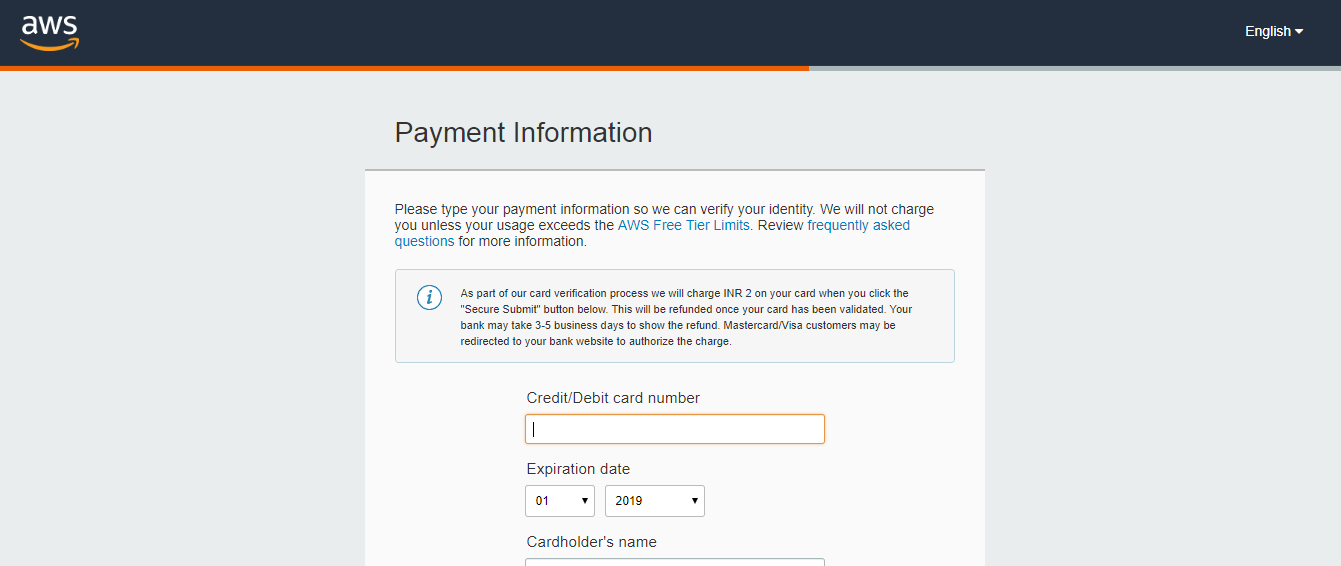
AD



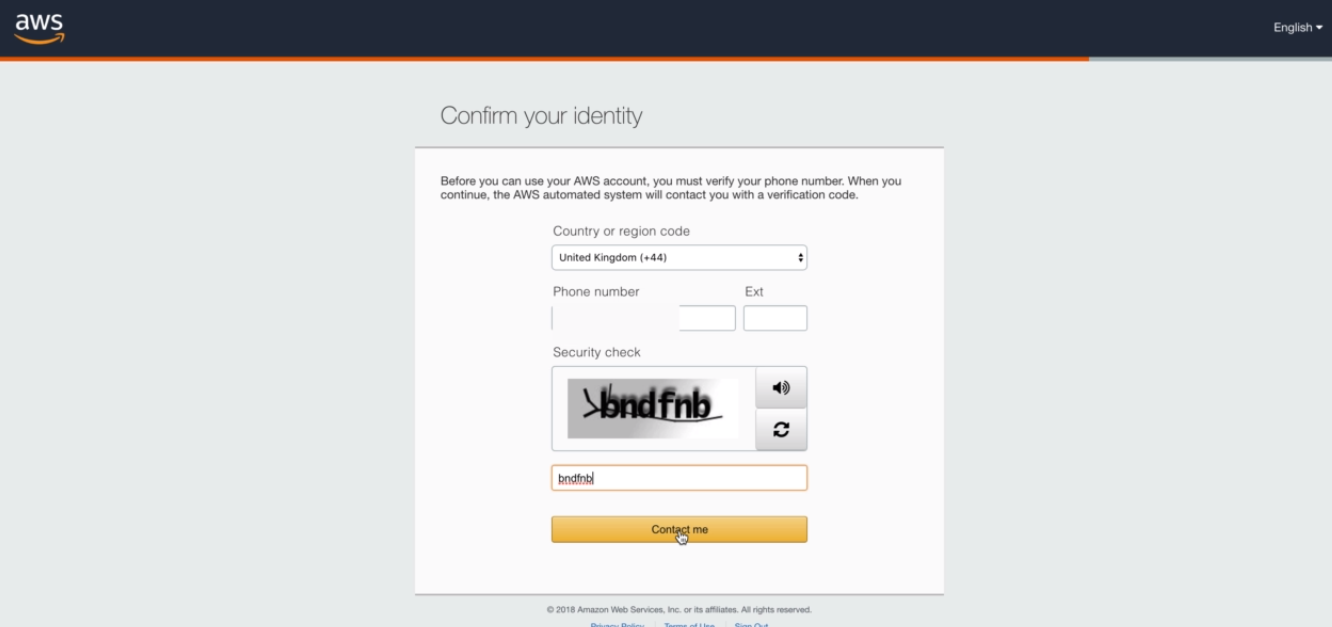
* Now, fill your contact information.



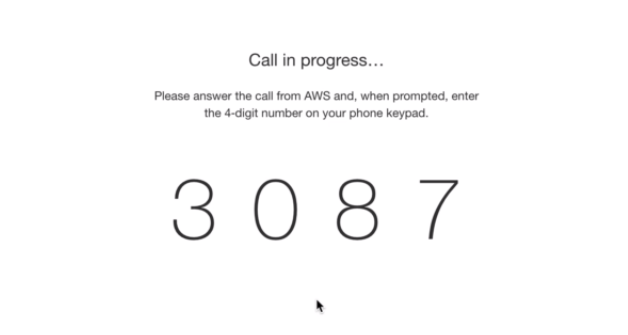
* After providing the contact information, fill your payment information.



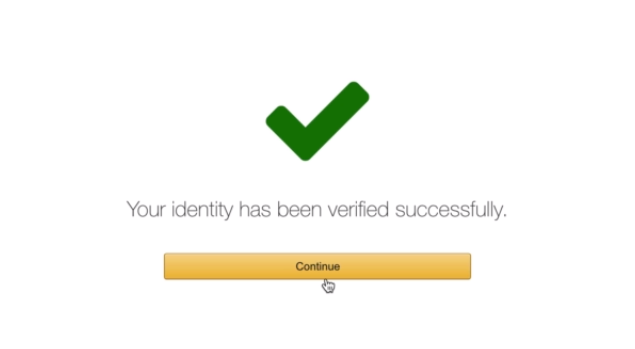
* After providing your payment information, confirm your identity by entering your phone number and security check code, and then click on the "Contact me" button.



* AWS will contact you to verify whether the provided contact number is correct or not.



* When number is verified, then the following message appears on the screen.

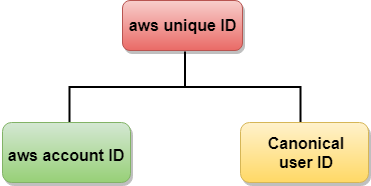


* The final step is the confirmation step. Click on the link to log in again; it redirects you to the **"Management Console"**.

## AWS Account Identifiers

**AWS assigns two types of unique ID to each user's account:**

* An AWS account ID
* A canonical user ID



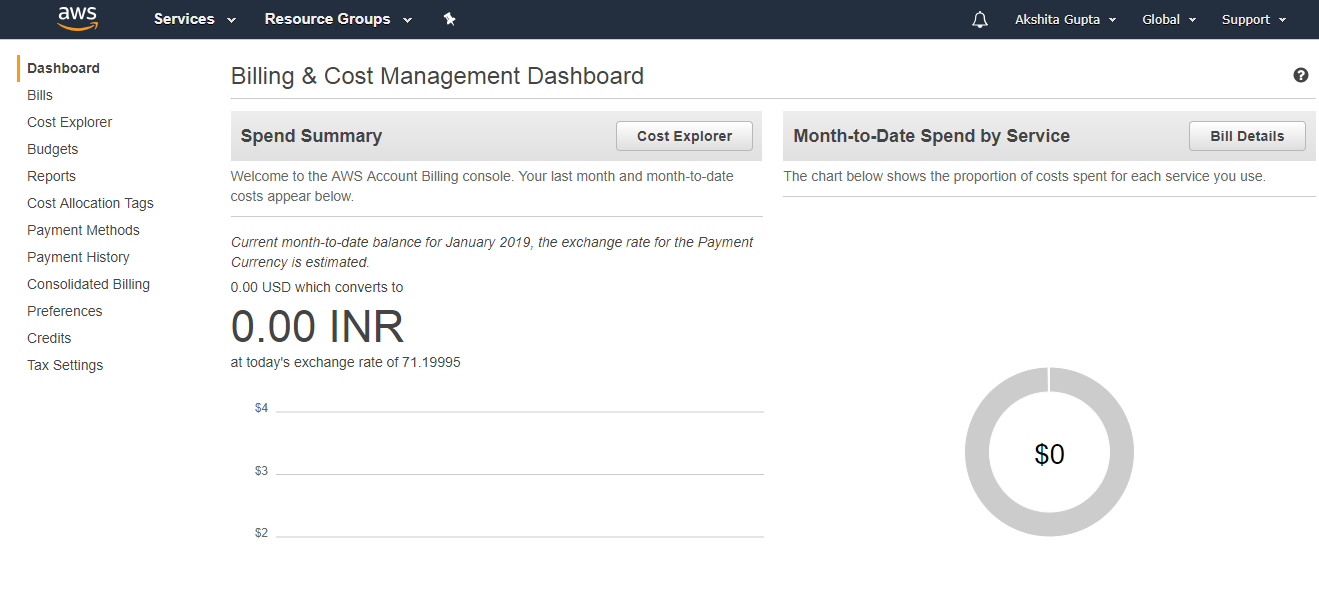
### AWS account ID

AWS account ID is a 12-digit number such as 123456780123 which can be used to construct **Amazon Resource Names (ARNs)**. Suppose we refer to resources such as an IAM user, the AWS account ID distinguishes the resources from resources in other AWS accounts.

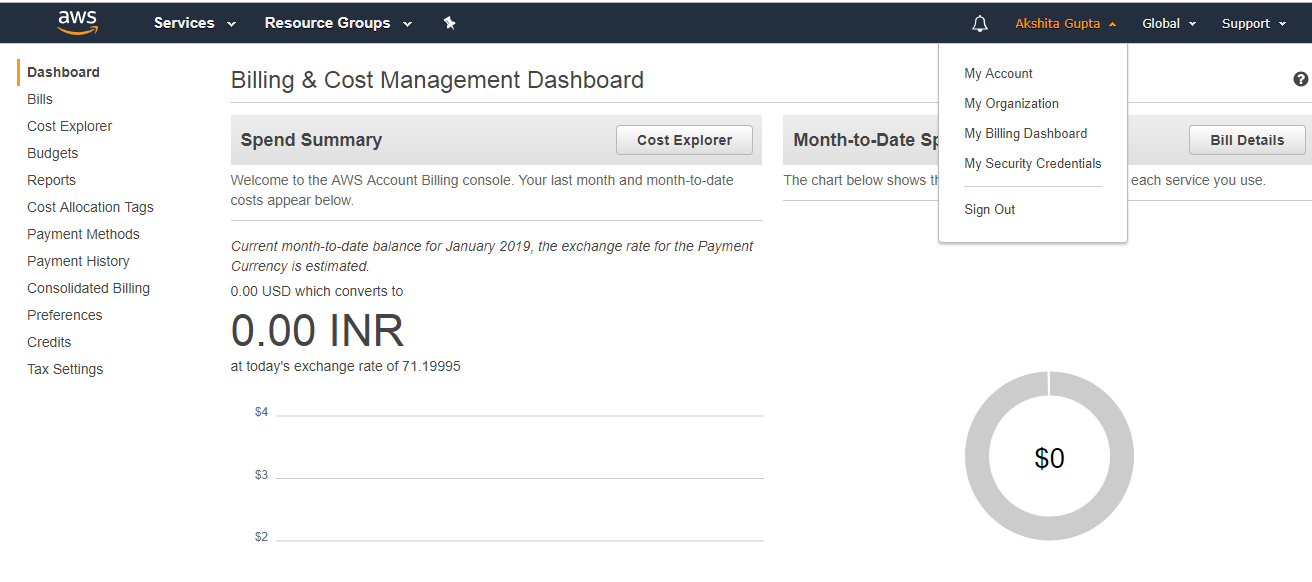
**Finding the AWS account ID**

We can find the AWS account ID from AWS Management Console. The following steps are taken to view your account ID:

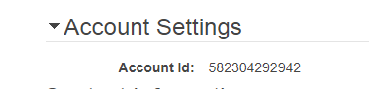
* Login to the aws account by entering your email address and password, and then you will move to the management console.



* Now, click on the account name, a dropdown menu appears.



* Click on **"My Account"** in the dropdown menu of account name to view your **account ID**.

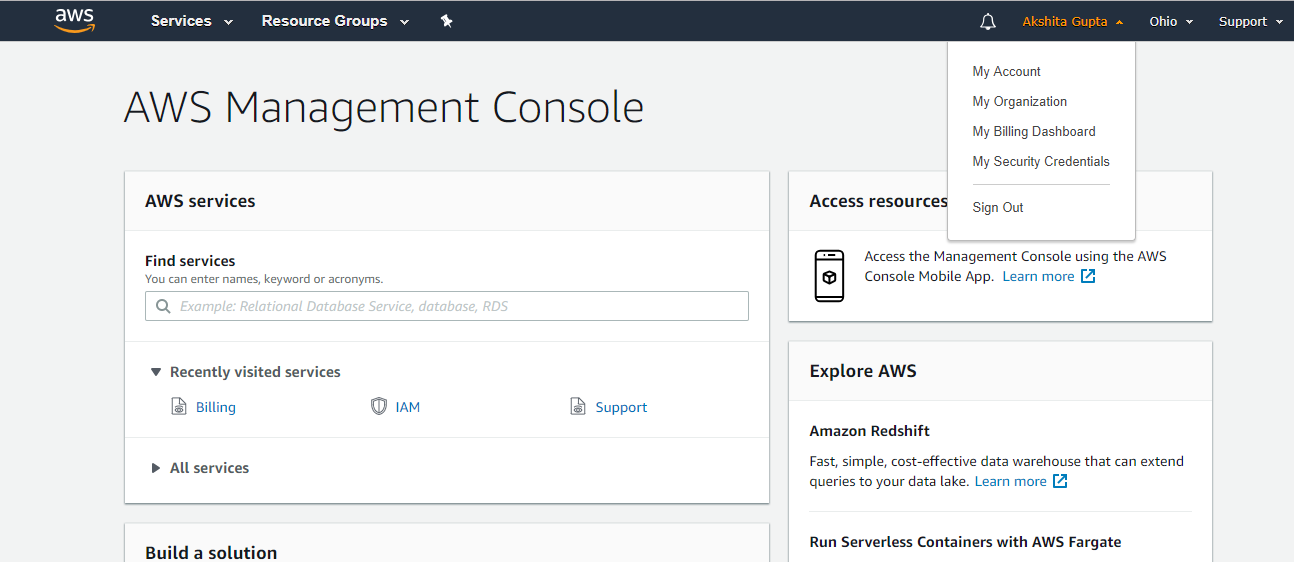


### Canonical User ID

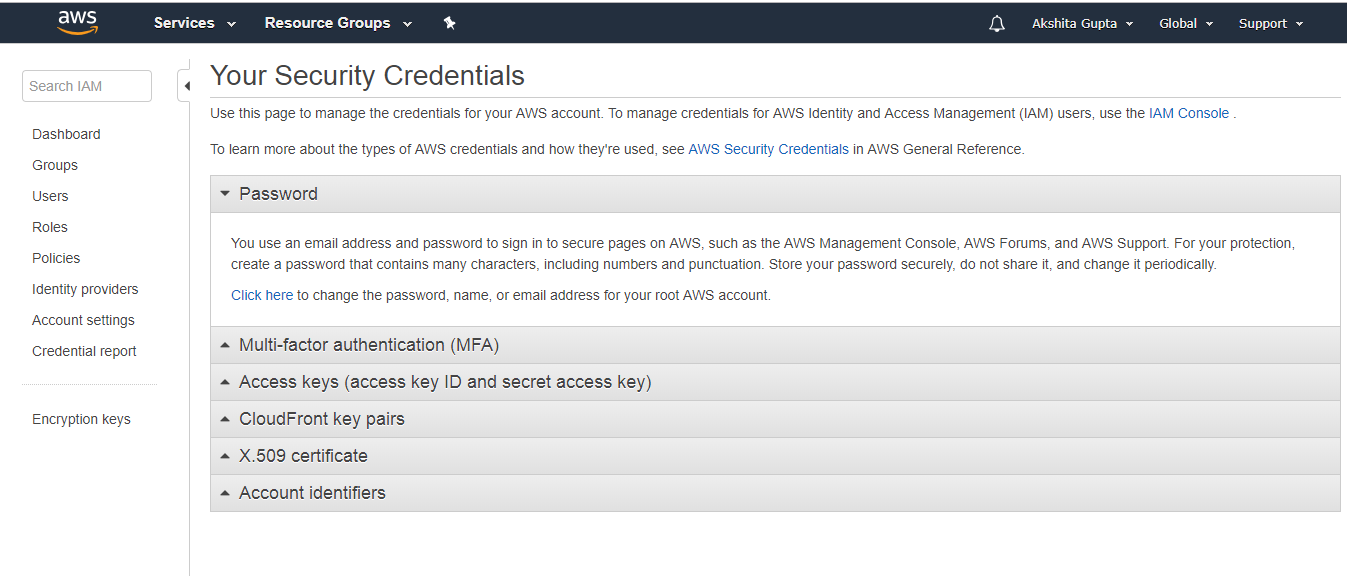
* A Canonical user ID is 64-digit hexadecimal encoded a 256-bit number.
* A canonical user ID is used in an Amazon S3 bucket policy for cross-account access means that AWS account can access the resources in another AWS account. For example, if you want AWS account access to your bucket, you need to specify the canonical user ID to your bucket's policy.

**Finding the canonical user ID**

* **Firstly, visit the website** [https://aws.amazon.com](https://aws.amazon.com/), and log in to the aws account by entering your email address and password.
* From the right side of the management console, click on the account name.



* Click on the **"My Security Credentials"** from the dropdown menu of the account name. The screen appears which is shown below:



#  Click on the Account identifiers to view the Canonical user ID. What is IAM?

* IAM stands for Identity Access Management.
* IAM allows you to manage users and their level of access to the aws console.
* It is used to set users, permissions and roles. It allows you to grant access to the different parts of the aws platform.
* AWS Identity and Access Management is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions in AWS.
* With IAM, Organizations can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.
* Without IAM, Organizations with multiple users must either create multiple user accounts, each with its own billing and subscriptions to AWS products or share an account with a single security credential. Without IAM, you also don't have control about the tasks that the users can do.
* IAM enables the organization to create multiple users, each with its own security credentials, controlled and billed to a single aws account. IAM allows the user to do only what they need to do as a part of the user's job.

## Features of IAM

* **Centralised control of your AWS account:** You can control creation, rotation, and cancellation of each user's security credentials. You can also control what data in the aws system users can access and how they can access.
* **Shared Access to your AWS account:** Users can share the resources for the collaborative projects.
* **Granular permissions:** It is used to set a permission that user can use a particular service but not other services.
* **Identity Federation:** An Identity Federation means that we can use Facebook, Active Directory, LinkedIn, etc with IAM. Users can log in to the AWS Console with same username and password as we log in with the Active Directory, Facebook, etc.
* **Multifactor Authentication:** An AWS provides multifactor authentication as we need to enter the username, password, and security check code to log in to the AWS Management Console.
* **Permissions based on Organizational groups:** Users can be restricted to the AWS access based on their job duties, for example, admin, developer, etc.
* **Networking controls:** IAM also ensures that the users can access the AWS resources within the organization's corporate network.
* **Provide temporary access for users/devices and services where necessary:** If you are using a mobile app and storing the data in AWS account, you can do this only when you are using temporary access.
* **Integrates with many different aws services:** IAM is integrated with many different aws services.
* **Supports PCI DSS Compliance:** PCI DSS (Payment Card Industry Data Security Standard) is a compliance framework. If you are taking credit card information, then you need to pay for compliance with the framework.
* **Eventually Consistent:** IAM service is eventually consistent as it achieves high availability by replicating the data across multiple servers within the Amazon's data center around the world.
* **Free to use:** AWS IAM is a feature of AWS account which is offered at no additional charge. You will be charged only when you access other AWS services by using IAM user.

