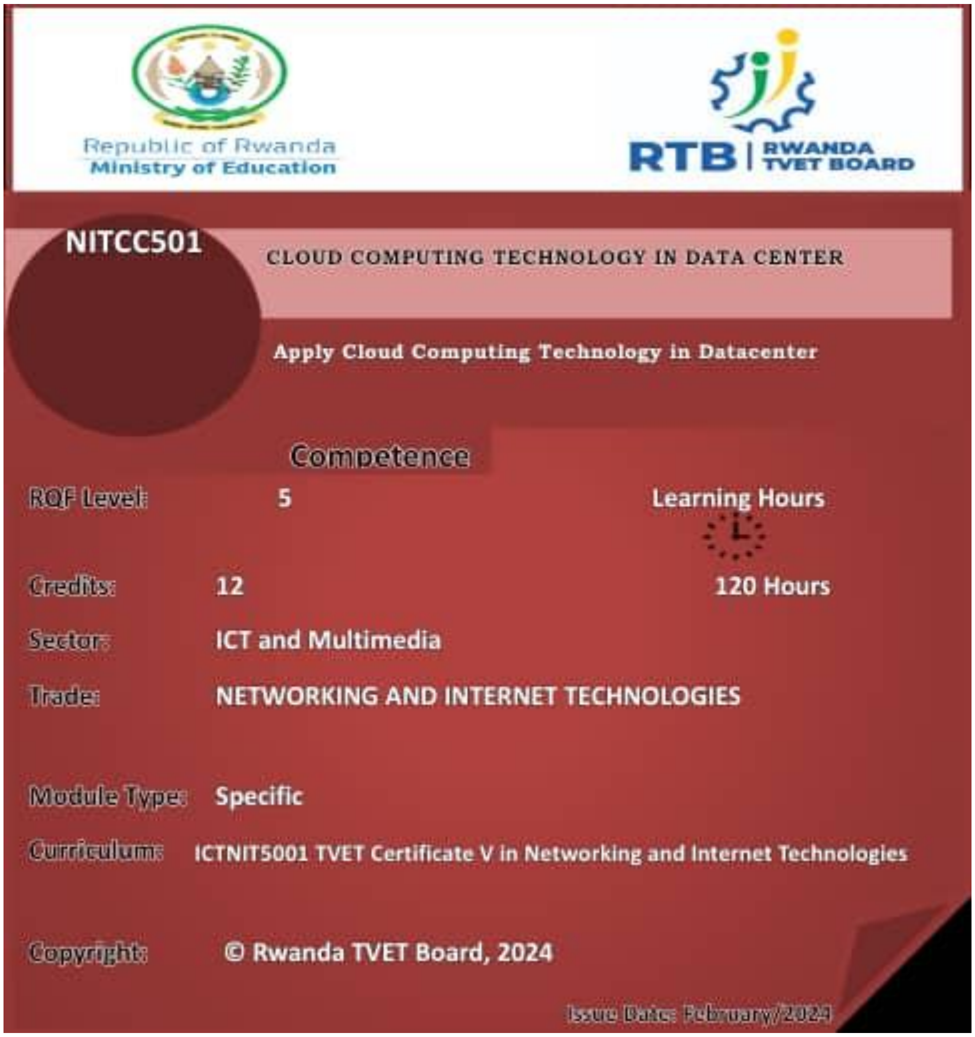
Learning outcomes



Republic of Rwanda
Ministry of Education

RTB | RWANDA TVET BOARD

NITCC501

CLOUD COMPUTING TECHNOLOGY IN DATA CENTER

Apply Cloud Computing Technology in Datacenter

Competence

RQF Level: 5

Learning Hours

Credits: 12

120 Hours

Sector: ICT and Multimedia

Trade: NETWORKING AND INTERNET TECHNOLOGIES

Module Type: Specific

Curriculum: ICTNIT5001 TVET Certificate V in Networking and Internet Technologies

Copyright: © Rwanda TVET Board, 2024

Issue Date: February/2024

At the end of the module the learner will be able to:

1. Consume cloud service model
2. Prepare Data center environment
3. Configure on-premises Data center
4. Connect on-premises Data center to cloud network

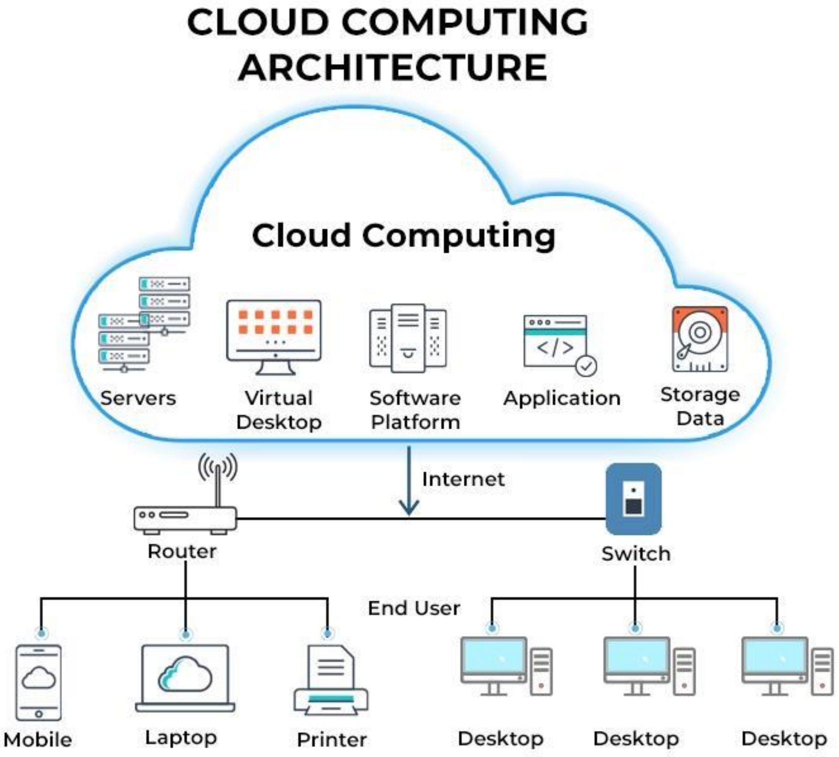
Learning outcome 1: Consume cloud service model

a. **Selection of cloud computing technology**

1.1 Introduction to Cloud Computing

1.1.1 **Definition:** Cloud computing is defined as the use of hosted services, such as data storage, servers, databases, networking, and software over the internet.

The data is stored on physical servers, which are maintained by a cloud service provider. Computer system resources, especially data storage and computing power, are available on-demand, without direct management by the user in cloud computing.



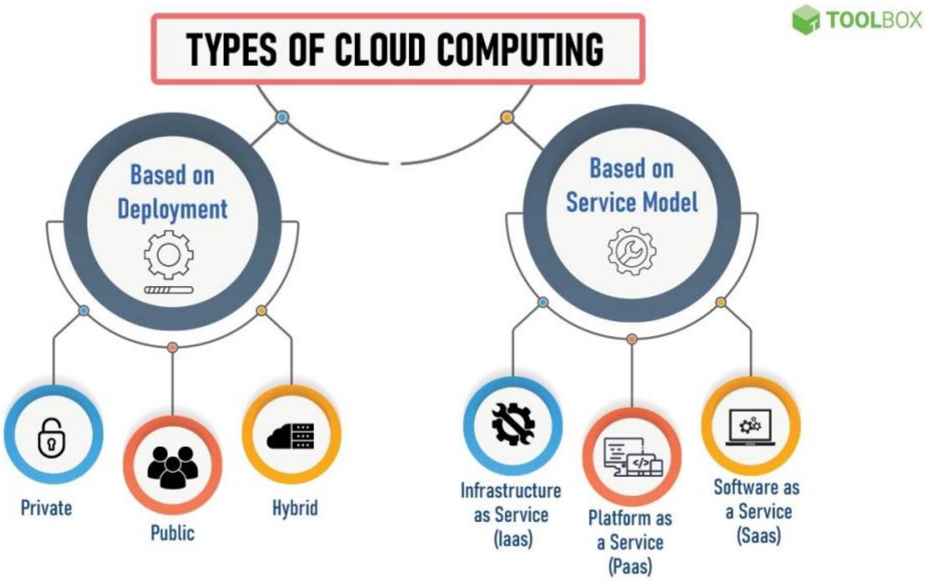
Instead of storing files on a storage device or hard drive, a user can save them on cloud, making it possible to access the files from anywhere, as long as they have access to the web. The services hosted on cloud can be broadly divided into infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS). Based on the deployment model, cloud can also be classified as public, private, and hybrid cloud.

Further, cloud can be divided into two different layers, namely, front-end and back-end. The layer with which users interact is called the front-end layer. This layer enables a user to access the data that has been stored in cloud through cloud computing software.

The layer made up of software and hardware, i.e., the computers, servers, central servers, and databases, is the back-end layer. This layer is the primary component of cloud and is entirely responsible for storing information securely. To ensure seamless connectivity between devices linked via cloud computing, the central servers use a software called middlewareOpens a new window that acts as a bridge between the database and applications.

1.1.2 Types of Cloud Computing

Cloud computing can either be classified based on the deployment model or the type of service. Based on the specific deployment model, we can classify cloud as public, private, and hybrid cloud. At the same time, it can be classified as infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) based on the service the cloud model offers.



Types of Cloud Computing

Private cloud

In private cloud, organization owns and manages its own infrastructure, which is not shared with other organizations. Private clouds are a good option for organizations that need exclusive control and security, and for businesses in highly regulated industries.

Also termed internal, enterprise, or corporate cloud, a private cloud is usually managed via internal resources and is not accessible to anyone outside the organization. Private cloud computing provides all the benefits of a public cloud, such as self-service, scalability, and elasticity, along with additional control, security, and customization.
Private clouds provide a higher level of security through company firewalls and internal hosting to ensure that an organization's sensitive data is not accessible to third-party providers. The drawback of private cloud, however, is that the organization becomes responsible for all the management and maintenance of the data centers, which can prove to be quite resource-intensive.

Public cloud

An external provider manages the infrastructure, which is shared among multiple customers. Public clouds are a good option for businesses looking for scalability and flexibility without a large initial investment.

Public cloud refers to computing services offered by third-party providers over the internet. Unlike private cloud, the services on public cloud are available to anyone who wants to use or purchase them. These services could be free or sold on-demand, where users only have to pay per usage for the CPU cycles, storage, or bandwidth they consume.

Hybrid cloud

Hybrid cloud uses a combination of public and private cloud features. The "best of both worlds" cloud model allows a shift of workloads between private and public clouds as the computing and cost requirements change. When the demand for computing and processing fluctuates, hybrid cloud allows businesses to scale their on-premises infrastructure up to the public cloud to handle the overflow while ensuring that no third-party data centers have access to their data.

In a hybrid cloud model, companies only pay for the resources they use temporarily instead of purchasing and maintaining resources that may not be used for an extended period. In short, a hybrid cloud offers the benefits of a public cloud without its security risks.

Based on the service model, cloud can be categorized into IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service), and SaaS (Software-as-a-Service).

Infrastructure as a service (IaaS)

Infrastructure as a service or IaaS is a type of cloud computing in which a service provider is responsible for providing servers, storage, and networking over a virtual interface. In this service, the user doesn't need to manage the cloud infrastructure but has control over the storage, operating systems, and deployed applications.
Instead of the user, a third-party vendor hosts the hardware, software, servers, storage, and other infrastructure components. The vendor also hosts the user's applications and maintains a backup.

Platform as a service (PaaS)

Platform as a service or PaaS is a type of cloud computing that provides a development and deployment environment in cloud that allows users to develop and run applications without the complexity of building or maintaining the infrastructure. It provides users with resources to develop cloud-based applications. In this type of service, a user purchases the resources from a vendor on a pay-as-you-go basis and can access them over a secure connection.

PaaS doesn't require users to manage the underlying infrastructure, i.e., the network, servers, operating systems, or storage, but gives them control over the deployed applications. This allows organizations to focus on the deployment and management of their applications by freeing them of the responsibility of software maintenance, planning, and resource procurement.

Software as a service (SaaS)

SaaS or software as a service allows users to access a vendor's software on cloud on a subscription basis.

In this type of cloud computing, users don’t need to install or download applications on their local devices. Instead, the applications are located on a remote cloud network that can be directly accessed through the web or an API.

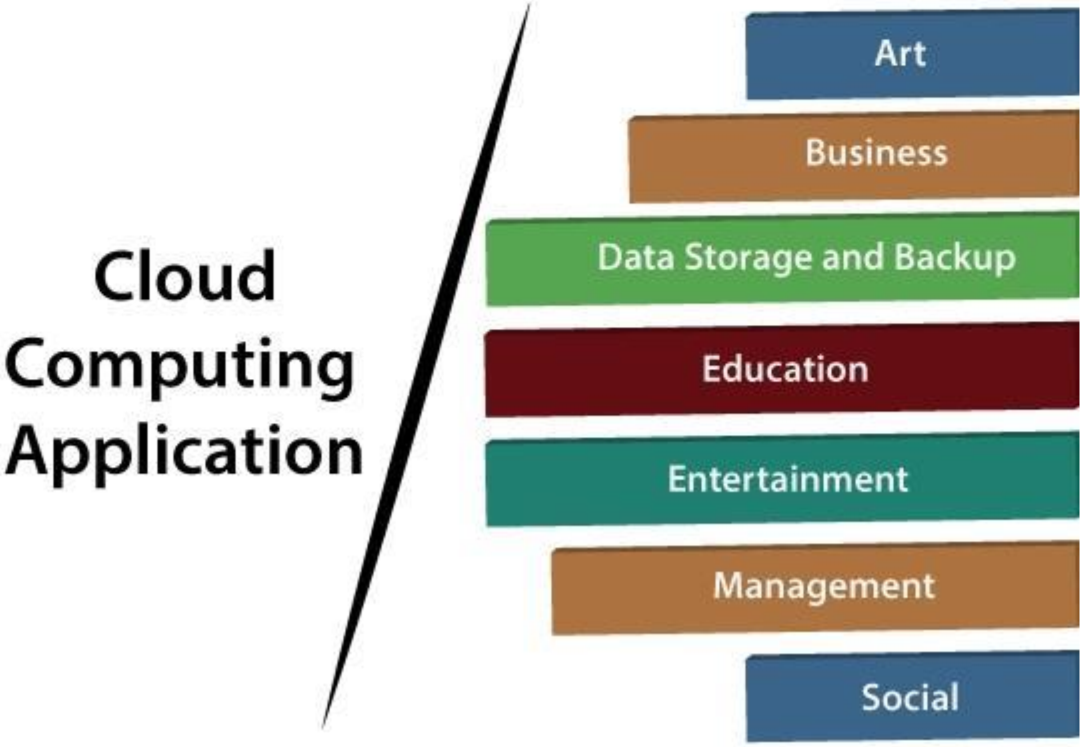
In the SaaS model, the service provider manages all the hardware, middleware, application software, and security. Also referred to as ‘hosted software’ or ‘on-demand software’, SaaS makes it easy for enterprises to streamline their maintenance and support.

Ex: Google Docs, DropBox.

1.1.3 **Cloud Computing Applications**

Cloud service providers provide various applications in the field of art, business, data storage and backup services, education, entertainment, management, social networking, etc.

The most widely used cloud computing applications are given below –



1. Art Applications

Cloud computing offers various art applications for quickly and easily design **attractive cards, booklets,** and **images**.

Examples: Adobe Creative Cloud , Moo, etc…

2. Business Applications

Business applications are based on cloud service providers. Today, every organization requires the cloud business application to grow their business. It also ensures that business applications are 24*7 available to users.

There are the following business applications of cloud computing –

I. Paypal

Paypal offers the simplest and easiest **online payment** mode using a secure internet account. Paypal accepts the payment through debit cards, credit cards, and also from Paypal account holders.

Ii. Salesforce

Salesforce platform provides tools for sales, service, marketing, e-commerce, and more. It also provides a cloud development platform.

3. Data Storage and Backup Applications

Cloud computing allows us to store information (data, files, images, audios, and videos) on the cloud and access this information using an internet connection. As the cloud provider is responsible for providing security, so they offer various backup recovery application for retrieving the lost data.

Example: Google G Suite, Box.com.

4. Education Applications

Cloud computing in the education sector becomes very popular. It offers various **online distance learning platforms** and **student information portals** to the students. The advantage of using cloud in the field of education is that it offers strong virtual classroom environments, Ease of accessibility, secure data storage, scalability, greater reach for the students, and minimal hardware requirements for the applications.

Example: Amazon Web Services (AWS) in education, Chromebooks for education.

5. Entertainment Applications

Entertainment industries use a **multi-cloud strategy** to interact with the target audience. Cloud computing offers various entertainment applications such as online games and video conferencing

Example: Video conferencing Apps, Online games apps (Playstation plus).

6. Management Applications

Cloud computing offers various cloud management tools which help admins to manage all types of cloud activities, such as resource deployment, data integration, and disaster recovery. These management tools also provide administrative control over the platforms, applications, and infrastructure.

Some important management applications are –

I. Toggl
II. Evernote
III. Got meeting

7. Social Applications

Social cloud applications allow a large number of users to connect with each other using social networking applications such as **Facebook, X (**former **Twitter), Linkedln,** etc.

1.1.4 Advantages and Disadvantages of Cloud Computing

The most important reason why cloud computing is growing rapidly is the various advantages it offers.

Accessibility: Users can access information from any device, time and location, including clients and customers.

Collaboration: Users can share information with others, making it easier to collaborate on projects.

Cost savings: Cloud computing can replace fixed expenses with variable expenses and reduce the need to run and maintain data centers.

Data security: Cloud software can help protect data from threats, and cloud providers are responsible for fixing security issues.

Faster time to market: Developers can quickly spin up or retire instances to accelerate development.

Higher performance: Cloud computing can increase input/output operations per second (IOPS).

Scalability: Cloud computing can scale to meet demand.

Virtualized computing: Cloud computing can offer virtualized computing.

Now let's move on to discuss some challenges of cloud computing.

- **Downtime:** Almost every cloud user will tell you that outages tops their list of cloud computing challenges. At times, cloud service providers may get overwhelmed due to the huge number of clients they provide services to each day. This may lead to technical outages, due to which your applications may temporarily experience some downtime.

- **Internet connection dependency:** A user may not be able to access the data on cloud without a good internet connection and a compatible device. Moreover, using public Wi-Fi to access your files could pose a threat if the right security measures are not taken.

- **Financial commitment:** Cloud providers use a pay-as-you-go pricing model. However, businesses need to give a monthly or annual financial commitment for most subscription plans. This needs to be factored into their operating costs.

- **Security risks:** Even if your cloud service provider promises you that they have the most reliable security certifications, there's always a chance of losing your data. With hackers increasingly targeting cloud storage to gain access to sensitive business data, this might be an even greater concern, for which the appropriate measures need to be taken.

- **Limited access:** A user may have minimal control since the cloud service provider owns and manages the infrastructure. The user would only be able to manage applications and not the backend infrastructure.

1.2 Identification of service models

- **Identification of business needs**

Identifying business needs and requirements is a crucial step in any project or initiative. It helps you define the problem, scope, objectives, benefits, and solutions of your business case.

When identifying business needs for cloud computing, you can consider things like:

Scalability: How your business will scale its needs.

Data storage and processing: How your business will store and process data.

Security and compliance: How your business will protect data and comply with regulations.

Cost optimization: How your business will optimize costs.

AI/ML capabilities: What AI and ML capabilities your business needs.

Digital transformation: How your business's cloud use will align with its digital transformation strategy.

Business continuity: How your business will reduce downtime and improve business continuity.

Storage capacity: Whether your business is running out of storage capacity.

End-of-life technology: Whether your business's current systems and technology are reaching end-of-life.

1.3Existing System Analysis

Existing System Analysis is the process of examining an existing system to understand its components, functions, and how it operates. This analysis is crucial before any modifications, upgrades, or replacements are made.

Benefits of Existing System Analysis:

1. **Improved Understanding:** Gain a deeper understanding of the system's strengths, weaknesses, and limitations.
2. **Informed Decision Making:** Make informed decisions about system modifications, upgrades, or replacements.
3. **Reduced Risks:** Identify potential risks and challenges associated with changes to the system.
4. **Optimized Resources:** Allocate resources more effectively by identifying areas for improvement.
5. **Enhanced User Experience:** Improve the user experience by addressing pain points and inefficiencies.

Effective existing system analysis is essential for successful system development and maintenance.

System Analysis involves :

I. Legal compliance

Legal compliance involves ensuring that the system being developed, conducted or modified adheres to all relevant laws and regulations. This is particularly important for systems that handle sensitive data, such as personal information, financial data, or medical records.

II. Technical

Technical system analysis refers to the aspects of the system that relate to its design, development, and implementation. It encompasses the hardware, software, and other technical components that make up the system.

III. Financial

Financial system analysis refers to the monetary aspects of the system, including its costs, benefits, and return on investment (ROI).

IV. Security

Security system analysis refers to the measures taken to protect the system from unauthorized access, use, disclosure, disruption, modification, or destruction.

Security is a critical aspect of system analysis, as it can help to protect the system's data, reputation, and operations. By carefully considering security in the design and development of a system, organizations can reduce the risk of security breaches and ensure the confidentiality, integrity, and availability of their information.

Security is an ongoing process that requires constant attention and effort. By prioritizing security in system analysis, organizations can protect their systems and data from threats and build trust with their customers.

B. Selection of Cloud computing service provider

1. Identification of Cloud computing service provider

Cloud computing service provider is a company that delivers cloud computing services to its customers. These services allow organizations to access computing resources, such as servers, storage, and software, over the internet, rather than having to maintain their own physical infrastructure.

Identification of Cloud computing service provider involves evaluating various cloud service providers to determine the best fit for your organization's specific needs.

This process requires considering factors such as the services offered, deployment model, pricing model, security and compliance, scalability and performance, global reach, cu

stomer support, reputation, pricing, and future roadmap.

By carefully considering these factors, you can identify a cloud service provider that offers the right combination of features, benefits, and value for your organization.

2. Selection Criteria

Selection criteria for cloud computing service provider:

- **Technical consideration**

Considering technical factors, such as:

A. **Performance**: Evaluate the provider's performance metrics, such as CPU, memory, storage, and network performance.
B. **Scalability**: Assess the provider's ability to scale resources up or down as needed to meet changing demands.
C. **Interoperability**: Ensure that the provider's services are compatible with your existing systems and applications.
D. **Security**: Evaluate the provider's security measures, such as data encryption, access controls, and disaster recovery plans.
E. **Compliance**: Ensure that the provider complies with relevant industry standards and regulations, such as HIPAA, GDPR, or PCI DSS.
F. **Support**: Assess the provider's level of customer support, including availability, response time, and knowledge base.

By carefully considering these technical factors, you can select a cloud computing service provider that meets your organization's specific needs and provides a reliable and secure platform for your applications.

- **Strategic Consideration**

Strategic considerations when selecting a cloud computing service provider:

A. **Alignment with business goals:** Ensure that the cloud service provider aligns with your organization's overall business goals and strategy.
B. **Long-term vision:** Consider the provider's long-term vision and roadmap to ensure that they can meet your future needs.
C. **Innovation**: Evaluate the provider's commitment to innovation and their ability to stay ahead of the curve.
D. **Vendor lock-in:** Be aware of the potential for vendor lock-in and ensure that you have the flexibility to switch providers if necessary.
E. **Exit strategy:** Develop an exit strategy in case you need to move away from the cloud provider in the future.

By considering these strategic factors, you can select a cloud computing service provider that supports your organization's long-term success.

- ❖ **Pricing Plan**

Pricing plans when selecting a cloud computing service provider:

A. **Pay-as-you-go:** Pay only for the resources you use, on a per-hour or per-minute basis. This is a flexible option for organizations with unpredictable workloads.
B. **Reserved instances:** Discounted pricing long-term commitments. This is a good option for organizations with predictable workloads.
C. **Subscription-based:** Pay a fixed monthly or annual fee for a set of resources. This is a good option for organizations with consistent workloads.

When evaluating pricing plans, consider the following factors:

I. **Your organization's workload:** Determine whether your workload is predictable or unpredictable.
II. **Your budget:** Consider your overall budget and the level of cost savings you need to achieve.
III. **Hidden fees:** Be aware of potential hidden fees, such as data transfer fees or support fees.
IV. **Compare costs:** Compare Pricing costs across different providers and plans.

By carefully evaluating these factors, you can select a pricing plan that best meets your organization's needs and budget.

Creation of customer's account

1. Registration of customer

Customer registration is the process of collecting and verifying information from customers to establish a formal relationship with them.

It typically involves creating a customer account, providing essential information, and setting up preferences for future interactions.

Key purposes of customer registration:

a. **Establish a relationship:** Create a formal connection with the customer.

b. **Collect information:** Gather essential customer data for marketing, sales, and support purposes.
c. Provide a platform: Offer a platform for customer interactions, transactions, and communication.

Common steps in customer registration:

I. **Data collection:** Gather necessary information, such as name, contact details, shipping address, payment information, etc.
II. **Account verification:** Verify the collected data to ensure accuracy and prevent fraudulent registrations.
III. **Account creation:** Create a unique customer account with login credentials and preferences.
IV. **Welcome message:** Send a personalized welcome message to the customer.

Example:

A customer creates an account on an e-commerce website. They provide their name, email address, shipping address, and payment information. The website verifies their email address and sends a confirmation link. Once the account is created, the customer receives a welcome email with their login credentials and a link to their account dashboard.

2. Setting of Bills

During the customer registration process, a customer is asked to provide their billing name, address, and payment method. They select credit card as their preferred payment method and enter their card details. The system stores the payment information securely and sets the billing frequency to monthly. The customer will receive invoices via email on the first day of each month.

Purpose:

- Establish billing information for future transactions.
- Ensure accurate and timely invoicing.
- Enable efficient payment processing.

Key Steps:

I. **Billing Information Collection:**

- Gather necessary details: Billing name, address, payment method, tax information.

- Validate information for accuracy.

II. **Payment Method Setup:**

- Allow customers to choose preferred payment methods: Credit card, debit card, bank transfer, etc.
- Store payment information securely.

III. **Billing Frequency:**

- Determine billing frequency: Monthly, quarterly, annually.
- Consider customer preferences and business needs.

IV. **Invoice Delivery:**

- Choose delivery method: Email, physical mail, online portal.

Designation of an administrator

Refers to a process of granting administrative privileges to manage servers, networks, and users accounts to a **System Administrator.**

The Administrator is granted specific permissions to create, modify, and delete user accounts, install software, and troubleshoot system issues.

Purpose:

- Grant administrative privileges to a user or group.
- Allow for efficient management of system resources and access controls.
- Ensure proper oversight and accountability.

Use of Service models

Infrastructure as a service (IaaS)

Infrastructure as a Service (IaaS) is a cloud computing model that provides virtualized computing resources, such as servers, storage, and networking, over the internet.

IaaS providers manage the underlying hardware and infrastructure, allowing customers to focus on building and running their applications.

Key benefits of IaaS:

I. **Flexibility**: Scale resources up or down as needed to meet changing demands.
II. **Cost-effectiveness:** Pay only for the resources you use, on a pay-as-you-go basis.
III. **Reduced maintenance:** No need to manage physical infrastructure, such as servers and data centers.
IV. **Improved performance:** Benefit from high-performance infrastructure and advanced technologies.

Examples of IaaS providers:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)
- IBM Cloud
- Oracle Cloud Infrastructure (OCI)

- **Customize configuration settings**

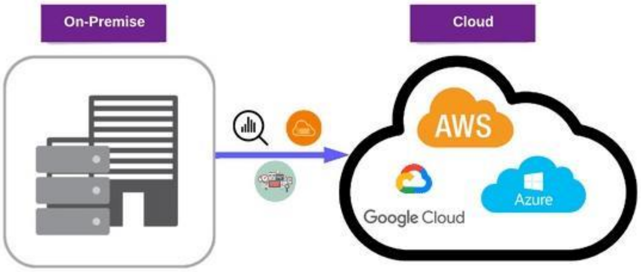
Refer to a process of modifying software or hardware default settings according to your preferences.

The purpose is to enhance your software or hardware experience.

- **Data Migration and integration**

I. **Data Migration**

The process of moving data from one system to another, usually for purposes like system upgrades, system consolidation, or the adoption of new technologies, is known as **data migration.**



Types of Data Migration

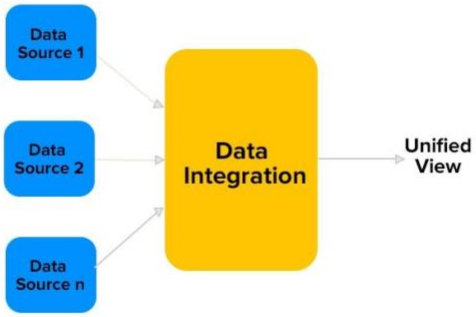
1. **Storage migration** is the process of transferring data between various formats or storage systems, sometimes requiring hardware changes.
2. **Data migration** between various database management systems (DBMS) or versions is known as database migration.
3. **Cloud migration** is the process of transferring data between multiple cloud providers or from on-premises systems to cloud-based platforms.
4. **Application migration** is the process of moving data from one application to another.
5. **Platform migration** is the process of transferring data across several technological platforms, such as switching between operating systems.

Tools and Technologies

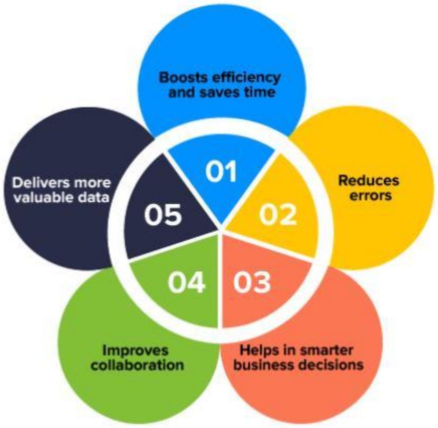
AWS Database movement Service, Azure Data Factory, and open-source tools like Apache NiFi are just a few of the solutions that make data movement easier.

II. Data Integration

Data Integration is the process of combining data from different sources into a single and unified view.



Why is data Integration important?


01
Boosts efficiency and saves time
02
Reduces errors
03
Helps in smarter business decisions
04
Improves collaboration
05
Delivers more valuable data

- **Implement security measures**

Cloud computing has revolutionized the way businesses operate, offering unparalleled flexibility, scalability, and cost efficiency. However, this shift to cloud environments brings new security challenges. Ensuring robust security in cloud computing is crucial to protect sensitive data and maintain trust. Here are the top security measures essential for safeguarding cloud infrastructures.

1. Data Encryption

Data encryption is a fundamental security measure for protecting information both in transit and at rest. By converting data into a coded format, encryption ensures that even if unauthorized users gain access, they cannot read the data without the decryption key.

- In Transit Encryption: Protects data as it moves between the user and the cloud service provider. Using protocols like TLS (Transport Layer Security) ensures data integrity and privacy during transmission.

- At Rest Encryption: Safeguards stored data on cloud servers. Many cloud providers offer encryption services that manage keys for users or allow them to manage their own keys, ensuring data remains secure even if physical security is compromised.

2. Identity and Access Management (IAM)

Effective IAM is critical for controlling who can access cloud resources and what actions they can perform. It involves defining and managing user roles and permissions to ensure that only authorized individuals have access to sensitive information.

- Multi-Factor Authentication (MFA): Adds an extra layer of security by requiring users to provide two or more verification factors to gain access.

- Role-Based Access Control (RBAC): Assigns permissions to users based on their role within the organization, minimizing the risk of unauthorized access.

3. Regular Security Audits and Compliance

Regular security audits and compliance checks help ensure that cloud infrastructure adheres to industry standards and regulations. This proactive approach identifies vulnerabilities and enforces best practices.

- Automated Monitoring Tools: Tools like AWS CloudTrail and Azure Security Center continuously monitor cloud environments for suspicious activities and policy violations.

- Compliance Standards: Adhering to standards such as GDPR, HIPAA, and ISO/IEC 27001 ensures that cloud services meet legal and regulatory requirements.

4. Data Loss Prevention (DLP)

DLP strategies are designed to prevent unauthorized access and leakage of sensitive data. By monitoring, detecting, and blocking potential data breaches, DLP protects intellectual property and personal information.

- DLP Software: Tools that classify sensitive data and enforce policies to prevent unauthorized sharing or movement of data outside the organization.

- Regular Backups: Ensuring regular and secure backups helps recover data in case of accidental deletion, corruption, or ransomware attacks.

5. Network Security

Securing the network layer is crucial to prevent unauthorized access and attacks on cloud infrastructure. Implementing robust network security measures helps protect data integrity and availability.

- Firewalls and Intrusion Detection Systems (IDS): Firewalls control incoming and outgoing traffic based on security rules, while IDS monitor and analyze network traffic for signs of potential threats.

- Virtual Private Networks (VPNs): Securely connect remote users to cloud resources, ensuring encrypted communication channels over public networks.

6. **Patch management:** Keep software up-to-date with security patches.

Conclusion

Securing Cloud Computing environments requires a multi-faceted approach that addresses various potential vulnerabilities. By implementing robust data encryption, effective IAM, regular security audits, DLP strategies, and network security measures, organizations can significantly enhance their cloud security posture. Staying vigilant and proactive in adopting these security measures is essential for protecting sensitive data and maintaining the trust of customers and stakeholders in the increasingly cloud-dependent business landscape.

- **Monitor performance and usage**

Monitoring performance and usage is the process of managing and evaluating the performance, availability, and the usage of cloud based infrastructure.

Platform as a service (PaaS)

- **Deploy application**

Deploying an application, also known as platform deployment, is the process of making an application available for use by end-users. This involves a number of steps, including:

Preparation: Gathering and packaging the code, configuration files, and other resources

Testing: Identifying and fixing bugs and errors

Deployment: Transferring the application's code and configurations from the staging environment to the live production environment

Monitoring: Analyzing the application's performance

Application deployment is a critical phase in the application development lifecycle. It ensures that the application is accessible and functional for its intended users.

- **Customize and configure**

Customizing and configuring a cloud application involves modifying or enhancing a cloud service to meet specific business needs.

Customization: Modifying or enhancing a product to meet desired objectives.

Configuration: Altering a solution to change runtime behavior and attributes.

Here are some ways to customize and configure cloud applications:

Zscaler

Add a custom cloud application by:

1. **Entering the application's name**
2. **Selecting the application's status**
3. **Choosing the application's risk index**
4. **Selecting the application's tags**
5. **Entering the application's URLs or IP addresses**
6. **Adding a description**

- **Monitor and optimize performance**

To monitor and optimize the performance of a cloud application, you need to actively track key metrics like response time, error rates, resource utilization (CPU, memory, network), database query performance, and user interactions, using cloud monitoring tools to identify bottlenecks and proactively implement adjustments to your infrastructure and application code to ensure optimal performance and user experience

Key steps involved:

1. Identify Critical Metrics:

- **Application level:**

Response time: Average time taken to process a request.

Throughput: Number of requests processed per unit time.

Error rate: Percentage of failed requests.

User interaction time: Time taken for users to complete specific actions.

- **Infrastructure level:**

CPU usage: Percentage of CPU capacity utilized.

Memory usage: Amount of RAM consumed

Disk I/O: Read/write operations on storage

Network bandwidth: Data transfer rate

Database query latency: Time taken for database queries to execute

2. Choose Monitoring Tools:

Cloud provider monitoring services:

Most cloud platforms (AWS, Azure, GCP) offer built-in monitoring tools to track resource usage and application performance within their environment.

Software as a service

- **Cloud Software deploymen**t

Software deployment in the cloud is the process of making an application available through a cloud-based platform, such as Amazon Web Services (AWS), Google Cloud Platform (GCP), or Microsoft Azure. It involves deploying code to a remote server that can be accessed over the internet.

Cloud deployment can offer many benefits, including: scalability, reliability, security, and cost-effectiveness.

Why cloud computing, what problems we had that cloud computing comes to solve?