CHAPTER

13

Identity-as-a-Service

Overview

Employees in a company require to login into system to perform various tasks. These systems may be based on local server or cloud based. Following are the problems that an employee might face:

- Remembering different username and password combinations for accessing multiple servers.
- If an employee leaves the company, it's required to ensure that each of the user's account has been disabled. This increases workload on IT staff.

To solve above problems, a new technique emerged which is known as **Identity as a Service (IDaaS)**.

IDaaS offers management of identity (information) as a digital entity. This identity can be used during electronic transactions.

Identity

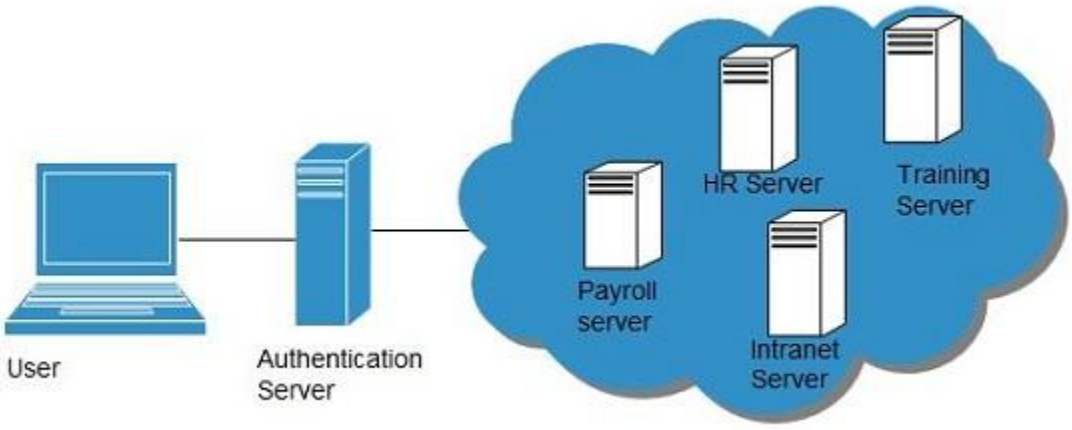
Identity refers to set of attributes associated with something and make it recognizable. All objects may have same attributes, but their identity cannot be the same. This unique identity is assigned through unique identification attribute.
There are several **identity services** that have been deployed to validate services such as validating web sites, transactions, transaction participants, client, etc. Identity as a Service may include the following:

- Directory Services
- Federated Services
- Registration
- Authentication Services
- Risk and Event monitoring
- Single sign-on services
- Identity and Profile management

Single Sign-On (SSO)

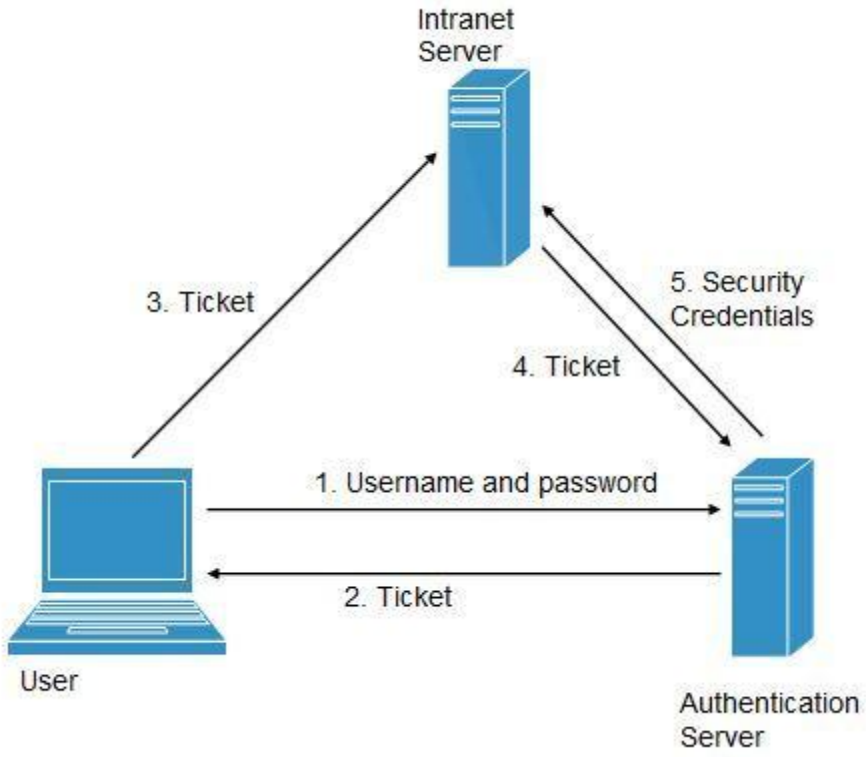
To solve the problem of using different username & password combination for different servers, companies now employ Single Sign-On software, which allows the user to login only one time and manages the user's access to other systems.

SSO has single authentication server, managing multiple accesses to other systems, as shown in the following diagram:



SSO WORKING

There are several implementations of SSO. Here, we will discuss the common working of SSO:



Following steps explain the working of Single Sign-On software:

1. User logs into the authentication server using a username and password.

2. The authentication server returns the user's ticket.

3. User sends the ticket to intranet server.

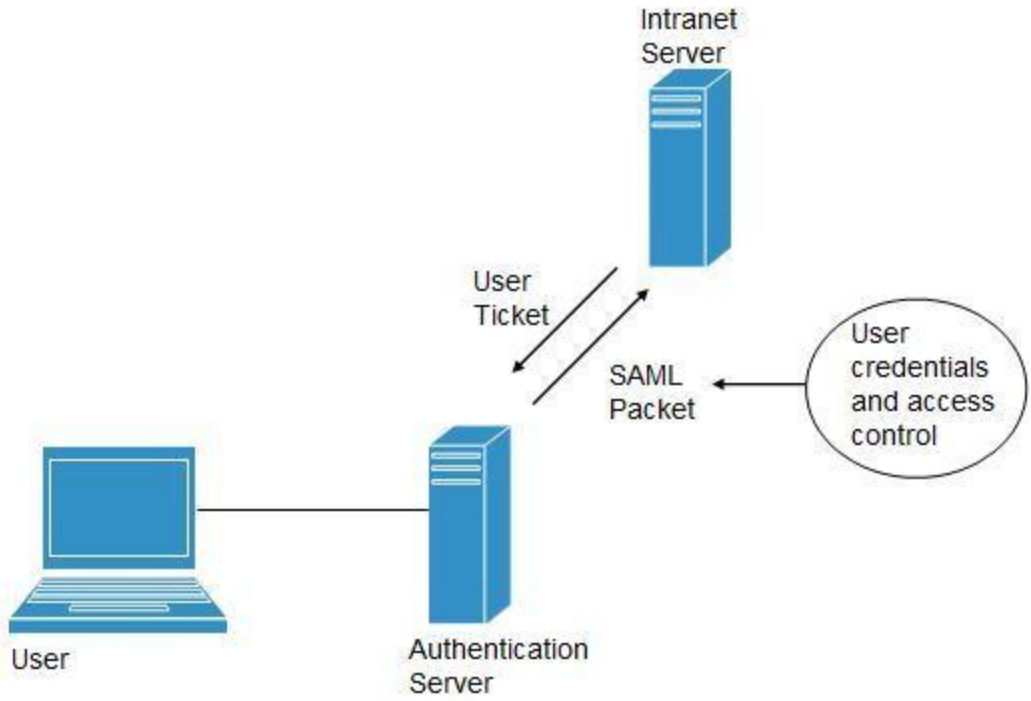
4. Intranet server sends the ticket to the authentication server.

5. Authentication server sends the user's security credentials for that server back to the intranet server.

If an employee leaves the company, then it just required to disable the user at the authentication server, which in turn disables the user's access to all the systems.

Federated Identity Management (FIDM)

FIDM describes the technologies and protocols that enable a user to package security credentials across security domains. It uses **Security Markup Language (SAML)** to package a user's security credentials as shown in the following diagram:



OpenID

It offers users to login into multiple websites with single account. Google, Yahoo!, Flickr, MySpace, WordPress.com are some of the companies that support OpenID.

Benefits

- Increased site conversation rates.
- Access to greater user profile content.
- Fewer problems with lost passwords.
- Ease of content integration into social networking sites.

CHAPTER

15

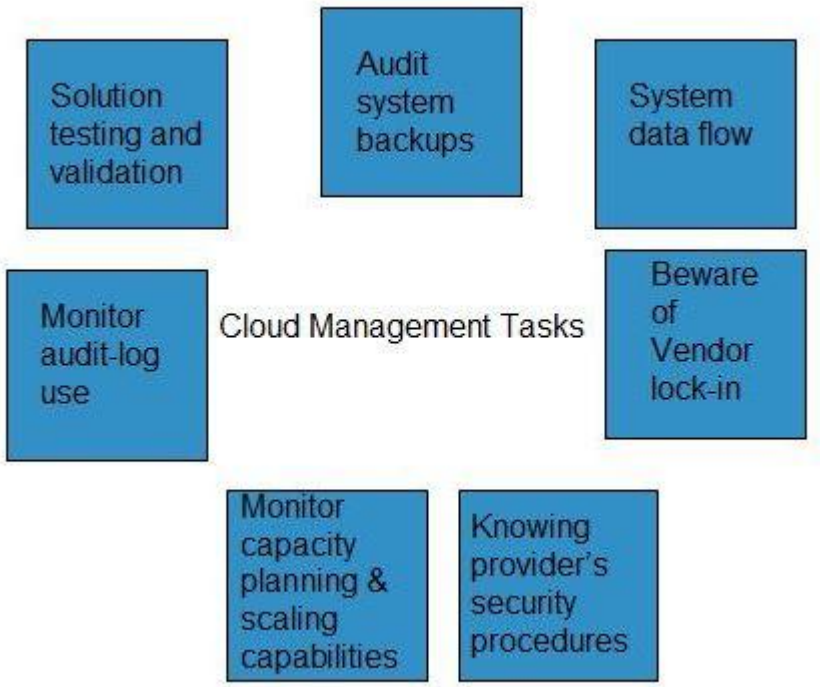
Cloud Computing Management

Overview

It is the responsibility of cloud provider to manage resources and their performance. Management may include several aspects of cloud computing such as **load balancing, performance, storage and backups, capacity, deployment** , etc. Management is required to access full functionality of resources in the cloud.

Cloud Management Tasks

Cloud Management involves a number of tasks to be performed by the cloud provider to ensure efficient use of cloud resources. Here, we will discuss some of these tasks:



AUDIT SYSTEM BACKUPS

It is required to timely audit the backups to ensure you can successfully restore randomly selected files of different users. Backups can be performed in following ways:

- Backing up files by the company, from on-site computers to the disks that reside within the cloud.
- Backing up files by the cloud provider.

It is necessary to know if cloud provider has encrypted the data, who has access to that data and if the backup is taken at different locations, you must know where.

SYSTEM'S DATA FLOW

The managers should develop a diagram describing a detailed process flow. This process flow will describe the movement of company's data throughout the cloud solution.

BEWARE OF VENDOR LOCK-IN

The managers must know the procedure to exit from services of a particular cloud provider. There must exist procedures, enabling the managers to export company's data to a file and importing it to another provider.

KNOWING PROVIDER'S SECURITY PROCEDURES

The managers should know the security plans of the provider for different services:

- Multitenant use
- E-commerce processing
- Employee screening
- Encryption policy

MONITOR CAPACITY PLANNING AND SCALING CAPABILITIES

The managers should know the capacity planning in order to ensure whether the cloud provider will meet the future capacity requirement for his business or not.

It is also required to manage scaling capabilities in order to ensure services can be scaled up or down as per the user need.

MONITOR AUDIT-LOG USE

In order to identify the errors in the system, managers must audit the logs on a regular basis.

SOLUTION TESTING AND VALIDATION

It is necessary to test the solutions provided by the provider in order to validate that it gives the correct result and is error-free. This is necessary for a system to be robust and reliable.

CHAPTER

18

Cloud Computing Security

Security in cloud computing is a major concern. Data in cloud should be stored in encrypted form. To restrict client from direct accessing the shared data, proxy and brokerage services should be employed.

Security Planning

Before deploying a particular resource to cloud, one should need to analyze several attributes about the resource such as:

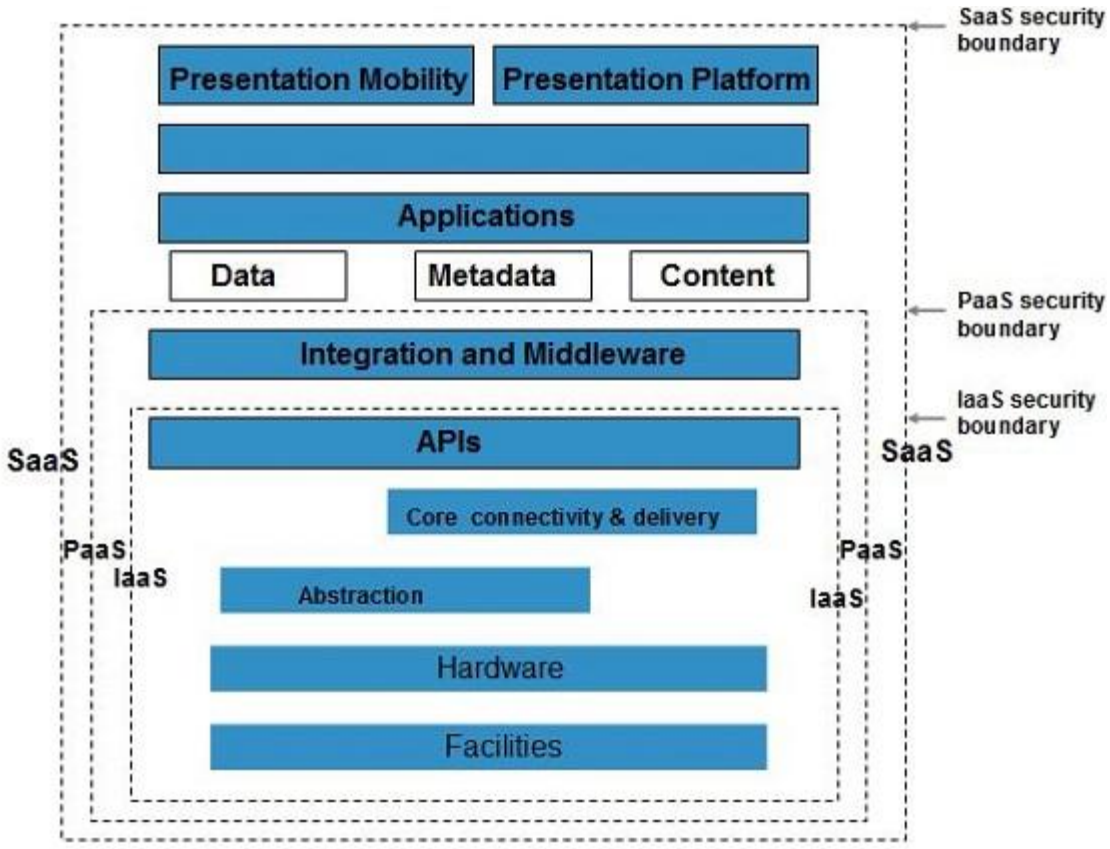
- Select which resources he is going to move to cloud and analyze its sensitivity to risk.
- Consider cloud service models such as **IaaS, PaaS**, and **SaaS**. These models require consumer to be responsible for security at different levels of service.
- Consider which cloud type such as **public, private, community** or **hybrid**.
- Understand the cloud service provider's system that how data is transferred, where it is stored and how to move data into and out of cloud.

Mainly the risk in cloud deployment depends upon the service models and cloud types.

Understanding Security of Cloud

SECURITY BOUNDARIES

A particular service model defines the boundary between the responsibilities of service provider and consumer. **Cloud Security Alliance (CSA)** stack model defines the boundaries between each service model and shows how different functional units relate to each other. The following diagram shows the**CSA stack model:**



KEY POINTS TO CSA MODEL:

- IaaS is the most basic level of service with PaaS and SaaS next two above levels of service.
- Moving upwards each of the service inherits capabilities and security concerns of the model beneath.
- IaaS provides the infrastructure, PaaS provides platform development environment and SaaS provides operating environment.
- IaaS has the least level of integrated functionalities and integrated security while SaaS has the most.
- This model describes the security boundaries at which cloud service provider's responsibility ends and the consumer's responsibilities begin.
- Any security mechanism below the security boundary must be built into the system and above should me maintained by the consumer.

Although each service model has security mechanism but security needs also depends upon where these services are located, in private, public, hybrid or community cloud.

UNDERSTANDING DATA SECURITY

Since all the data is transferred using Internet, data security is of major concern in cloud. Here are key mechanisms for protecting data mechanisms listed below:

- Access Control

- Auditing
- Authentication
- Authorization

All of the service models should incorporate security mechanism operating in all above-mentioned areas.

ISOLATED ACCESS TO DATA

Since data stored in cloud can be accessed from anywhere, therefore to protect the data, we must have a mechanism to isolate data from direct client access.

Brokered Cloud Storage Access is one of the approaches for isolating storage in cloud. In this approach, two services are created:

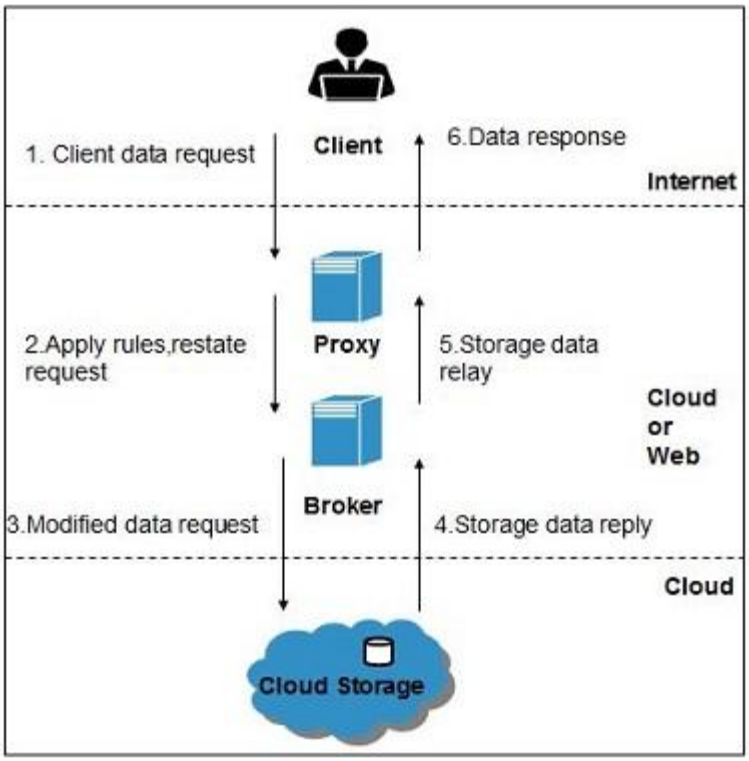
- A broker with full access to storage but no access to client.
- A proxy with no access to storage but access to both client and broker.

WORKING OF BROKERED CLOUD STORAGE ACCESS SYSTEM

When the client issue request to access data:

- The client data request goes to proxy's external service interface.
- The proxy forwards the request to the broker.
- The broker requests the data from cloud storage system.
- The cloud storage system returns the data to the broker.
- The broker returns the data to proxy.
- Finally the proxy sends the data to the client.

All of the above steps are shown in the following diagram:



Encryption

Encryption helps to protect data from being compromised. It protects data that is being transferred as well as data stored in the cloud. Although encryption helps to protect data from any unauthorized access, it does not prevent from data loss.

CHAPTER

19

Cloud Computing Operations

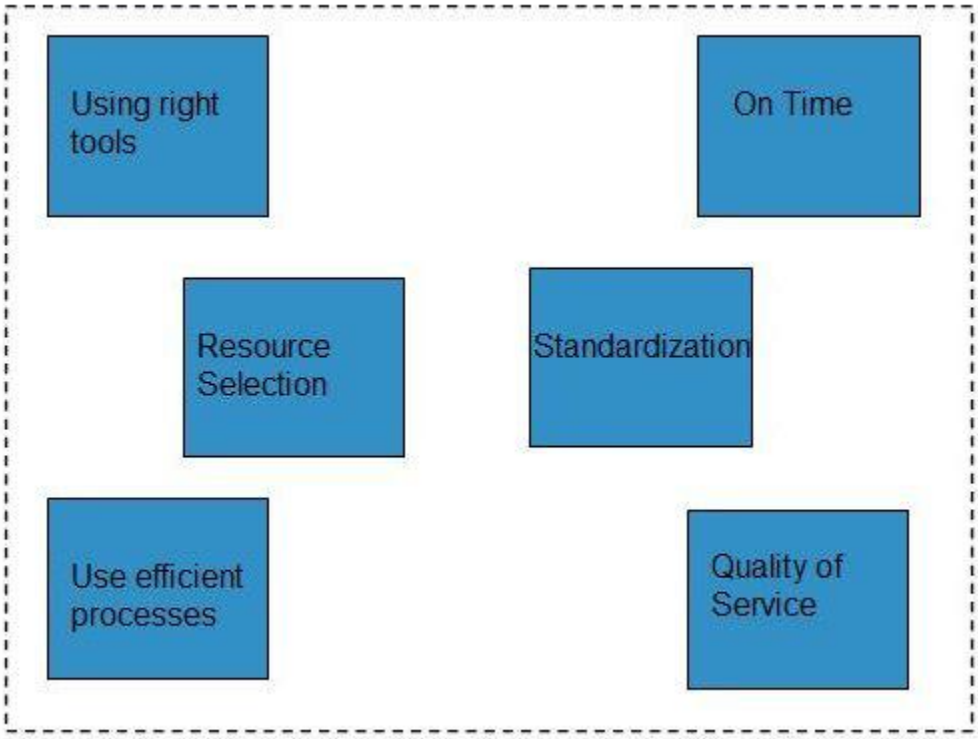
Overview

Cloud Computing operation refers to delivering superior cloud service. Today, cloud computing operations have become very popular and widely employed by many of the organizations just because it allows to perform all business operations over the Internet.

These operations can be performed using a web application or mobile based applications. There are a number of operations that are performed in cloud, some of them are shown in the following diagram:

Managing Cloud Operations

There are several ways to manage day-to-day cloud operations, as shown in the following diagram:



- Always employ right tools and resources to perform any function in the cloud.
- Things should be done at right time and at right cost.
- Selecting an appropriate resource is mandatory for operation management.
- The process should be standardized and automated to avoid repetitive tasks.
- Using efficient process will eliminate the waste and redundancy.
- One should maintain the quality of service to avoid re-work later.

CHAPTER

20

Cloud Computing Applications

Cloud Computing has its applications in almost all the fields such as **business, entertainment, data storage, social networking, management, entertainment, education, art** and **global positioning system**, etc. Some of the widely famous cloud computing applications are discussed here in this tutorial:

Business Applications

Cloud computing has made businesses more collaborative and easy by incorporating various apps such as **MailChimp, Chatter, Google Apps for business**, and **Quickbooks**.

SN	Application Description
1	**MailChimp** It offers an **e-mail publishing platform.** It is widely employed by the businesses to design and send their e-mail campaigns.
2	**Chatter** **Chatter app** helps the employee to share important information about organization in real time. One can get the instant feed regarding any issue.
3	**Google Apps for Business** **Google** offers **creating text documents, spreadsheets, presentations**, etc., on **Google Docs**which allows the business users to share them in collaborating manner.
4	**Quickbooks** It offers **online accounting solutions** for a business. It helps in **monitoring cash flow, creating VAT returns** and **creating business reports**.

Data Storage and Backup

Box.com, Mozy, Joukuu are the applications offering data storage and backup services in cloud.

SN	Application Description
1	**Box.com** **Box.com** offers drag and drop service for files. It just required to drop the files into Box and access from anywhere.
2	**Mozy** **Mozy** offers online backup service for files during a data loss.
3	**Joukuu**

	Joukuu is a web-based interface. It allows to display a single list of contents for files stored in**Google Docs, Box.net and Dropbox**.

Management Applications

There are apps available for management task such as **time tracking, organizing notes**. Applications performing such tasks are discussed below:

SN	Application Description
1	**Toggl** It helps in tracking time period assigned to a particular project.
2	**Evernote** Evernote is an application that organizes the sticky notes and even can read the text from images which helps the user to locate the notes easily.
3	**Outright** It is an accounting app. It helps to track income, expenses, profits and losses in real time.

Social Applications

There are several social networking services providing websites such as Facebook, Twitter, etc.

SN	Application Description
1	**Facebook** **Facebook** offers social networking service. One can share photos, videos, files, status and much more.
2	**Twitter** **Twitter** helps to interact directly with the public. One can follow any celebrity, organization and any person, who is on twitter and can have latest updates regarding the same.

Entertainment Applications

SN	Application Description
1	**Audiobox.fm** It offers streaming service, i.e., music can be stored online and can be played from cloud using service's own media player.

Art Applications

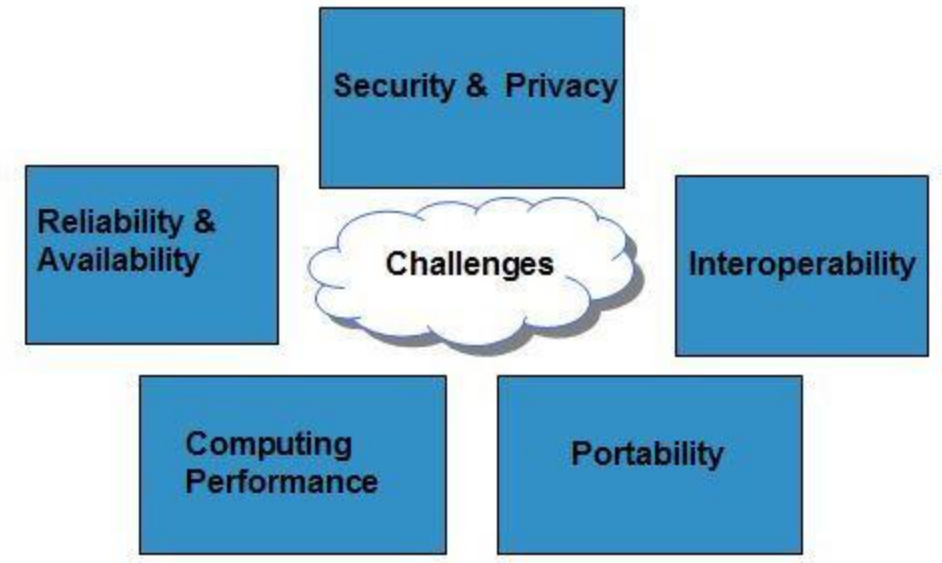
SN	Application Description
1	**Moo** It offers art services such as designing and printing **business cards, postcards** and **minicards.**

CHAPTER

22

Cloud Computing Challenges

Cloud Computing, an emergence technology, has placed many challenges in different aspects. Some of these are shown in the following diagram:



SECURITY & PRIVACY

Security and Privacy of information is the biggest challenge to cloud computing. Security and privacy issues can be overcome by employing encryption, security hardware and security applications.

PORTABILITY

This is another challenge to cloud computing that applications should easily be migrated from one cloud provider to another. There should not be vendor lock-in. However, it is not yet made possible because each of the cloud provider uses different standard languages for their platforms.

INTEROPERABILITY

Application on one platform should be able to incorporate services from other platform. It is made possible via web services. But writing such web services is very complex.

COMPUTING PERFORMANCE

To deliver data intensive applications on cloud requires high network bandwidth, which results in high cost. If done at low bandwidth, then it does not meet the required computing performance of cloud application.

RELIABILITY AND AVAILABILITY

It is necessary for cloud systems to be reliable and robust because most of the businesses are now becoming dependent on services provided by third-party.

CHAPTER

23

Mobile Cloud Computing

CloudComputing offers such smartphones that have rich Internet media experience and require less processing, less power. In term of Mobile Cloud Computing, processing is done in cloud, data is stored in cloud. And the mobile devices serve as a media for display.

Today smartphones are employed with rich cloud services by integrating applications that consume web services. These web services are deployed in cloud.

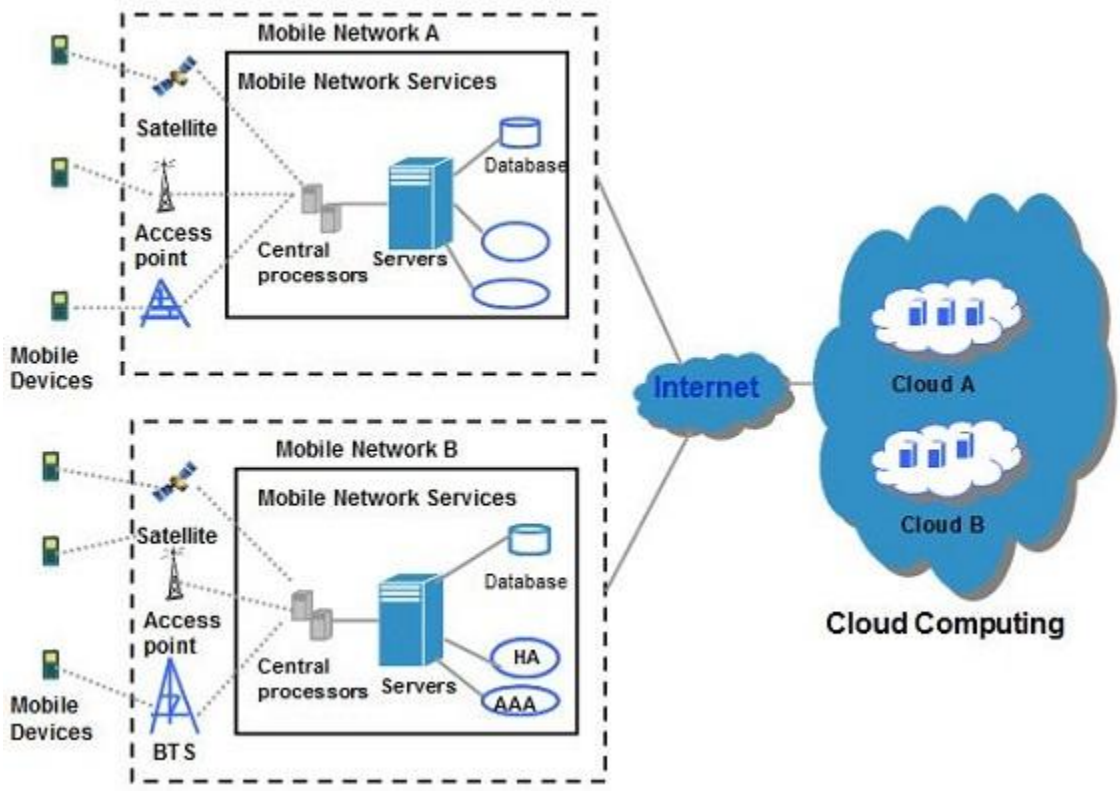
There are several Smartphone operating systems available such as **Google's Android, Apple's iOS, RIM BlackBerry, Symbian,** and **Windows Mobile Phone**. Each of these platforms support third-party applications that are deployed in cloud.

Architecture

MCC includes four types of cloud resources:

- Distant mobile cloud
- Distant immobile cloud
- Proximate mobile computing entities
- Proximate immobile computing entities
- Hybrid

The following diagram shows the framework for mobile cloud computing architecture:



Issues

Despite of having significant development in field of mobile computing, there still exists many issues:

EMERGENCY EFFICIENT TRANSMISSION

There should be a frequent transmission of information between cloud and the mobile devices.

ARCHITECTURAL ISSUES

Mobile cloud computing is required to make architectural neutral because of heterogeneous environment.

LIVE VM MIGRATION

It is challenging to migrate an application, which is resource-intensive to cloud and to execute it via Virtual Machine.

MOBILE COMMUNICATION CONGESTION

Due to continuous increase demand for mobile cloud services, the workload to enable smooth communication between cloud and mobile devices has been increased.