CLOUD COMPUTING

Dr. D Muhammad Noorul Mubarak

Head, Department of Computer Science,

University of Kerala

Module IV

Cloud Management

- **Cloud computing management** is maintaining and controlling the cloud services and resources be it public, private or hybrid.
- Some of its aspects include load balancing, performance, storage, backups, capacity, deployment etc.
- To do so a cloud managing personnel needs full access to all the functionality of resources in the cloud.
- Different software products and technologies are combined to provide a cohesive cloud management strategy and process.

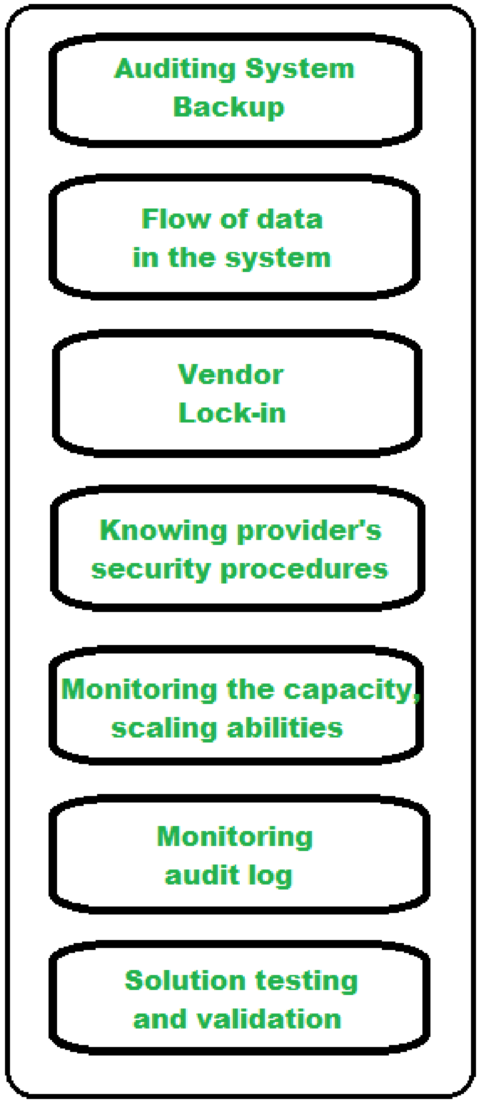
Cloud Management

- Private infrastructure is operated only for a single organization, so that can be managed by the organization or by a third party.
- Public cloud services are delivered over a network that is open and available for public use.
- In this model, the IT infrastructure is owned by a private company and members of the public can purchase or lease data storage or computing capacity as needed.
- Hybrid cloud environments are a combination of public and private cloud services from different providers.
- Most organizations store data on private cloud servers for privacy concerns, while leveraging public cloud applications at a lower price point for less sensitive information.
- The combination of both the public and private cloud are known as Hybrid cloud servers.

Why Cloud Management

- Cloud is nowadays preferred by huge organizations as their primary data storage.
- A small downtime or an error can cause a great deal of loss and inconvenience for the organizations.
- So as to design, handle and maintain a cloud computing service specific members are responsible who make sure things work out as supposed and all arising issues are addressed.

Cloud Management Task



Auditing System Backup

Flow of data in the system

Vendor Lock-in

Knowing provider's security procedures

Monitoring the capacity, scaling abilities

Monitoring audit log

Solution testing and validation

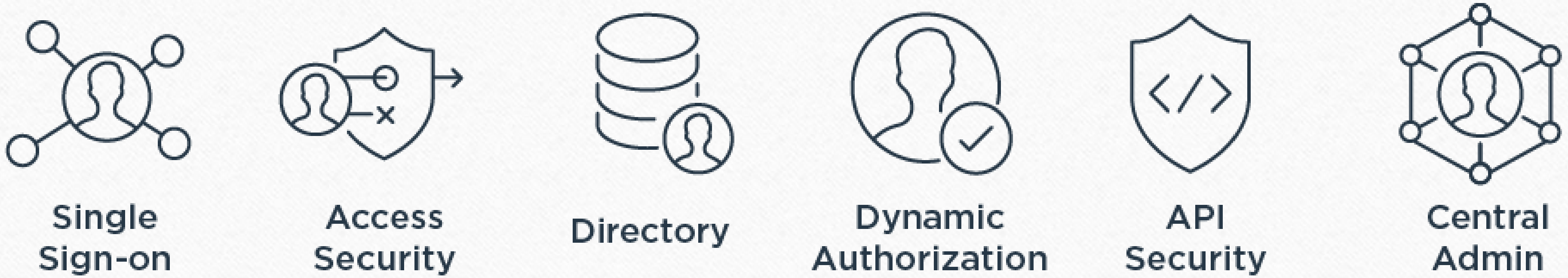
Cloud Management Task

- **Auditing System Backups:** It is required to audit the backups from time to time to ensure restoration of randomly selected files of different users. This might be done by the organization or by the cloud provider.
- **Flow of data in the system:** The managers are responsible for designing a data flow diagram that shows how the data is supposed to flow throughout the organization.
- **Vendor Lock-In:** The managers should know how to move their data from a server to another in case the organization decides to switch providers.
- **Knowing provider's security procedures :** The managers should know the security plans of the provider, especially Multitenant use, E-commerce processing, Employee screening and Encryption policy.
- **Monitoring the Capacity, Planning and Scaling abilities :** The manager should know if their current cloud provider is going to meet their organization's demand in the future and also their scaling capabilities.
- **Monitoring audit log :** In order to identify errors in the system, logs are audited by the managers on a regular basis.
- **Solution Testing and Validation :** It is necessary to test the cloud services and verify the results and for error-free solutions.

Cloud IAM (Identity Access Management)

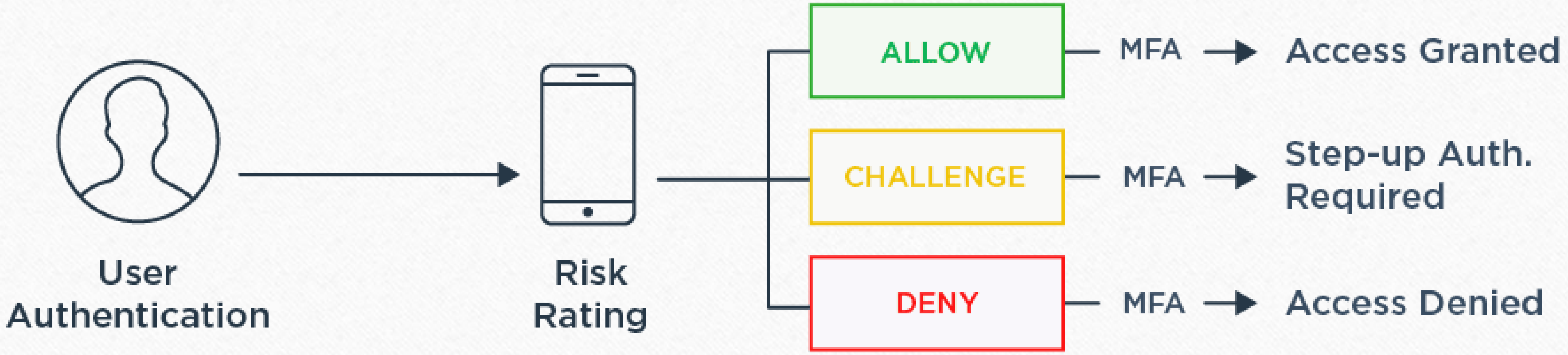
- Authentication and access control are two of the capabilities of identity and access management solutions.
- Cloud IAM allows you to authenticate users no matter where they are and secure access to resources across cloud, SaaS, on-prem and APIs, all the while increasing your speed, agility and efficiency.
- IAM solutions are available for customers, employees and partners, and can be integrated to provide a complete solution for your enterprise.

The Full Range of IAM Capabilities



Authentication Management

- Ensuring an individual is who they claim to be isn't a new concept.
- Banks require proof of identity in order for customers to withdraw money and bartenders require youthful looking customers to verify they are old enough to buy alcohol.
- Authentication takes that process online, with multiple forms of proof required for increased security.



Authentication Management

- Multi-factor authentication (MFA) uses two or more authentication factors to verify a user's identity, and encompasses two-factor authentication (2FA).
  - Authentication factors include something you know, something you are, and something you have.
  - MFA and 2FA both provide layers of security to protect a user's account from hackers who may have guessed, stolen or bought passwords or primary credentials.
  - For a high-value transaction, an enterprise using MFA could require a password (something you know), a one-time passcode sent to a smartphone or email (something you have), and a fingerprint scan on the smartphone (something you are).
  - If any of these actions are not correctly completed, access is denied.

Authentication Management

- Single sign-on (SSO), used in conjunction with MFA, gives users the ability to sign on once with their verified credentials to gain access to multiple services and resources.
    - SSO combined with adaptive authentication lets you match authentication requirements to the access being requested, stepping up authentication requirements where needed, like a login from a high-risk IP address.

Access Control

- Access management makes sure the right people are granted access to the right resources and nothing more.
- Even verified users can pose a threat to an enterprise, so following the principle of least privilege ensures access is limited to just what is needed by a user to safeguard sensitive information.
- For example, you don’t want customers to have access to employee-only resources or give all employees access to personnel files maintained by the HR department.

Cloud Computing Contracts

- When purchased as a service, cloud computing is highly cost effective as it is based on pay-per-use.
- It has the potential to slash user IT expenditure and optimise use of digital technologies throughout the economy.
- Making full use of the cloud could deliver 2.5 million extra jobs in Europe and add around 1% a year to EU GDP by 2020.
- **How can contracts promote cloud computing?**
  - Unfortunately, consumers and companies are often reluctant to take advantage of cloud computing services either because contracts are unclear or are unbalanced in favour of service providers.
  - Existing regulations and national contract laws may not always be adapted to cloud-based services. Protection of personal data in a cloud environment also needs to be addressed.
  - Adapting contract law is therefore an important part of the Commission's cloud computing strategy.
- **Safe and fair contracts for cloud computing**
  - The Commission is working towards cloud computing contracts that contain safe and fair terms and conditions for all parties.
  - On 18 June 2013, the Commission set up a group of experts to define safe and fair conditions and identify best practices for cloud computing contracts.
  - The Commission also performed studies on cloud computing contracts to explore these issues.

Disaster Recovery

- Data is the most valuable asset of modern-day organizations.
- Its loss can result in irreversible damage to your business, including the loss of productivity, revenue, reputation, and even customers.
- It is hard to predict when a disaster will occur and how serious its impact will be.
- However, what you can control is the way you respond to a disaster and how successfully your organization will recover from it.

Disaster Recovery

- **How does disaster recovery in cloud computing differ from traditional disaster recovery?**
  - – Traditional disaster recovery involves building a remote disaster recovery (DR) site, which requires constant maintenance and support on your part. In this case, data protection and disaster recovery are performed manually, which can be a time-consuming and resource-intensive process.
  - Disaster recovery in cloud computing entails storing critical data and applications in cloud storage and failing over to a secondary site in case of a disaster. Cloud computing services are provided on a pay-as-you-go basis and can be accessed from anywhere and at any time. Backup and disaster recovery in cloud computing can be automated, requiring minimum input on your part.

Disaster Recovery

- **How does disaster recovery works in cloud computing?**
  - Creating, testing, and updating a DR plan can prepare your organization for an unexpected disaster and ensure safety and continuity for your business.
  - A comprehensive DR plan should take into account your infrastructure, potential threats and vulnerabilities, most critical assets and the order of their recovery, and workable DR strategies.
  - Integration of cloud computing services in disaster recovery allows you to design a DR plan and automate each step of the recovery process.

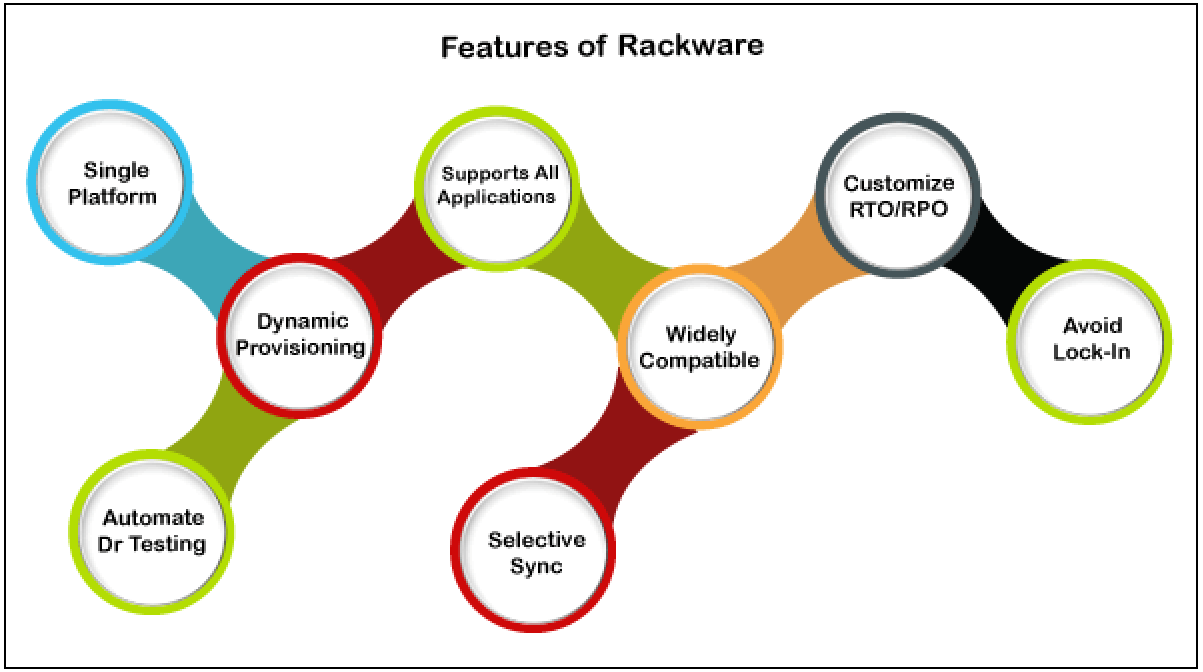
Disaster Recovery

- Cloud computing is the on-demand delivery of computing services over the internet (more often referred to as 'the cloud') which operates on a pay-as-you-go basis. Cloud computing vendors generally provide access to the following services:
    - Infrastructure as a service (IaaS) allows you to rent IT infrastructure, including servers, storages and network component, from the cloud vendor.
    - Platform as a service (PaaS) allows you to rent a computing platform from the cloud provider for developing, testing, and configuring software applications.
    - Software as a service (SaaS) allows you to access software applications which are hosted on the cloud.

Disaster Management

- Rackware evolves cloud management technology that helps businesses relocate implementations, offer additional disaster recovery and fallback, and cloud storage management.

- The RackWare Management Module (RMM) offers Information systems adaptability to companies by streamlining disaster recovery and fallback to any server. Several of the features are discussed as follows:



Disaster Recovery Plan

- A cloud-based disaster recovery plan typically follows three key stages
  - analysis, implementation, and testing.
- **Analysis**
  - The analysis phase of your disaster recovery plan should include a comprehensive risk assessment, as well as impact analysis of your existing IT infrastructure and workloads. Once you have identified all of these risks, you can identify potential disasters and vulnerabilities.
  - Once you collected all of this information you can evaluate how your current infrastructure stands against these challenges, and determine the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) of your workloads.

Disaster Recovery Plan

- Implementation
  - The implementation phase of a DR plan helps you outline the steps and technologies needed to address disasters as they occur. The goal is to lay out a plan that helps you implement all necessary measures and respond in a timely manner. Here are four key steps of a DR implementation:
  - **Preparedness—**a detailed plan explaining how to respond during events, including clear roles and responsibilities.
  - **Prevention—**measures taken to reduce potential threats and vulnerabilities. Typically includes regular updates and employee training.
  - **Response—**manual and automated measures implemented to ensure quick response during disasters.
  - **Recovery—**manual and automated measures that quickly recover the data needed for normal operations.

Disaster Recovery Plan

- Testing
  - To ensure the viability of your plan, you need to test and update it on a regular basis.
  - This can help you ensure your staff remain properly trained and that the plan remains relevant to your needs.
  - You should also ensure that all technologies and automated processes are working properly and are ready to be used at all times.
  - Additionally, you can leverage testing to detect gaps and update your plan accordingly.