Cloud Computing Unit 4

Inter Cloud Resource Management

Contents

- What is inter cloud?
- Types of inter cloud resource management
- What is resource provisioning?
- Resource Provisioning Types
- Parameters for resource Provisioning
- Global Exchange of Cloud Resources

Inter cloud

- **Cloud based services are a growing** business trend in the IT industry, where **service providers** establish cloud and **offer computing resources (Infrastructure, Platform and Software) to consumers**.
- Consumers often require computing resources across multiple regions, to address their application needs. **Single cloud provider may not be able to address such requests** due to lack of presence or capacity in multiple regions.
- This blueprint proposes a solution to address this concern by introducing a concept of **Inter Cloud Resource Federation** (a.k.a. Alliance). Using this technical approach **multiple cloud entities can work in alliance to form a bigger cloud entity with massive resource capacities.**

Contd…

- The Inter-Cloud is **an interconnected global "cloud of clouds" and an extension of the Internet "network of networks" on which it is based.**
- Inter-Cloud computing is **interconnecting multiple cloud providers' infrastructures.**
- To provide cloud services as utility successfully, **interconnected clouds are required** and interoperability and portability are important factors in Inter-Cloud.

What is inter cloud?

- The idea behind an inter cloud is that a single common functionality would combine many different individual clouds into one seamless mass in terms of on-demand operations.
- Cloud hosting is largely intended **to deliver on-demand ser**vices. Through careful use of **scalable** and highly engineered technologies, cloud providers are able to offer customers the ability to change their levels of service in many ways without waiting for physical changes to occur.

What is inter cloud?

- Terms like **rapid elasticity**, **resource pooling and on-demand self-service are already part of cloud** hosting service designs that are set up to make sure the customer or client never has to deal with limitations or disruptions.
- **Building on all of these ideas, the inter cloud would simply make sure that a cloud could use resources beyond its reach by taking advantage of pre-existing contracts with other cloud providers.**

Need of Inter-Cloud

- The limitations of cloud are that they **have limited physical resources**. **If a cloud has exhausted all the computational and storage resources, it cannot provide service to the clients.** The **Inter-Cloud addresses such situations where each cloud would use the computational, storage, or any kind of resource of the infrastructures of other clouds.**
- The Inter-Cloud environment provides benefits like diverse Geographical locations, better application resilience and avoiding vendor lock-in to the cloud client.
- **Benefits for the cloud provider are expand-on-demand and better service level agreements (SLA) to the cloud client.**

Types of inter cloud resource management

1. Federation Clouds

2. Multi-Cloud

Federation Clouds: A Federation cloud is an Inter-Cloud where a set of **cloud providers willingly interconnect their cloud infrastructures in order to share resources among each other.**

- **The cloud providers in the federation voluntarily collaborate to exchange resources.** This type of Inter-Cloud is suitable for collaboration of governmental clouds (Clouds owned and utilized by nonprofit institution or government) or private cloud portfolios (Cloud is a part of a portfolio of clouds where the clouds belong to the **same organization** for example all IITs federation). Types of federation clouds are Peer to Peer and Centralized clouds.

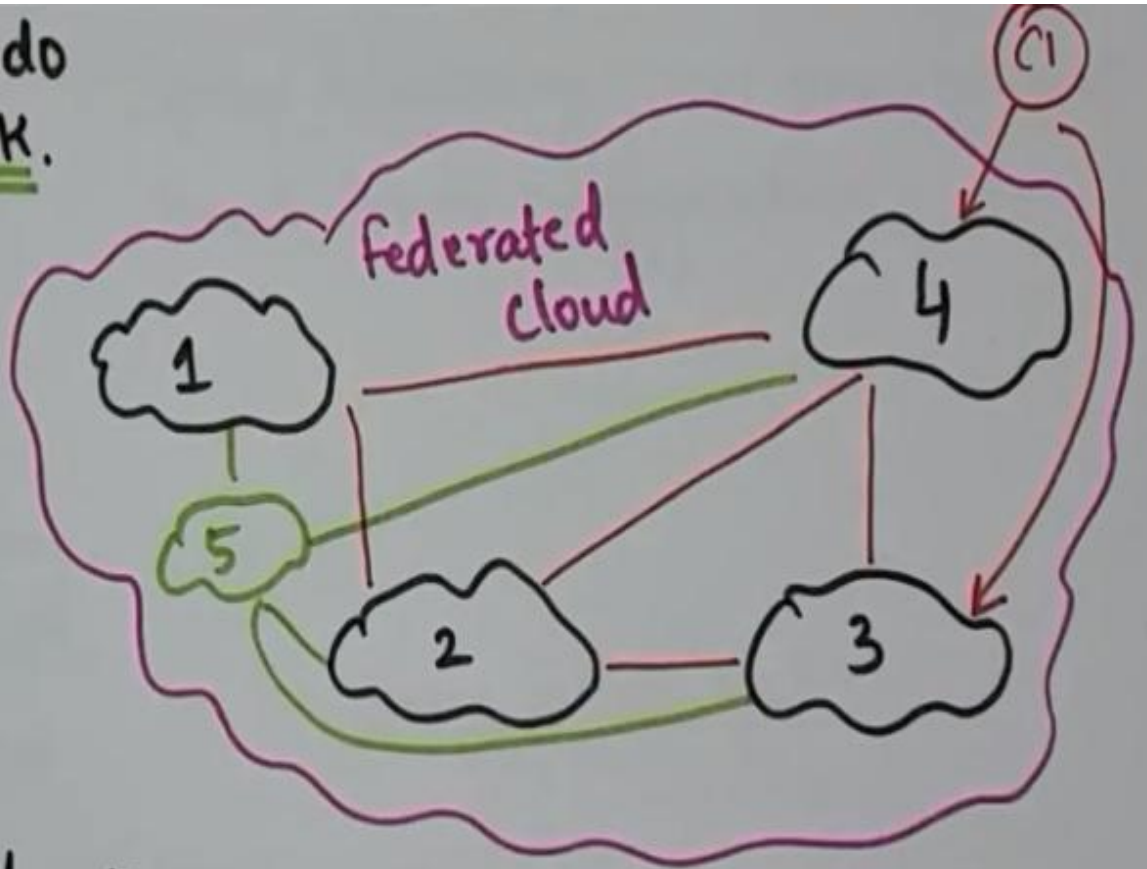
Federation Clouds

Federated Cloud: union of Small parts that do Common work.

↳ Also called Cloud Federation.

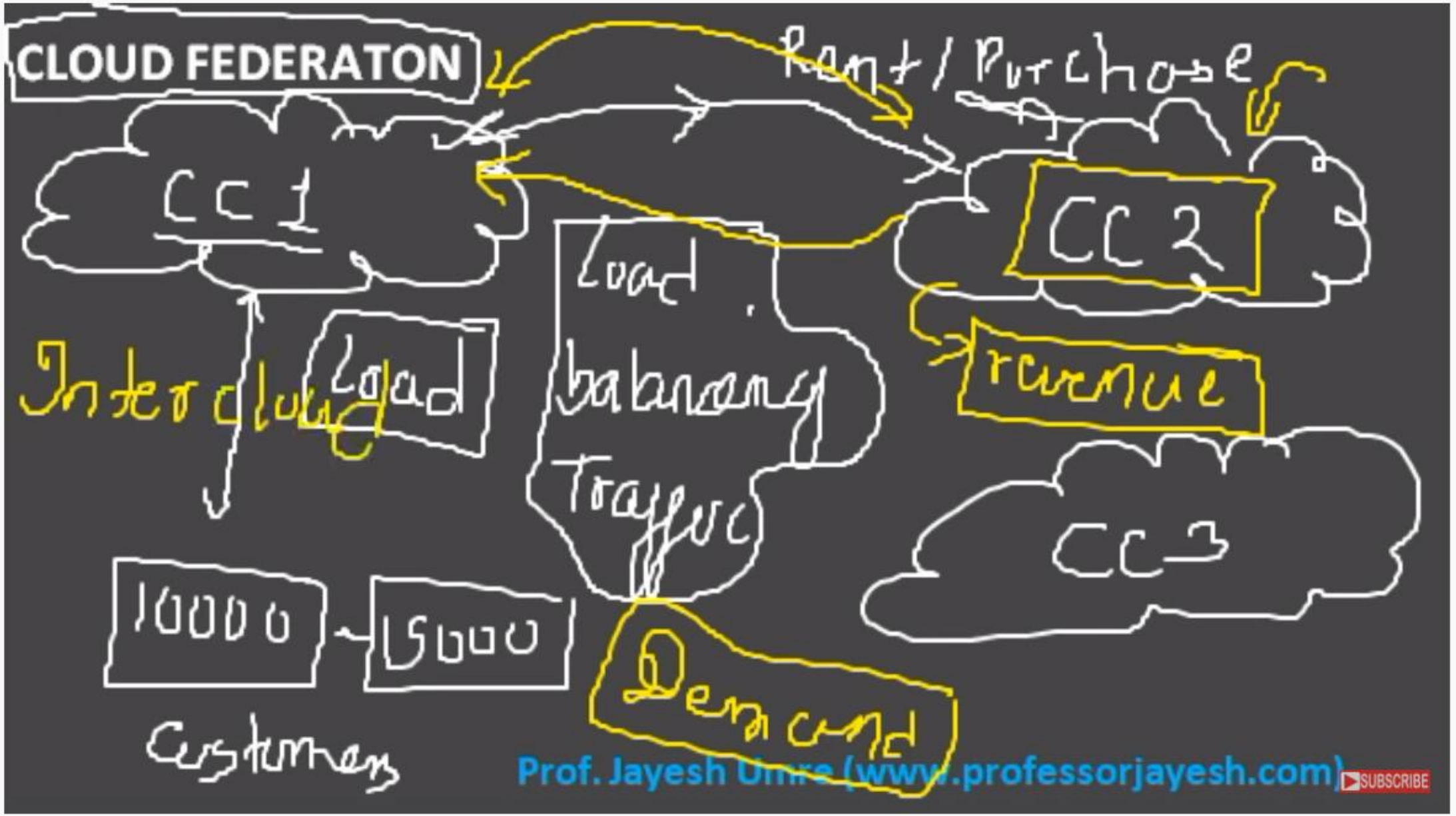
↳ It is the deployment and management of multiple external and internal cloud computing services to match business needs.

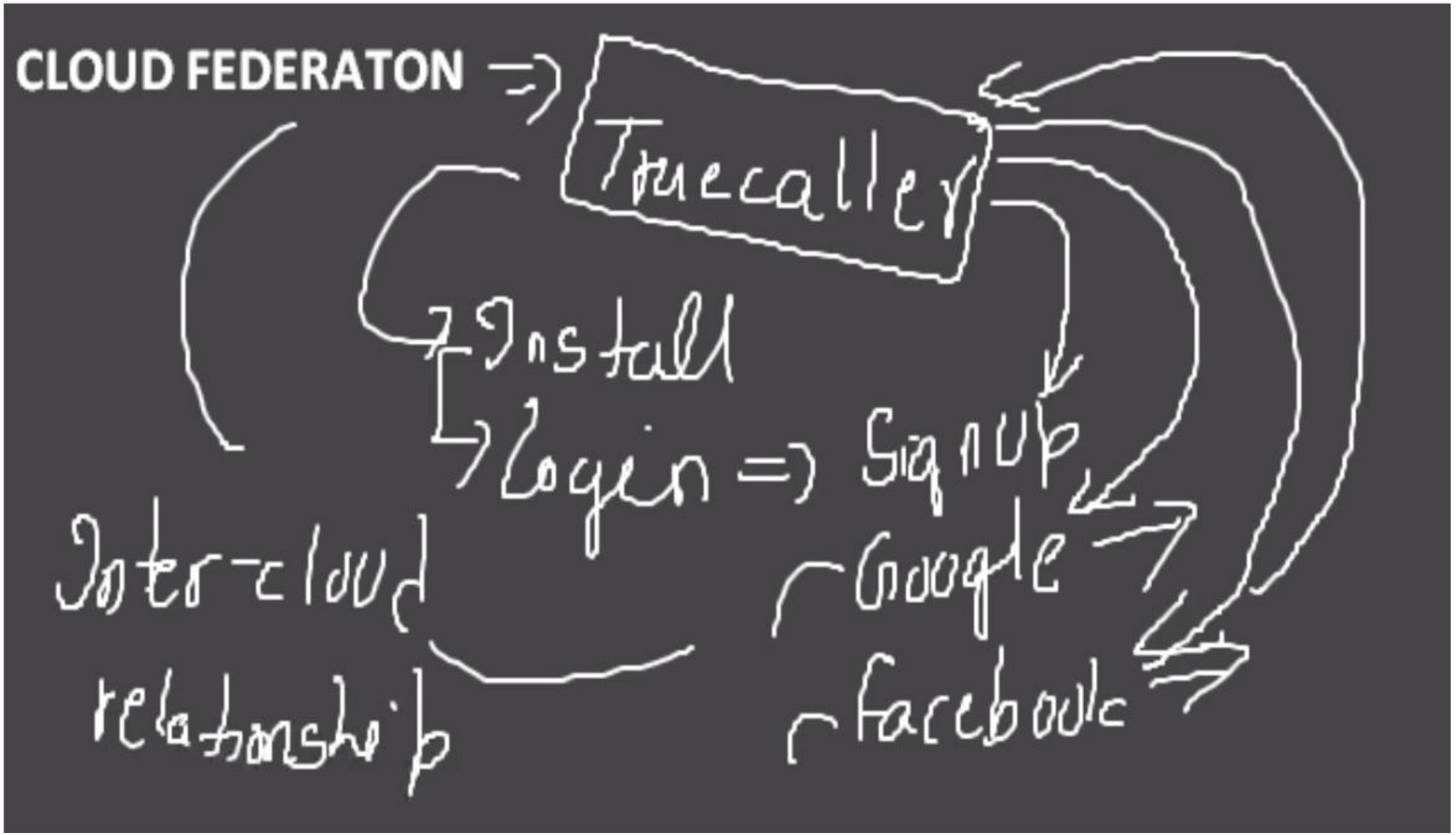
↳ It is a multi-national cloud system that integrates Community, private, public clouds into Scalable Computing platform.



↳ Easily Scale up to any no. of resources.

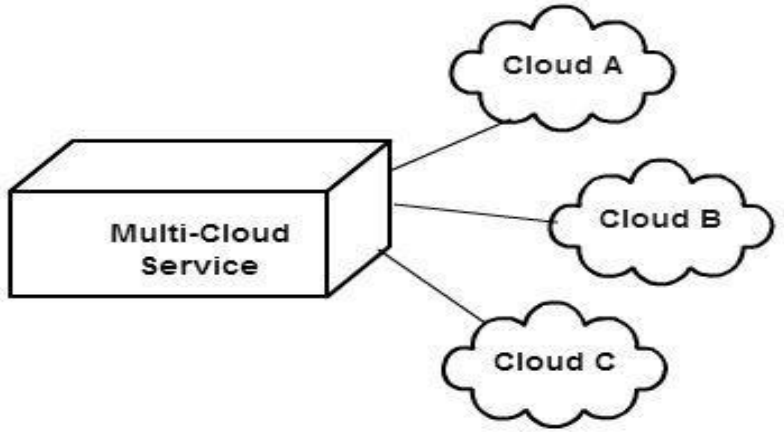
↳ Reliability


CLOUD FEDERATON
Rent / Purchase
CC 1
CC 2
CC 3
Load balancing Traffic
Inter cloud
Load
revenue
10000
5000
Customers
Demand
Prof. Jayesh Umre (www.professorjayesh.com)
SUBSCRIBE


CLOUD FEDERATON
Truecaller
Install
Login
Signup
Inter-cloud
relationship
Google
facebook

Multi-Cloud

- Multi-Cloud: In a Multi-Cloud, **a client** or service (IaaS, PaaS, SaaS etc.) uses multiple independent clouds. **A multi-cloud environment has no volunteer interconnection and sharing of the cloud service providers' infrastructures. Clients access multiple clouds through a service**. A service is hosted by the cloud client either externally or in-house.



What is Resource Provisioning

or

Resource management/ plan/ arrangement/preparation /providing, prearrangement

- Resource Provisioning means the selection, deployment, and run-time **management of software** (e.g., database server management systems, load balancers) and **hardware resources** (e.g., CPU, storage, and network) **for ensuring guaranteed performance for applications.**
- **This resource provisioning takes Service Level Agreement (SLA) into consideration for providing service to the cloud users.**

What is Resource Provisioning

- This is an initial agreement between the cloud users and cloud service providers which ensures **Quality of Service** (QoS) parameters like performance, availability, reliability, response time etc.
- Based on the application needs Static Provisioning/Dynamic Provisioning and **Static/Dynamic Allocation of resources** have to be made in order to efficiently make use of the resources **without violating SLA and meeting these QoS parameters.**

Types of Resource Provisioning

Resource Provisioning Methods

The cloud provisioning process can be conducted using one of three delivery models. Each delivery model differs depending on the kinds of resources or services an organization purchases, how and when the cloud provider delivers those resources or services, and how the customer pays for them.

The **three models are**

- **advanced provisioning**
- **dynamic provisioning**
- **user self-provisioning**

Types of Resource Provisioning

They are of 3 Types:-

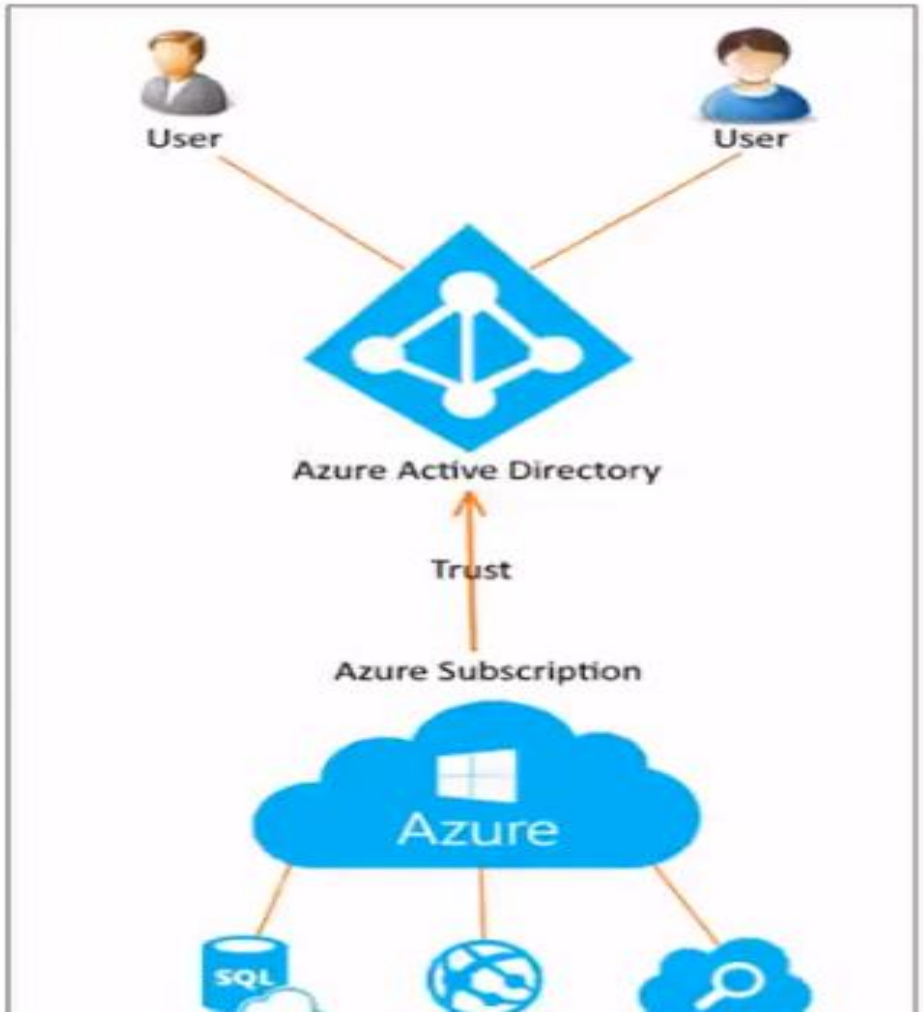
1. Static Provisioning or Advanced Provisioning : For applications that have predictable and generally **unchanging demands/workloads**, it is possible to use “static provisioning" effectively.

- With advance provisioning, the **customer contracts with the provider for services and the provider prepares the appropriate resources in advance of start of service. The customer is charged a flat fee or is billed on a monthly basis.**

Static Provisioning or Advanced Provisioning

1. With **advanced provisioning**, the customer **signs a formal contract of service with the cloud provider**. The provider then prepares the agreed-upon resources or services for the customer and delivers them

The customer is **charged a flat fee or is billed on a monthly basis**



Continue..

2. Dynamic Provisioning: In cases where **demand by applications may change or vary,** "dynamic provisioning" techniques have been suggested whereby **VMs may be migrated on-the-fly to new compute nodes within the cloud.** With dynamic provisioning, **the provider allocates more resources as they are needed and removes them when they are not. The customer is billed on a pay-per-use basis.**

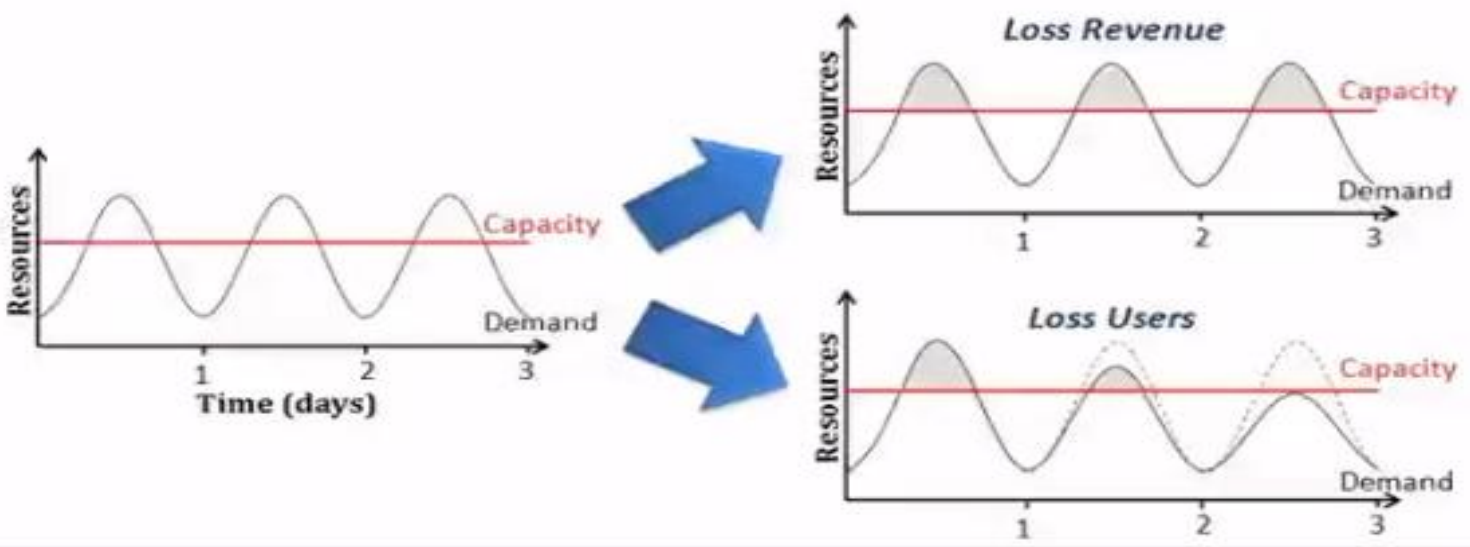
- When dynamic provisioning is used to create a **hybrid cloud**, it is sometimes referred to as **cloud bursting**.

Dynamic Provisioning

2. With **dynamic provisioning**, cloud **resources are deployed flexibly to match a customer's fluctuating demands**. The deployments typically scale up to accommodate spikes in usage and scale down when demands decrease.

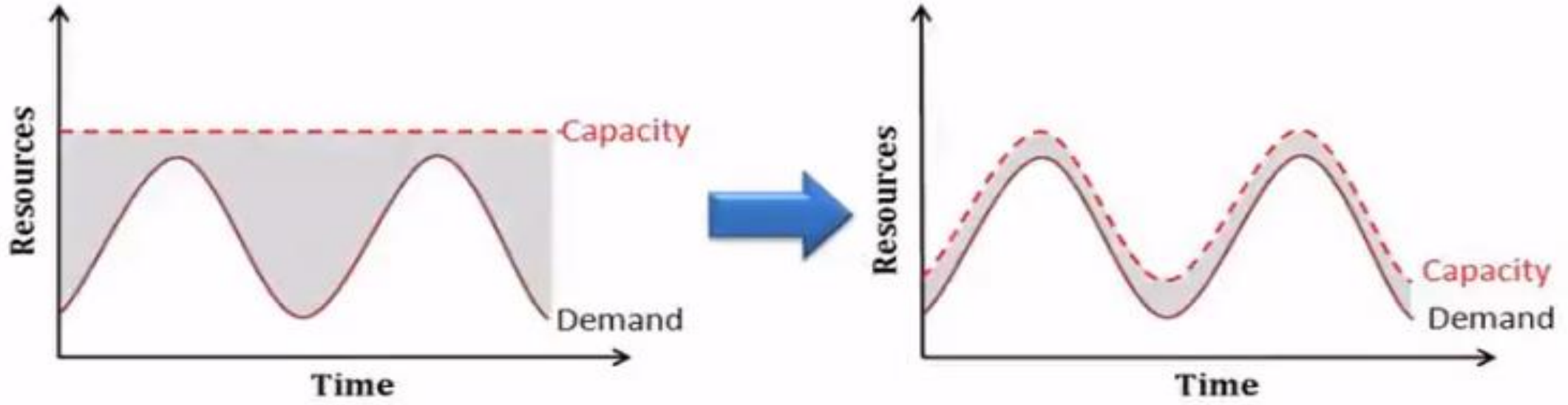
The **customer is billed on a pay-per-use basis. When dynamic provisioning is used to create a hybrid cloud environment, it is sometimes referred to as cloud bursting.**

- In traditional computing model, two common problems :
  - Underestimate system utilization which result in under provision

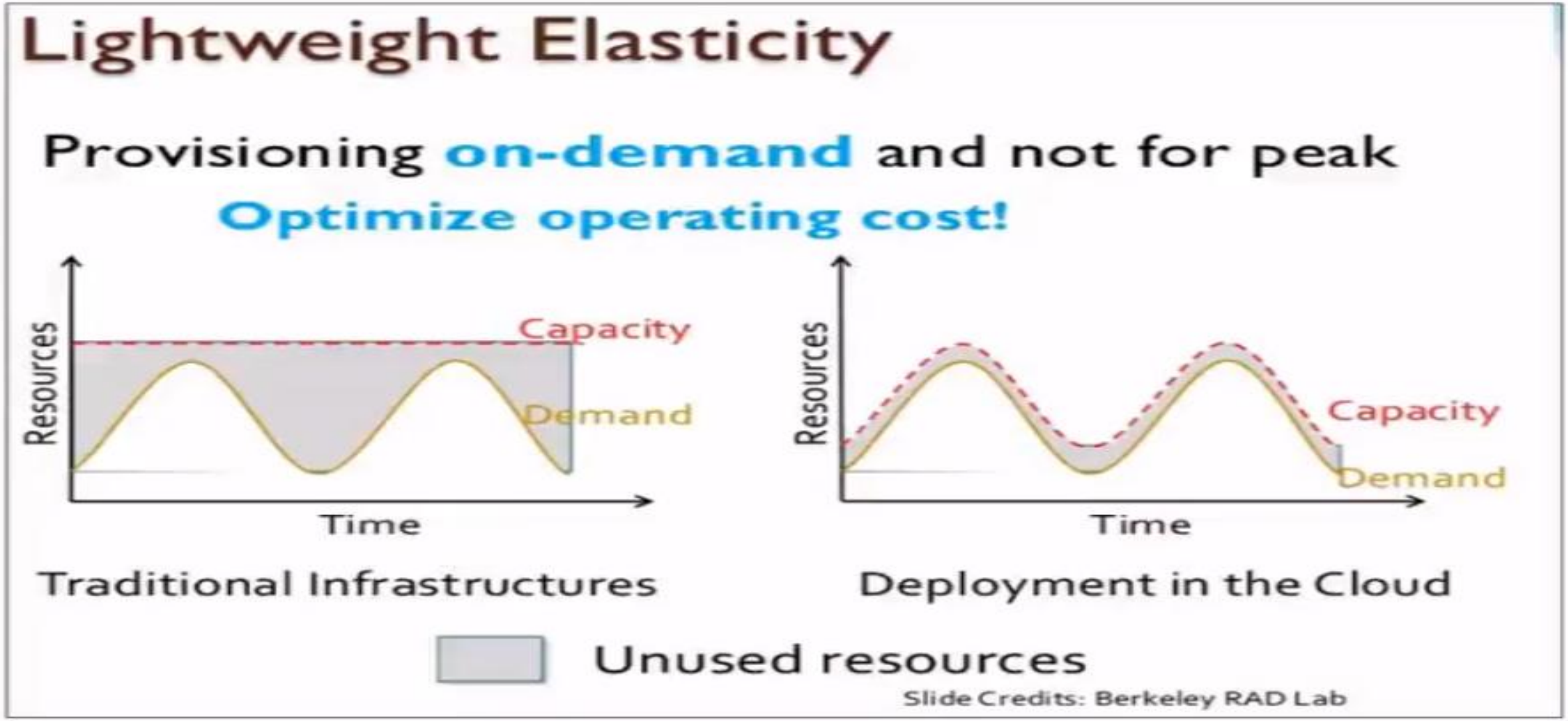


Dynamic Provisioning

- Cloud resources should be provisioned dynamically
  - Meet seasonal demand variations
  - Meet demand variations between different industries
  - Meet burst demand for some extraordinary events



Dynamic Provisioning



Continue…

3. User Self-provisioning: With user self- provisioning (also known as cloud self-service), **the customer purchases resources from the cloud provider through a web form**, creating a customer account and **paying for resources with a credit card.** The provider's resources are available for customer use within hours, if not minutes.

3. With **user self-provisioning**, also called cloud self-service, the **customer buys resources from the cloud provider through a web interface or portal**. This usually involves creating a user account and paying for resources with a credit card. Those resources are then quickly spun up and made available for use -- within hours, if not minutes

Examples of this type of cloud provisioning include an employee purchasing cloud-based productivity applications via the **Microsoft Office 365 suite or Google Apps for Business**

Cloud provisioning in three models

Advanced	Dynamic	User self-provisioning
Customer signs formal contract with cloud provider	Customer can purchase cloud resources based on average consumption needs	Customer selects cloud resources and services via a web interface
Cloud provider prepares and distributes agreed-upon resources in advance of start of service	Cloud provider deploys and adjusts resources to match customer's usage demands	Cloud provider makes resources available shortly after purchase
Flat-fee or monthly bill	Pay-per-use billing	Customer pays for services with a credit card

Parameters for Resource Provisioning

i) Response time: The resource provisioning algorithm designed **must take minimal time** to respond when executing the task.

ii) Minimize Cost: From the **Cloud user point of view cost should be minimized**.

iii) Revenue Maximization: This is to be achieved from the Cloud Service Provider's view.

iv) Fault tolerant: The **algorithm should continue to provide service in spite of failure of nodes.**

v) Reduced SLA Violation: The algorithm designed must be able to reduce SLA violation.

vi) Reduced Power Consumption: VM placement & migration techniques must lower power consumption.

Global Exchange of Cloud Resources

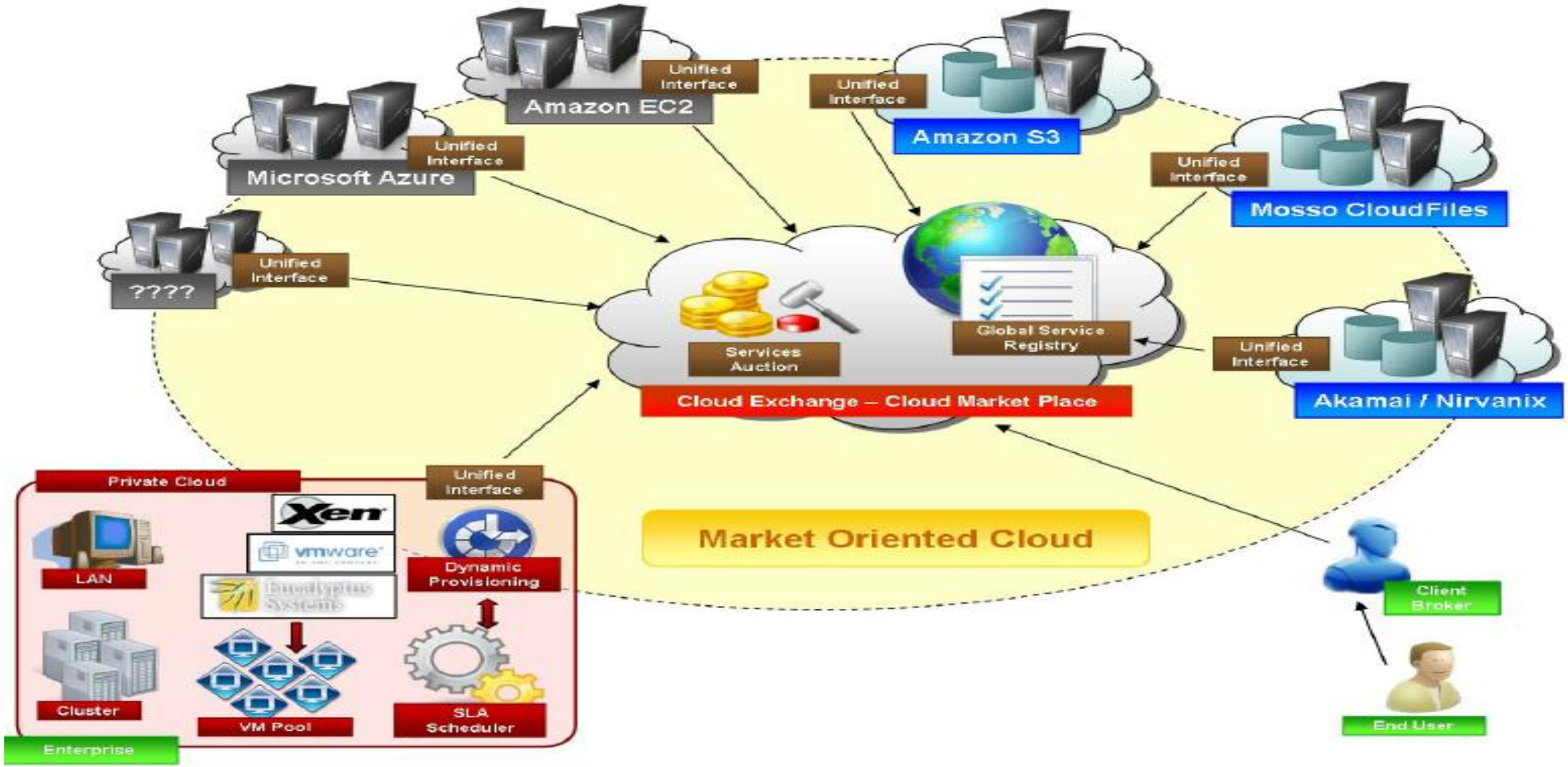
Limitations of present service providers:

1. Inflexible pricing
2. No standard interface
3. Unable to swap one for another
4. Consumer are restricted to offering from a single provider at a time

Global Cloud Exchange

- In order to support **a large number of application service consumers from around the world**, cloud infrastructure providers (i.e., IaaS providers) have established data centers in multiple geographical locations to provide redundancy and ensure reliability in case of site failures. For example, Amazon has data centers in the United States (e.g., one on the East Coast and another on the West Coast) and Europe. However, currently Amazon expects its cloud customers (i.e., SaaS providers) to express a preference regarding where they want their application services to be hosted.
- In addition, **no single cloud infrastructure provider will be able to establish its data centers at all possible locations throughout the world**. As a result, cloud application service (SaaS) providers will have difficulty in meeting QoS expectations for all their consumers. Hence, they would like to make **use of services of multiple cloud infrastructure service providers who can provide better support for their specific consumer needs.**
- Market Directory
- Banking System (Payment gateway etc)
- Brokers
- price setting mechanism
- Admission control mechanism
- consumer utility function

Continue..


Amazon EC2
Unified Interface
Amazon S3
Microsoft Azure
Mosso CloudFiles
????
Services Auction
Global Service Registry
Cloud Exchange – Cloud Market Place
Akamai / Nirvanix
Private Cloud
Xen
vmware
LAN
Dynamic Provisioning
Cluster
VM Pool
SLA Scheduler
Enterprise
Market Oriented Cloud
Client Broker
End User

Cloud Security

Cloud Security

- Cloud computing, all your data is stored on the cloud, so cloud users ask some questions like: **How secure is the cloud? Can unauthorized users gain access to your confidential data?**
- **Cloud computing companies say that data is secure**, but it is too early to be completely sure of that. **Only time will tell if your data is secure in the cloud.**
- **To address these concerns, the cloud provider must develop sufficient controls to provide the same or a greater.**
- While cost and simplicity of use are two great benefits of cloud computing, there are significant security concerns that need to be addressed when considering moving critical applications and **sensitive data to public and shared cloud environments**.

There are three types of data in cloud computing

- **Data in transit (transmission data)**
- **Data at rest (storage data)**
- **Data in processing (processing data).**

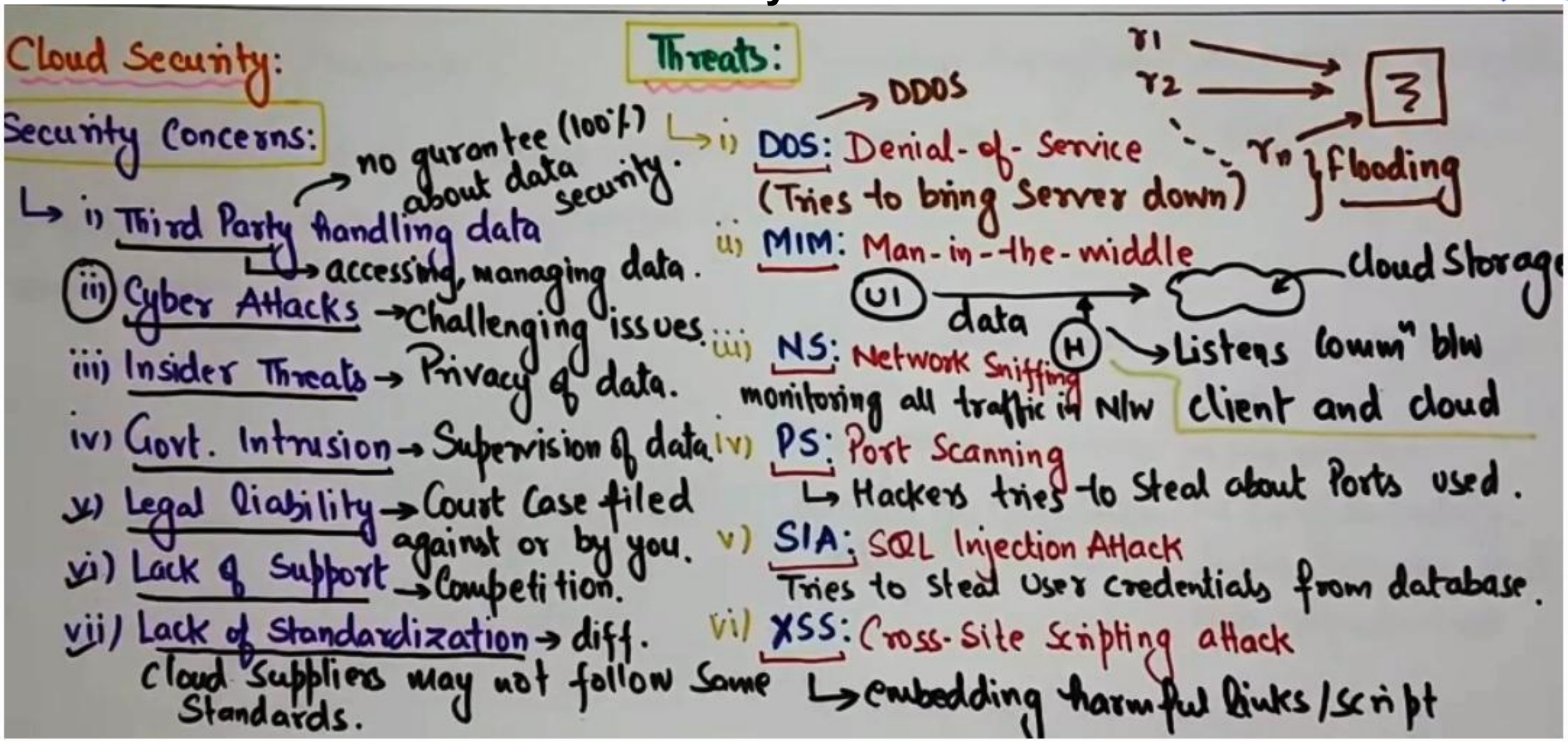
These complexities create many issues related to security. Security of data and trust problem has always been a primary and challenging issue in cloud computing.

Most cloud computing providers..

1. **Authenticates** (e.g., Transfer usernames and password) via secure connections and secondly,

2**. Transfer** (e.g., via **HTTPS**) data securely to/from their servers (so-called “data in transit encrypts stored data (so-called “data at rest”) automatically.

Cloud Computing Security Concerns, Threats in Cloud Computing Security



Contd..

Cloud data security model must ensure…

1. **OTP authentication system. Use strong authentication.**
2. **Data must be encrypted automatically**
3. **Check data integrity by using hashing algorithms.**
4. **Use the strong encryption algorithm that must be fast to retrieve data faster**. Encrypt data automatically with the highest strong/ fast encryption algorithm and finally ensure the fast recovery of data.

In cloud computing, to ensure correctness of user data, in first, **user must be make authentication.**

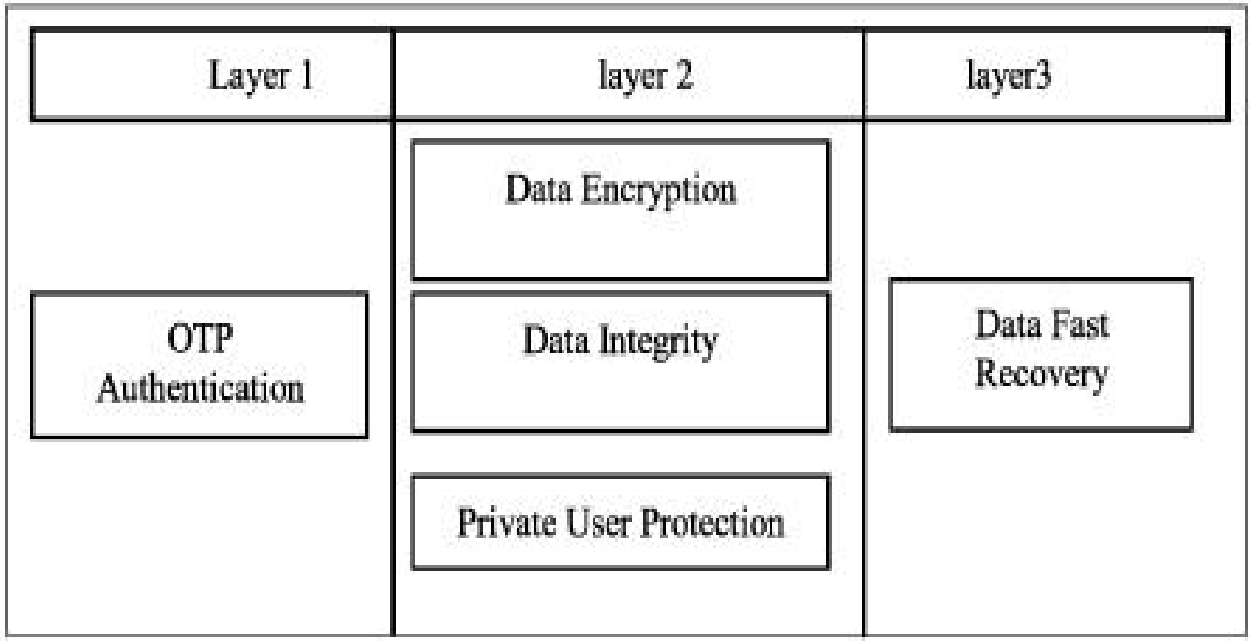
Authentication is the process of validating or confirming that access credentials provided by a user (for instance, **a user ID and password) are valid.**

Contd.

- **Amazon web services encourage user's to encrypt sensitive data by using TrueCrypt software.**

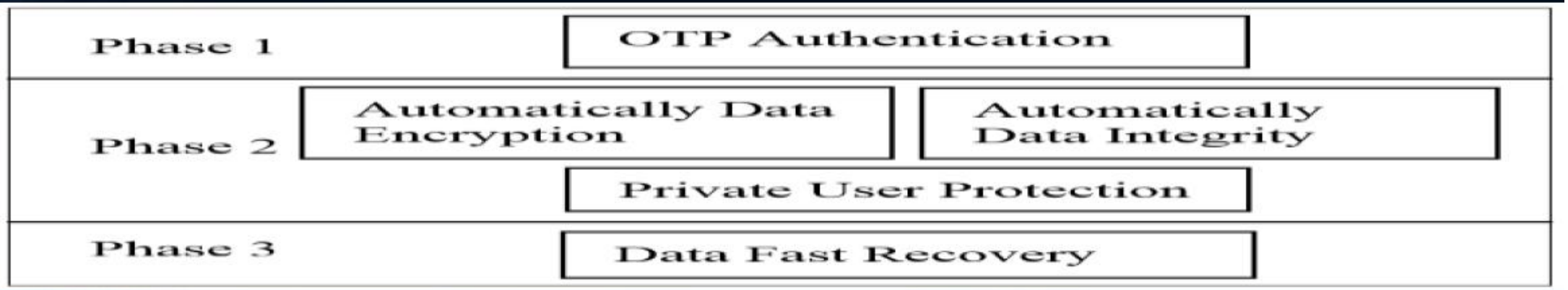
TrueCrypt is a computer software program whose primary purposes are to…

- Secure data by encrypting it before it is written to a disk.
- Decrypt encrypted data after it is read from the disk.
- TrueCrypt uses only three methods (AES, Serpent and Twofish) to encrypt data.



Cloud Data Security

- The proposed data security model uses three-level defense system structure…
  - Strong authentication is achieved by using OTP.
  - Data are encrypted automatically by using strong/fast encryption algorithm.
  - Fast recovery of user data.



Cloud Data Security

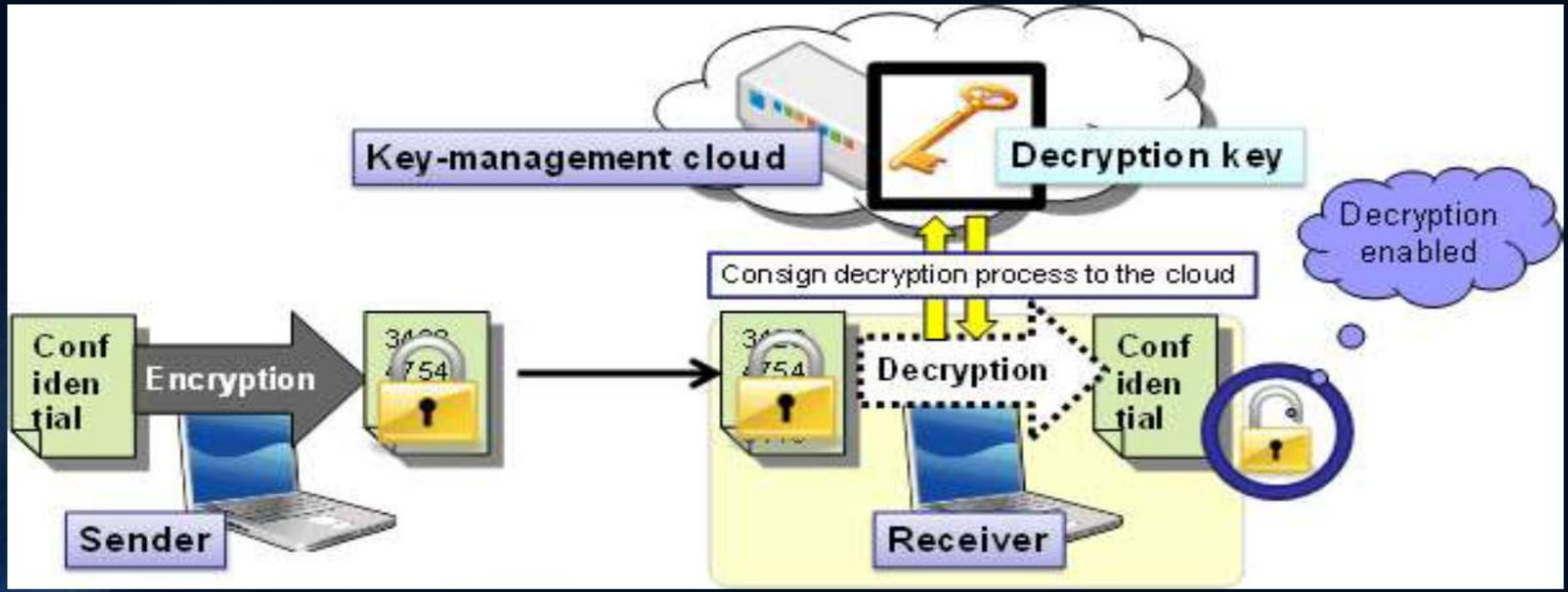
- OTP Authentication:
  - The cloud controller verifies user OTP from the temporary OTP database.
  - If OTP is true, send OTP login success.

Cloud Data Security

- Evaluation Algorithm Results:
  - Select the strongest and the fastest encryption algorithm by proposing algorithm called "Evaluation algorithm".
  - This algorithm used for selecting eight modern encryption techniques namely: RC4, RC6, MARS, AES, DES, 3DES, Two-Fish and Blowfish.
  - The evaluation has performed for those encryption algorithms according to randomness testing by using NIST statistical testing.
  - This evaluation algorithm performed at Amazon EC2 Micro Instance cloud computing environment.
  - RC4 has an advantage over other DES, RC6, MARS, 3DES and Twofish in terms of time consumption.
  - Twofish has low performance when compared with other algorithms.

Cloud Data Security

Encryption and Decryption Process



Ensuring Integrity:

- This is an extra concern for customers that now they have to worry about how to keep data hidden from auditors.
- This integrity check can be done by using cryptographic hash functions.

High Level Summary of Cloud Data Security Features

Features	Description
Authentication	OTP Authentication System (mathematical generation).
Provider encryption	Software implemented to select the highest security and faster encryption algorithm based on NIST statistical tests.
Private user encryption	TrueCrypt system or proposed software CloudCrypt v.10.
Data integrity	Hashing-MD5-MD4-SHA-1-SHA-2.
Data fast recovery	Based on decryption algorithm speed.
Key management	User keys not stored in provider control domain.

Security Issues and Challenges in Cloud Computing

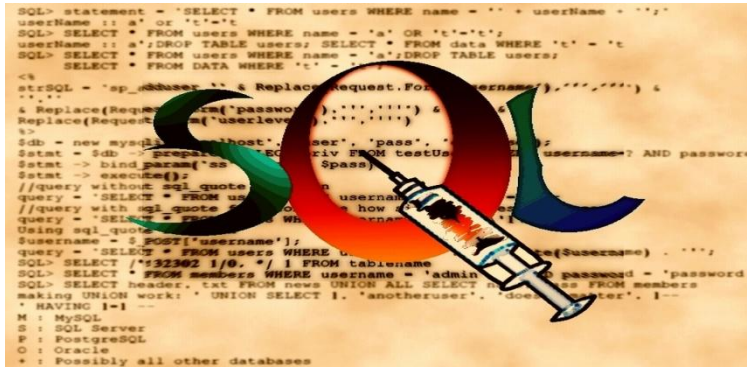
Data Related Security

- **Data Lock in**: Users **may lose data if they migrate from one vendor to another vendor**.
- **Data Recovery:** Sometimes **server may break down and cause damage or loss to users data**. To avoid this, **data should be backed up** to be recovered in future.
- **Data Locality:** In SaaS model of cloud environment, the **user doesn't know where the data is stored which may be an issue**. The issue can be solved by creating secure SaaS model which can provide reliability to the customer on the location of the data of the user.

Application related security issues

- **Cloud malware injection attack:** In this attack a **malicious virtual machine or a service implementation is injected into the cloud system**. one solution to prevent this is to perform the integrity check to the service instance.
- **Cookie poisoning: In this an unauthorized access is made into the application by modifying the contents of the cookie. One solution is to clean up the cookie** or encrypt the cookie data.
- **Hidden Field Manipulation: Certain fields are hidden in the web-site and is used by the developers. Hacker can easily modify on the web page.**

- **SQL injection:** It can be done by **injecting the SQL commands into the database of an application to crash the database.**
- **Malicious Insider: In <u>private cloud, its employee is granted access to the sensitive data</u>** of some or all customer administrators. **Such <u>privileges may expose information to security threats.</u>**

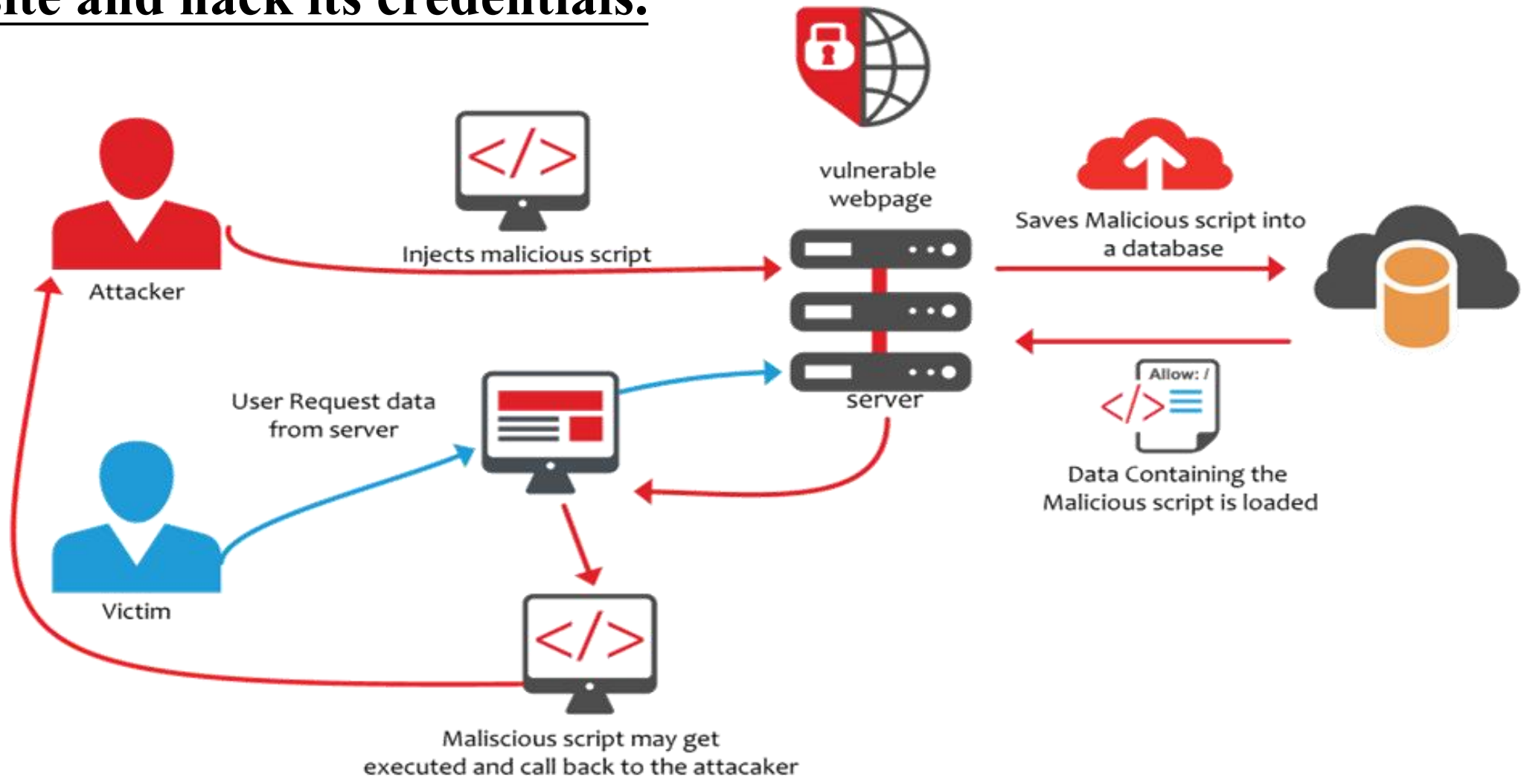


Network level attacks

- DNS attacks:

Domain hijacking: Domain hijacking is defined as **changing the name of a domain without the knowledge or permission from the domain's owner or creator.** This enable the intruders to access the sensitive information.

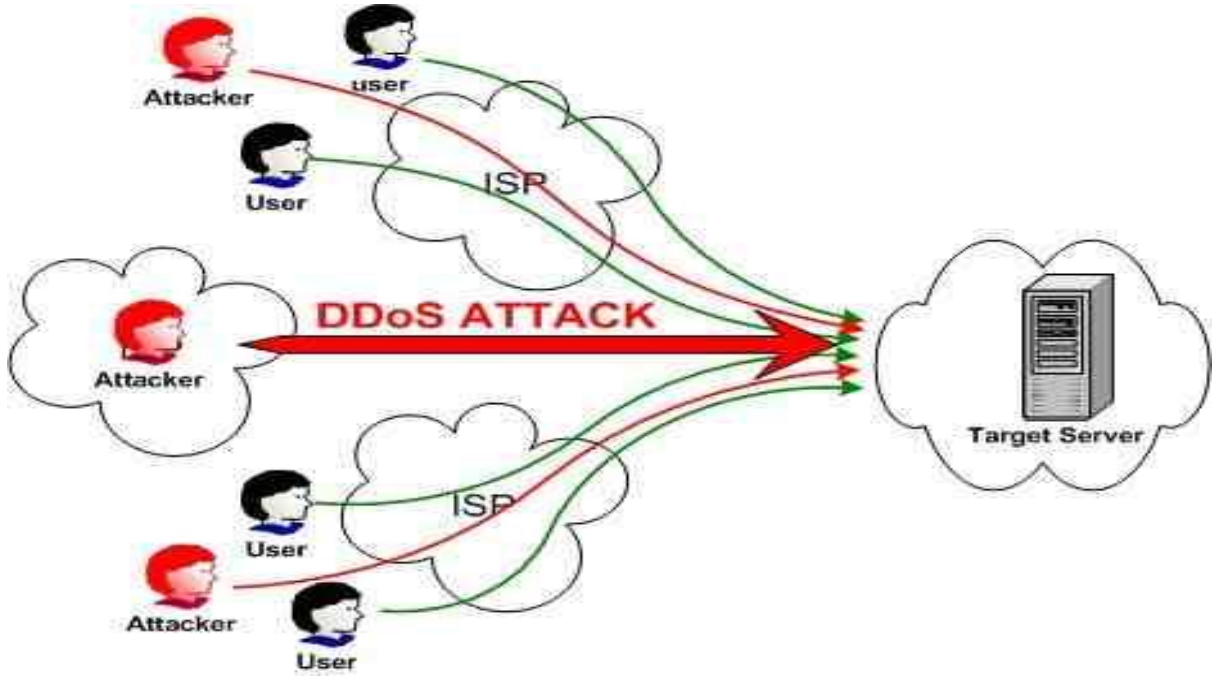
Cross site scripting: It is a type of attack in which user enters right URL of a website and **hacker on the other site redirect the user to its own website and hack its credentials.**



Network level attacks

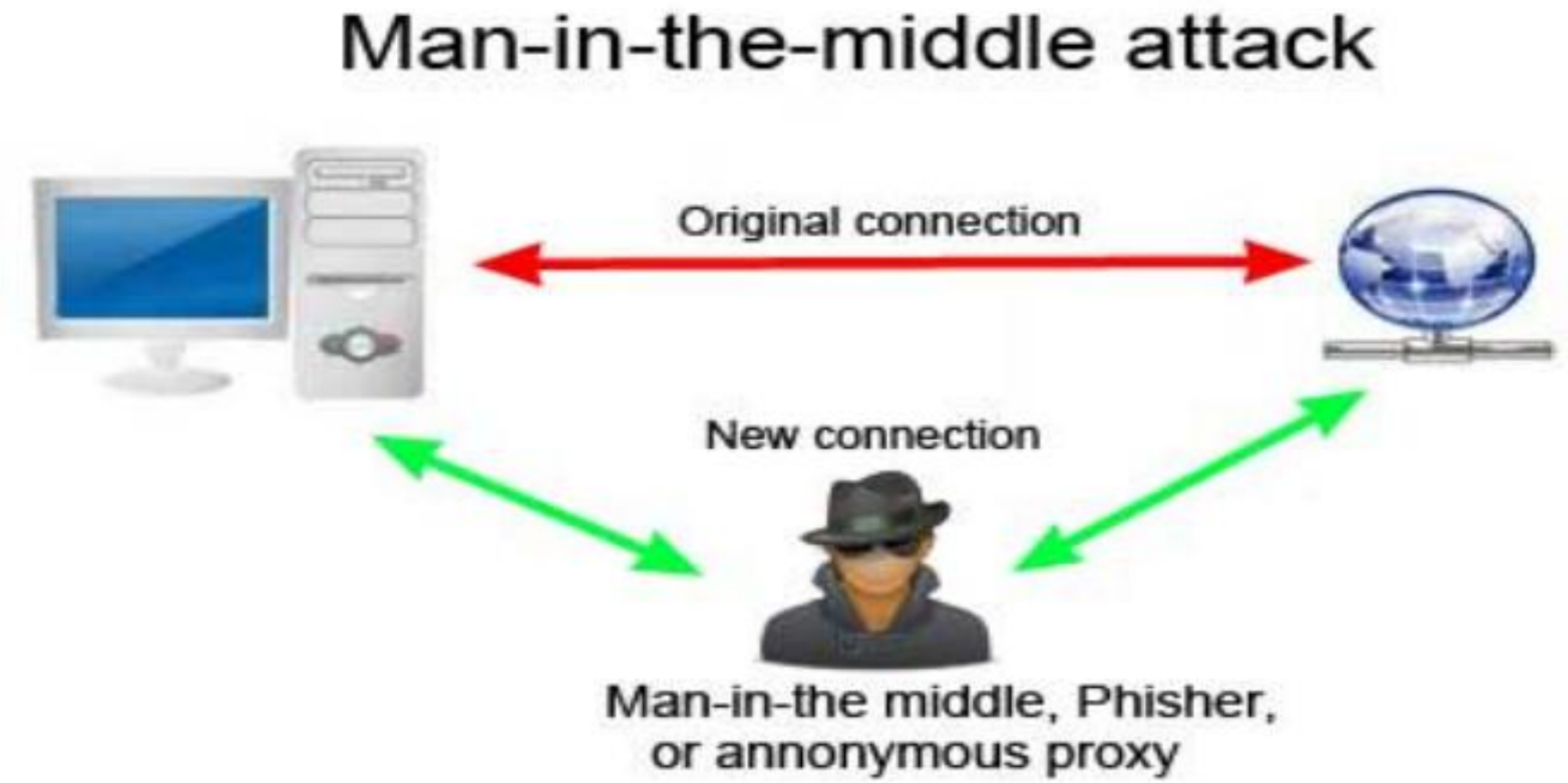
- **IP spoofing:**

  DOS attack: **When hackers overflows a network server or web server with frequent request of services to damage the network**, the denial of service cannot keep up with them, **server could not real client regular requests.**



Network level attacks

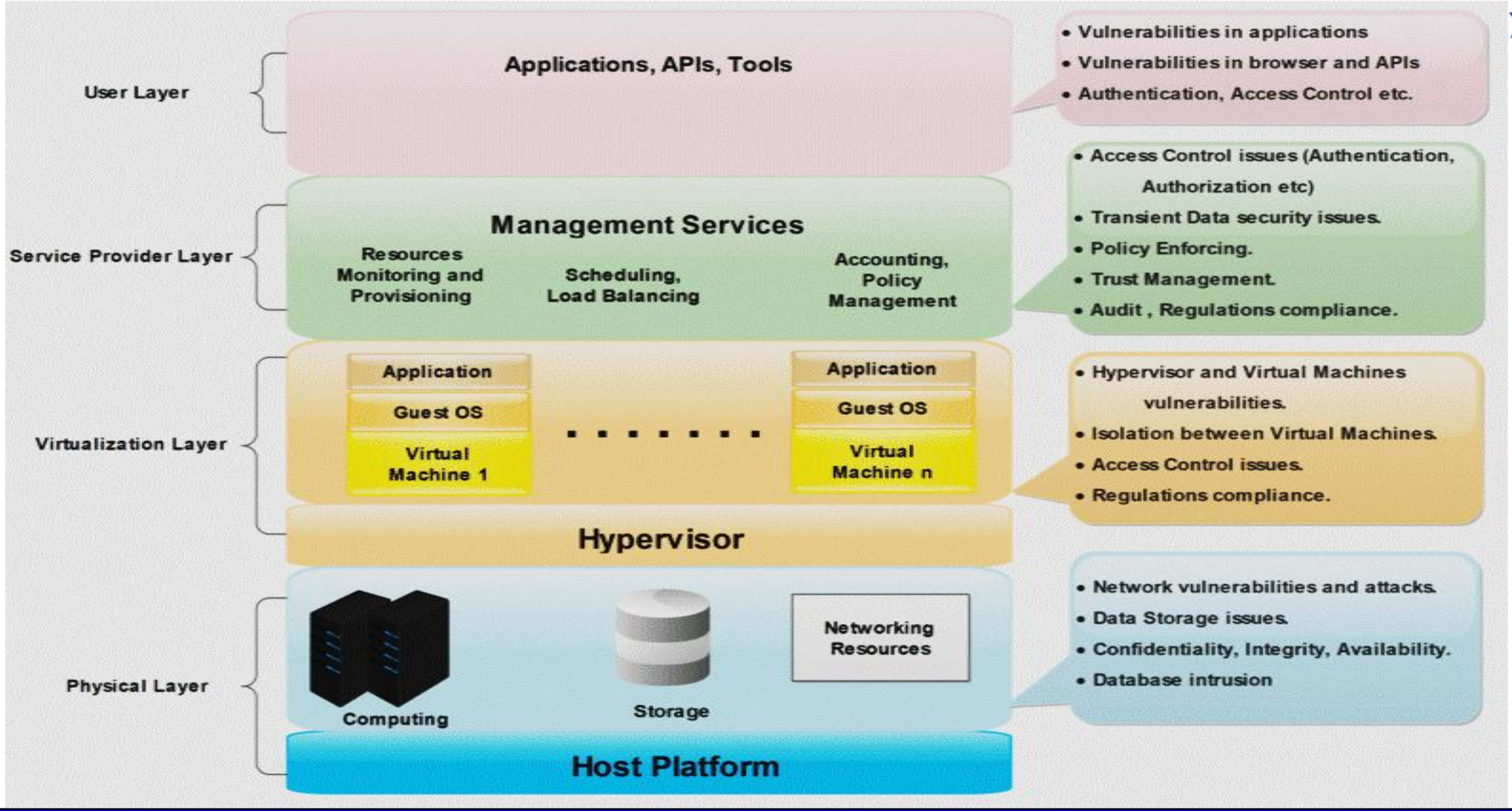
- **Man in the middle attack:** This is another issue of network security that will happen if secure socket layer (SSL) is not properly configured.



Security requirements for cloud computing

- Identification and Authenticity:
- Authorization
- Non-repudiation
- Availability

Cloud Architecture Layers and Related Security Issues



Cloud Computing

Topic: Virtual Machine Security, IAM, Cloud Security Standards

Contents

- Virtual Machine Security,
- IAM,
- Cloud Security Standards

Virtual machine security

Security Risks in Virtualization

- Scaling: **it is easy to replicate a VM or creating a copy is very easy.**
- A single fatal event or **a single system attacked with worm or malicious** code can be replicated which **can cause destruction to the virtual environment.**
- Transience: in a virtual environment **large number of mobile machines comes and goes very frequently**. Network with traditional machines were much more stable as it was easy to analyze the configuration of the existing network.

- Diversity: in a virtual environment **it is difficult to enforce homogeneity in the network.**
- **Some of the VM will be running with new updated patches, but some will be still running with the older version of OS.**
- **If one has to migrate their machine from one version to another it would be difficult to migrate all the system from older version to newer version.**
- Mobility: **it is easy to copy VMs and it can give increase to security threats.**

Steps to ensure virtual machine security in cloud computing

Protect hosted elements by segregating them

- **Step one** in securing virtual machine security in cloud computing is **to *isolate the new hosted elements*.**
- It's possible your hosting and management processes will become visible and vulnerable.
- **If you isolate your hosting and feature connections inside a private sub network, they're protected from outside access.**

Ensure all components are tested and reviewed

- ***Certify virtual features and functions for security compliance before you allow them to be deployed*.**
- **Outside attacks are a real risk in virtual networking, but an insider attack is a disaster.**

Separate management APIs to protect the network

- **Step three** is to *separate infrastructure management*.
- **Management APIs will always represent a major risk because they're designed to control features, functions and service behavior.**
- **It's important to protect all such APIs**, but it's critical to protect the APIs that oversee infrastructure elements that should never be accessed by service users.

Keep connections secure and separate

- **The fourth** and final point in cloud-virtual network security is to *ensure that virtual network connections don't cross over between tenants or services*.

Cloud Computing Security Mechanism – Identity and Access Management (IAM)

Cloud Security mechanism: IAM

Identify and Access Management

"IAM" encompasses the components and policies necessary to control and track user identities and access privileges for IT resources, environments and systems.

AAUC

[Deals with preventing unauthorized access Resources

IAM Main Components:

Authentication :- username + pwd Combination. ↳ Digital Signatures ↳ Digital certificates ↳ Biometric	**Authorization** Access Control U1 → r1 (✓) → r2 (✗)
User management ↳ Creating new user ↳ adding user to the required access grp ↳ maintaining pwd policies, privileges	**Credential management** ↳ establishes identities & access control rules for users.

Identity and access management (IAM)

IDENTITY AND ACCESS MANAGEMENT

- **Identity =** the fact of being who or what a person [*Identification / Recognition*].
- **Access =** Opportunity to use something.
- **Management =** Process of Dealing with or Controlling things.
- **Identity Access Management [IAM] deals with Products, Processes and Policies used to Manage users access.**
- IAM enable IT to control users access to critical information and resources within their organization.
- **Only Identified [*i.e., authorized users*] users can access the Resources.**
- **Users = Customers**

IDENTITY AND ACCESS MANAGEMENT

- **IAM Tools**
- **IAM tools Includes**
  1) Users Identity Management Tools
  2) Users/Customer Passwords Management Tools
  3) User Security Policies
  4) User Login Monitoring Tools
  5) User Access Management Tools
  6) Tools for Modification, Creation and Deletion Access

IDENTITY AND ACCESS MANAGEMENT

- **TASKS Performed by IAM**
  1) Users/Customer Authentication
  2) Users/Customer Authorization

Authentication = Process of User Verification [Identification of the users] – This is a Valid user or Not.

IDENTITY AND ACCESS MANAGEMENT

- **TASKS Performed by IAM**
  1) Users/Customer Authentication
  2) Users/Customer Authorization

Authentication = Process of User Verification [Identification of the users] – This is a Valid user or Not.

Authorization = Grant Access/Permission to Users – Official Permissions.

Identity and access management (IAM)

- Identity and access management (IAM) in enterprise IT is **about defining and managing the roles and access privileges of individual network users** and the circumstances in which **users are granted (or denied) those privileges.**
- **Those users might be customers (customer identity management) or employees (employee identity management. The core objective of IAM systems is one digital identity per individual.**
- **Once that digital identity has been established, it must be maintained, modified and monitored throughout each user's "access lifecycle."**

- Thus, the goal of identity management is to **“grant access to the right enterprise assets to the right users in the right context, from a user’s system onboarding to permission authorizations to the offboarding of that user as needed in a timely fashion,”**
- **IAM systems provide administrators with the tools and technologies to change a user’s role, track user activities, create reports on those activities, and enforce policies on an ongoing basis.**
- These systems are designed to provide a means of administering user access across an entire enterprise and to ensure compliance with corporate policies and government regulations.

CLOUD SECURITY STANDARDS

The standard will provide further security advice for both: clients and service providers. It will do that by offering advice for both side-by-side in each section.

1 Information Technology Infrastructure Library (ITIL)

- It is a **set of best practices and guidelines** that define an integrated, process-based approach **for managing information technology services.**
- ITIL helps make sure that proper **security measures are taken at all important levels, namely strategic, tactical, and operational level.**

2 Open Virtualization Format (OVF)

- Open Virtualization Format (OVF) is a standard pertaining to portability concern.
- **OVF provides the ability for an efficient, flexible and secure distribution of enterprise software over the cloud.**

- **OVF thus provides customers: vendor and platform independence as it facilitates mobility of virtual machines.**
- Across the cloud OVF plays a **major role in providing cross-platform portability. It also helps provide simplified deployment over multiple platforms.**

3 ITU-T X.1601

- **The ITU standard presents a sketch** of issues pertaining to **cloud computing and proposes a framework for cloud security.**
- **It talks in detail about various security challenges and ways to reduce these security risks in cloud computing.**
- **It also discusses a framework that provides an insight into what security capabilities are required for making the cloud secure and facing security challenges.**

4 PCI DSS

- **Payment Card Industry Data Security Standard** (PCI DSS) was released by PCI security standards council.
- **PCI's main objective is to provide security guidelines for credit card usage** and address Cloud service provider (CSP’s) and Cloud service consumer (CSC’s).
- **Cloud security is a shared responsibility between the CSP and its clients.**
- "For example, if payment card data is stored, processed or transmitted in a cloud environment, PCI DSS will apply to that environment, and will typically involve validation of both the CSP's infrastructure and the client's usage of that environment".

5 ISO/IEC 27017 Code of practice for information security controls

- **It aims to provide further guidance in the information security domain of cloud computing.**
- It is aimed at supplementing the guidance in ISO/IEC 27002 and various other ISO27k standards including ISO/IEC 27018 on the privacy aspects of cloud computing, ISO/IEC 27031 on business continuity, and ISO/IEC 27036-4 on relationship management, as well as all the other ISO27k standards

The scope and purpose:

- **It aims to provide an advancement to ISO/IEC 27002 in terms of adding value to its practices of control implementation**
- **Additionally the standard will provide further security advice for both: clients and service providers. It will do that by offering advice for both side-by-side in each section.**

Thank You