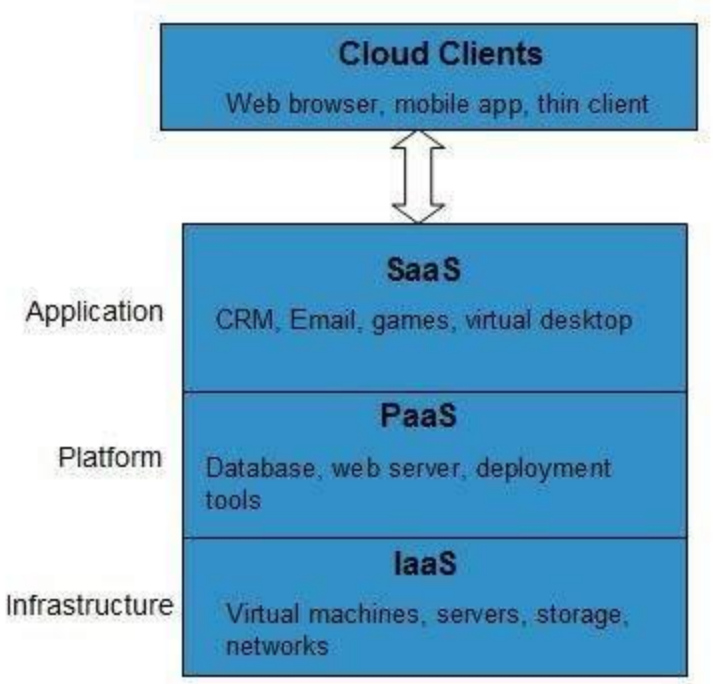
Chap-03

Cloud Computing Services and Data Security in Cloud

- Service Models
  - Cloud computing is based on service models. These are categorized into three basic service models which are -
    - Infrastructure-as–a-Service (IaaS)
    - Platform-as-a-Service (PaaS)
    - Software-as-a-Service (SaaS)
    - **Anything-as-a-Service (XaaS)** is yet another service model, which includes Network-as-a-Service, Business-as-a-Service, Identity-as-a-Service, Database-as-a-Service or Strategy-as-a-Service.

- The **Infrastructure-as-a-Service (IaaS)** is the most basic level of service.
- Each of the service models inherit the security and management mechanism from the underlying model, as shown in the following diagram:



- **INFRASTRUCTURE-AS-A-SERVICE (IAAS)**
  IaaS provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc.

- **PLATFORM-AS-A-SERVICE (PAAS)**

  PaaS provides the runtime environment for applications, development and deployment tools, etc.

- **SOFTWARE-AS-A-SERVICE (SAAS)**
  SaaS model allows to use software applications as a service to end-users.

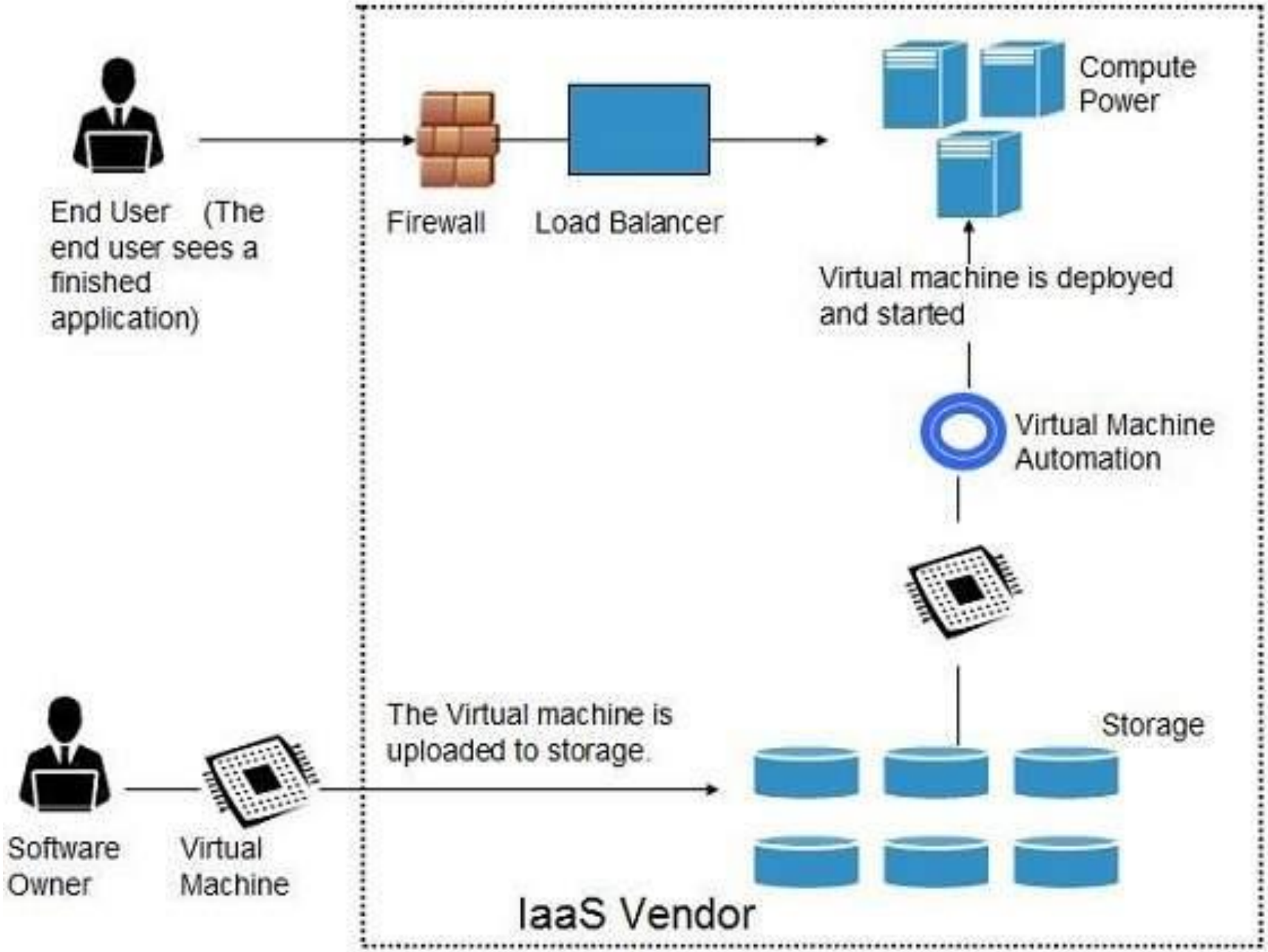
•**Infrastructure-as-a-Service** provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc.

Apart from these resources, the IaaS also offers:

- Virtual machine disk storage
- Virtual local area network (VLANs)
- Load balancers
- IP addresses
- Software bundles

• All of the above resources are made available to end user via **server virtualization.**

• Moreover, these resources are accessed by the customers as if they own them.


End User (The end user sees a finished application)
Firewall
Load Balancer
Compute Power
Virtual machine is deployed and started
Virtual Machine Automation
Software Owner
Virtual Machine
The Virtual machine is uploaded to storage.
Storage
IaaS Vendor

- **Benefits**

  IaaS allows the cloud provider to freely locate the infrastructure over the Internet in a cost-effective manner.

- Some of the key benefits of IaaS are listed below:
  - Full control of the computing resources through administrative access to VMs.
  - Flexible and efficient renting of computer hardware.
  - Portability, interoperability with legacy applications.

- Full control over computing resources through administrative access to VMs:
  IaaS allows the customer to access computing resources through administrative access to virtual machines in the following manner:

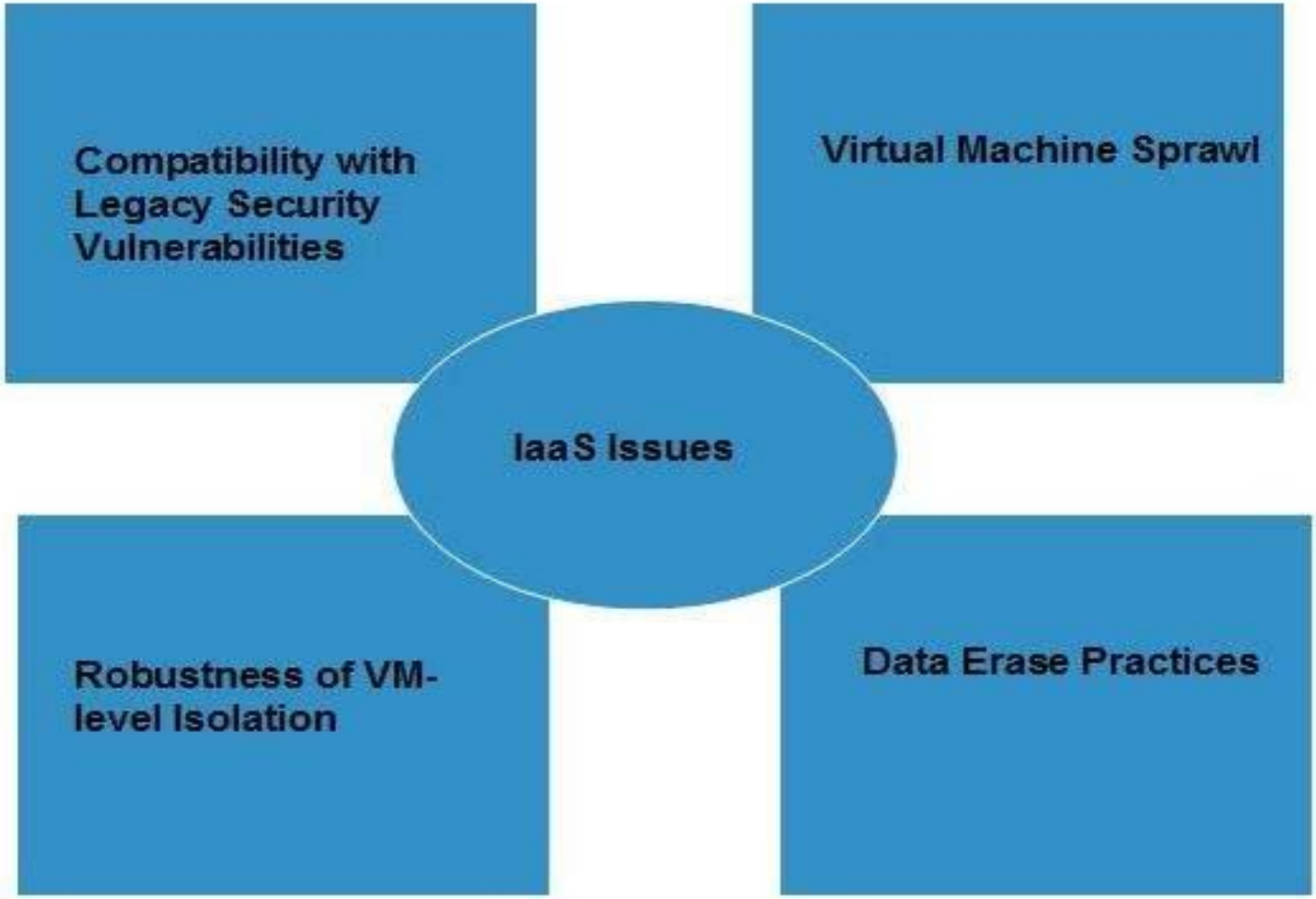
- Customer issues administrative command to cloud provider to run the virtual machine or to save data on cloud server.

- Customer issues administrative command to virtual machines they owned to start web server or to install new applications.

Flexible and efficient renting of computer hardware

- IaaS resources such as virtual machines, storage devices, bandwidth, IP addresses, monitoring services, firewalls, etc. are made available to the customers on rent.
- The payment is based upon the amount of time the customer retains a resource. Also with administrative access to virtual machines, the customer can run any software, even a custom operating system.

- **Portability, interoperability with legacy applications**
- It is possible to maintain legacy between applications and workloads between IaaS clouds.
- For example, network applications such as web server or e-mail server that normally runs on customer-owned server hardware can also run from VMs in IaaS cloud.


Compatibility with Legacy Security Vulnerabilities
Virtual Machine Sprawl
IaaS Issues
Robustness of VM-level Isolation
Data Erase Practices

Issues

IaaS shares issues with PaaS and SaaS, such as Network dependence and browser based risks. It also has some specific issues, which are mentioned in the following diagram:

Compatibility with legacy security vulnerabilities

Because IaaS offers the customer to run legacy software in provider's infrastructure, it exposes customers to all of the security vulnerabilities of such legacy software.

Virtual Machine sprawl

The VM can become out-of-date with respect to security updates because IaaS allows the customer to operate the virtual machines in running, suspended and off state. However, the provider can automatically update such VMs, but this mechanism is hard and complex.

Robustness of VM-level isolation

IaaS offers an isolated environment to individual customers through hypervisor.

Hypervisor is a software layer that includes hardware support for virtualization to split a physical computer into multiple virtual machines.

Data erase practices

The customer uses virtual machines that in turn use the common disk resources provided by the cloud provider.

When the customer releases the resource, the cloud provider must ensure that next customer to rent the resource does not observe data residue from previous customer.

Characteristics:

- Here are the characteristics of IaaS service model:

- Virtual machines with pre-installed software.

- Virtual machines with pre-installed operating systems such as Windows, Linux, and Solaris.

- On-demand availability of resources.

- Allows to store copies of particular data at different locations.

- The computing resources can be easily scaled up and down.

IAAS [Infrastructure-as-a Service]

↳ Provides access to → Physical machines
→ Virtual machines] Operates by (Hypervisor (KVM or Xen)
→ Virtual Storage.

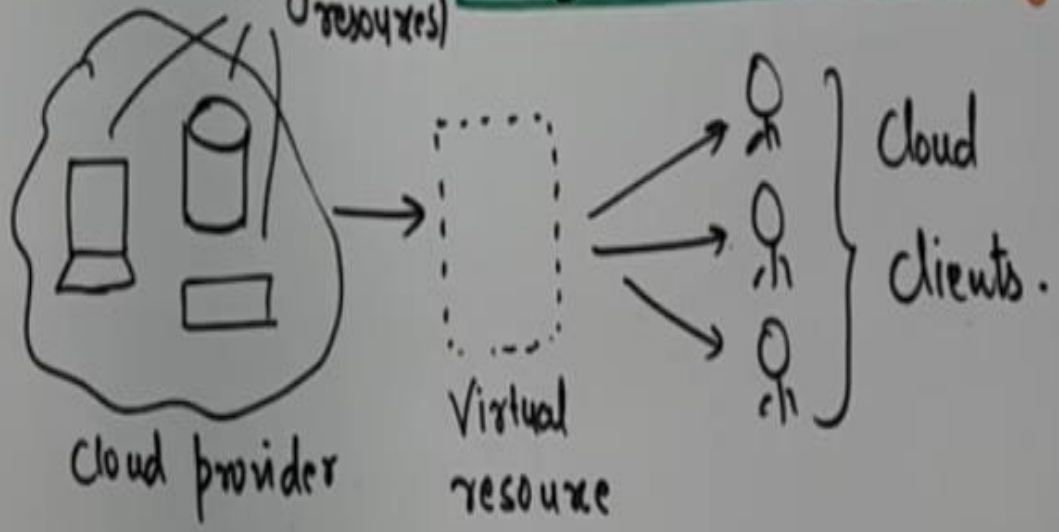
↳ other things that offers:

↳ i) Virtual LAN (VLANs)] N/w device
ii) IP addresses
iii) S/W bundles
iv) load balancers
v) Disk storage

[AMAZON, Google Compute Engine]

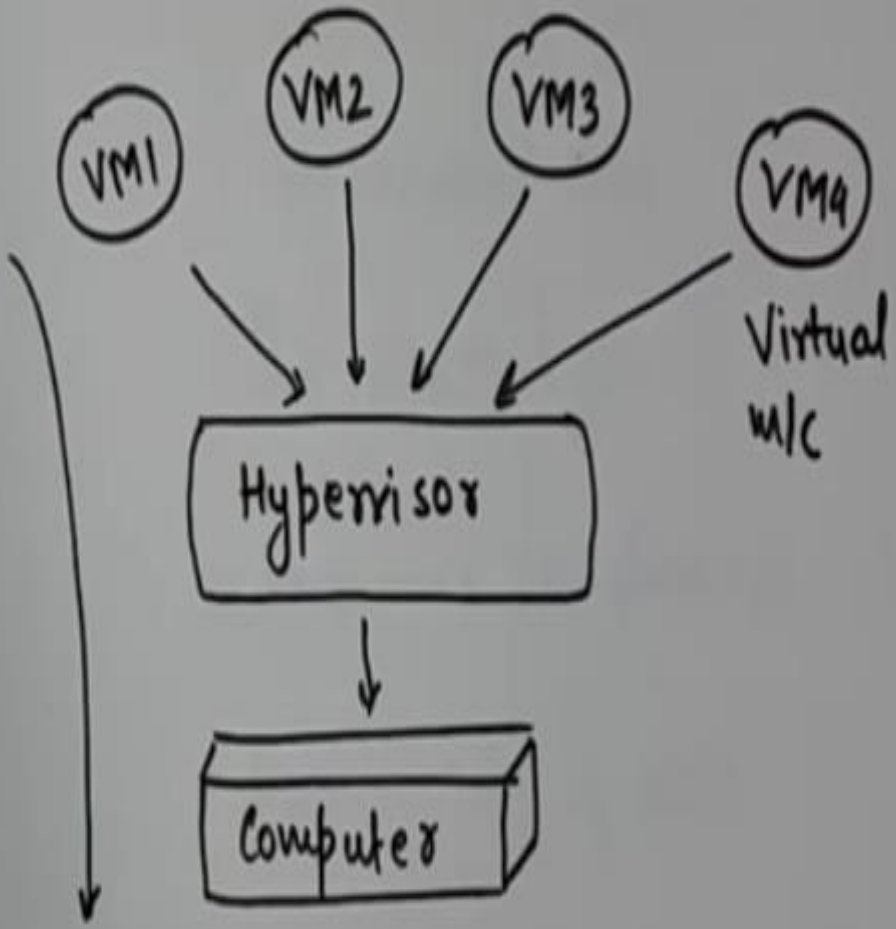
cloud Service Models:

(Saas) Email, Games, office etc.	Layer-3
(Paas) Database, web server, tools etc.	Layer-2
(Iaas) Storage, virtual m/c, N/w etc.	Layer-1



Benefits of IAAS: Using IAAS, cloud provider can freely locate infrastructure over-the internet in cost-effective manner.

↳ i) Global Accessibility
ii) Easy & Integration of devices
iii) Scalability is Easy
iv) Availability is High
v) Flexibility
vi) Full Control to Virtual m/c.



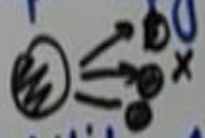
Services is being provided by virtual m/c through hypervisor.

IAAS Issues:-

- i) Compatibility:- Consumer need to use only legacy s/w on the Infrastructure.
  - ↳ ↑ cost.
- ii) Virtual Machine:- Mismatch b/w the VM security and cloud provide Security version.
- iii) Robustness:- Splitting of Single system resource into multiple virtual machines.
- iv) Data Deletion:- if client deletes the data then provider should also delete it permanently.

Characteristics of IAAS:-

- i) Pre-Installed s/w.
  - ↳ on virtual m/c.
- ii) Pre-Installed OS.
  - ↳ window, Linux, Solaris.
- iii) Resources On-demand
  - ↳ available.
- iv) Multiple copy of data [on multiple loc^{n}]



- v) Scalability of Computing.
  - ↳ ↑ scale
  - ↳ ↓ scale.

- **Platform-as-a-Service** offers the runtime environment for applications.

- It also offers development and deployment tools required to develop applications.

- PaaS has a feature of **point-and-click** tools that enables non-developers to create web applications.

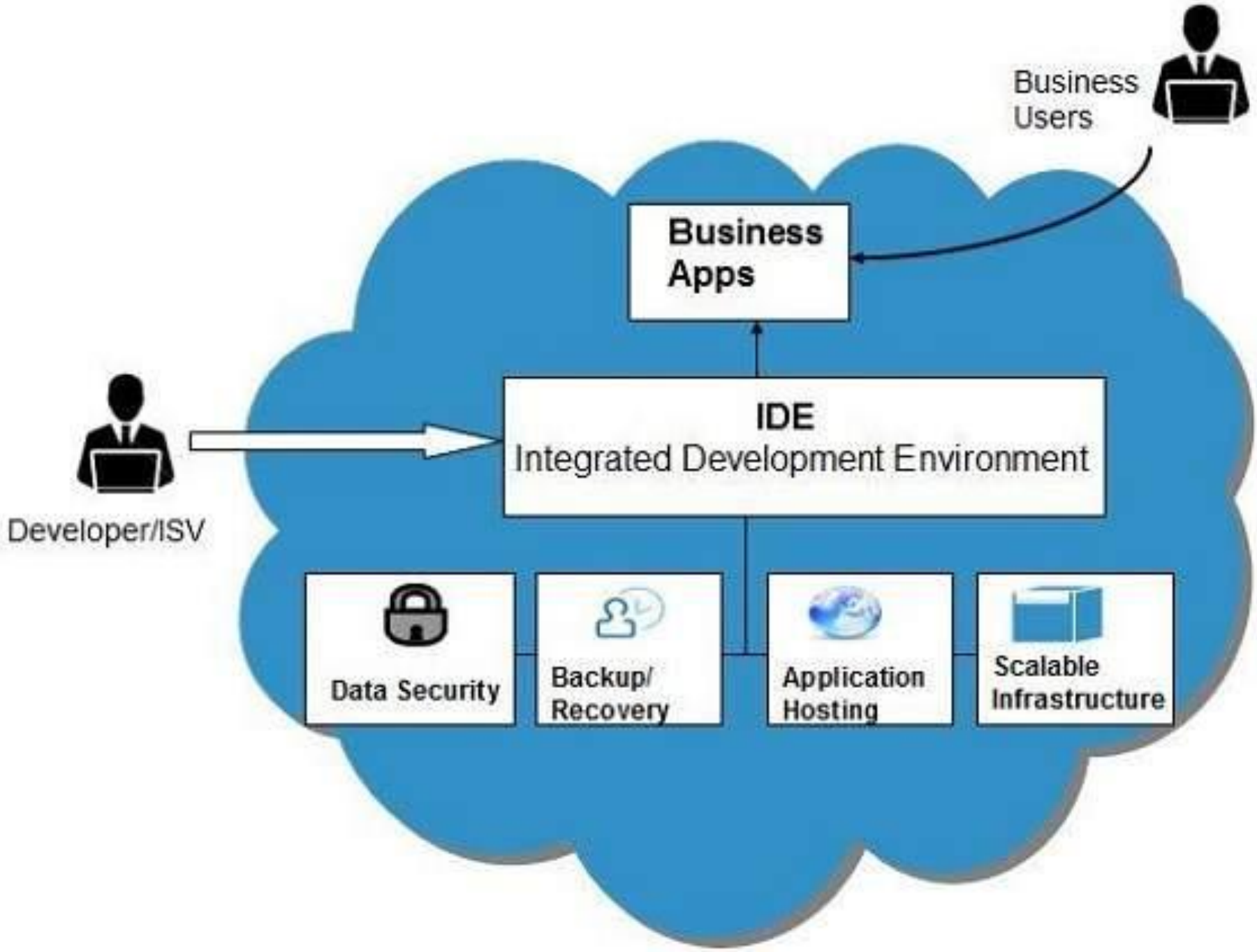
- **App Engine of Google** and **Force.com** are examples of PaaS offering vendors.

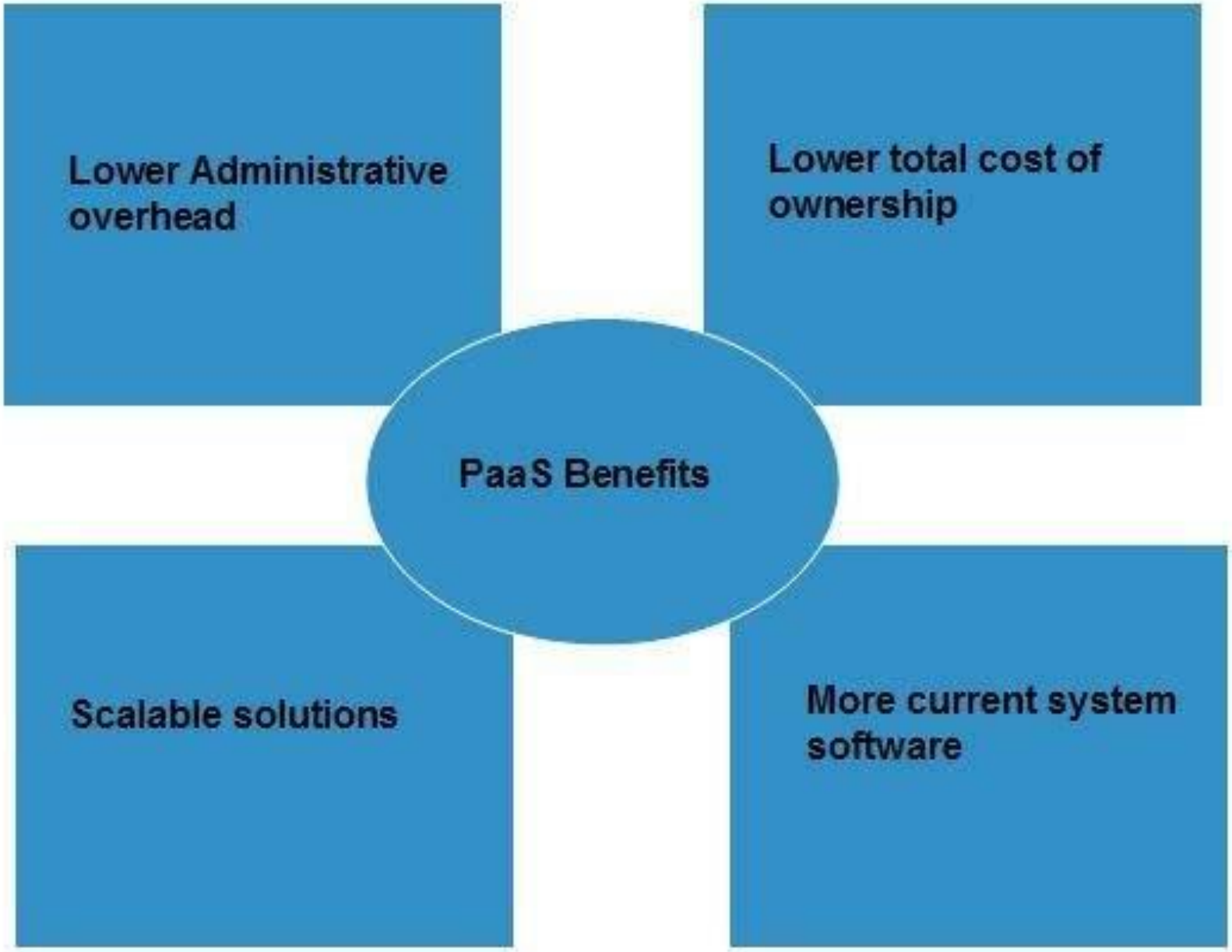
- Developer may log on to these websites and use the **built-in API** to create web-based applications.

- But the disadvantage of using PaaS is that, the developer **locks in** with a particular vendor.

- For example, an application written in Python against API of Google, and using App Engine of Google is likely to work only in that environment.

- The following diagram shows how PaaS offers an API and development tools to the developers and how it helps the end user to access business applications.


Business
Users
Business
Apps
IDE
Integrated Development Environment
Developer/ISV
Data Security
Backup/
Recovery
Application
Hosting
Scalable
Infrastructure


Lower Administrative overhead
Lower total cost of ownership
PaaS Benefits
Scalable solutions
More current system software

Benefits:

- **Lower administrative overhead**

Customer need not bother about the administration because it is the responsibility of cloud provider.

- **Lower total cost of ownership**

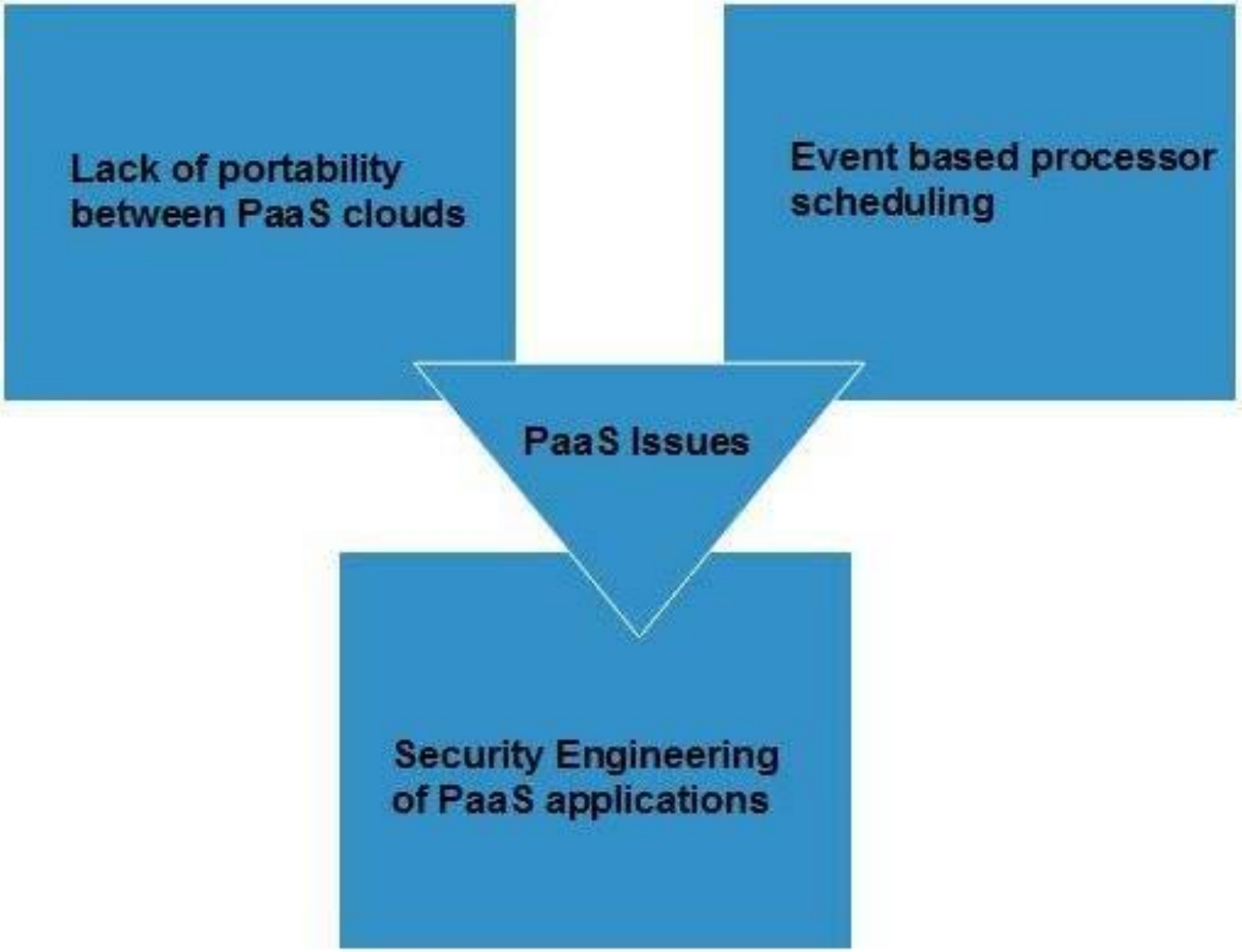
Customer need not purchase expensive hardware, servers, power, and data storage.

- **Scalable solutions**

It is very easy to scale the resources up or down automatically, based on their demand.

- **More current system software**

It is the responsibility of the cloud provider to maintain software versions and patch installations.


Lack of portability between PaaS clouds
Event based processor scheduling
PaaS Issues
Security Engineering of PaaS applications

➢Issues

- Like **SaaS, PaaS** also places significant burdens on customer's browsers to maintain reliable and secure connections to the provider’s systems.

- Therefore, PaaS shares many of the issues of SaaS.

- However, there are some specific issues associated with PaaS as shown in the diagram:

➢Lack of portability between PaaS clouds

- Although standard languages are used, yet the implementations of platform services may vary.

- For example, file, queue, or hash table interfaces of one platform may differ from another, making it difficult to transfer the workloads from one platform to another.

- **Event based processor scheduling**

The PaaS applications are event-oriented which poses resource constraints on applications, i.e., they have to answer a request in a given interval of time.

- **Security engineering of PaaS applications**

Since PaaS applications are dependent on network, they must explicitly use cryptography and manage security exposures.

Characteristics

Here are the characteristics of PaaS service model:

- PaaS offers **browser based development environment.**
- It allows the developer to create database and edit the application code either via Application Programming Interface or point-and-click tools.

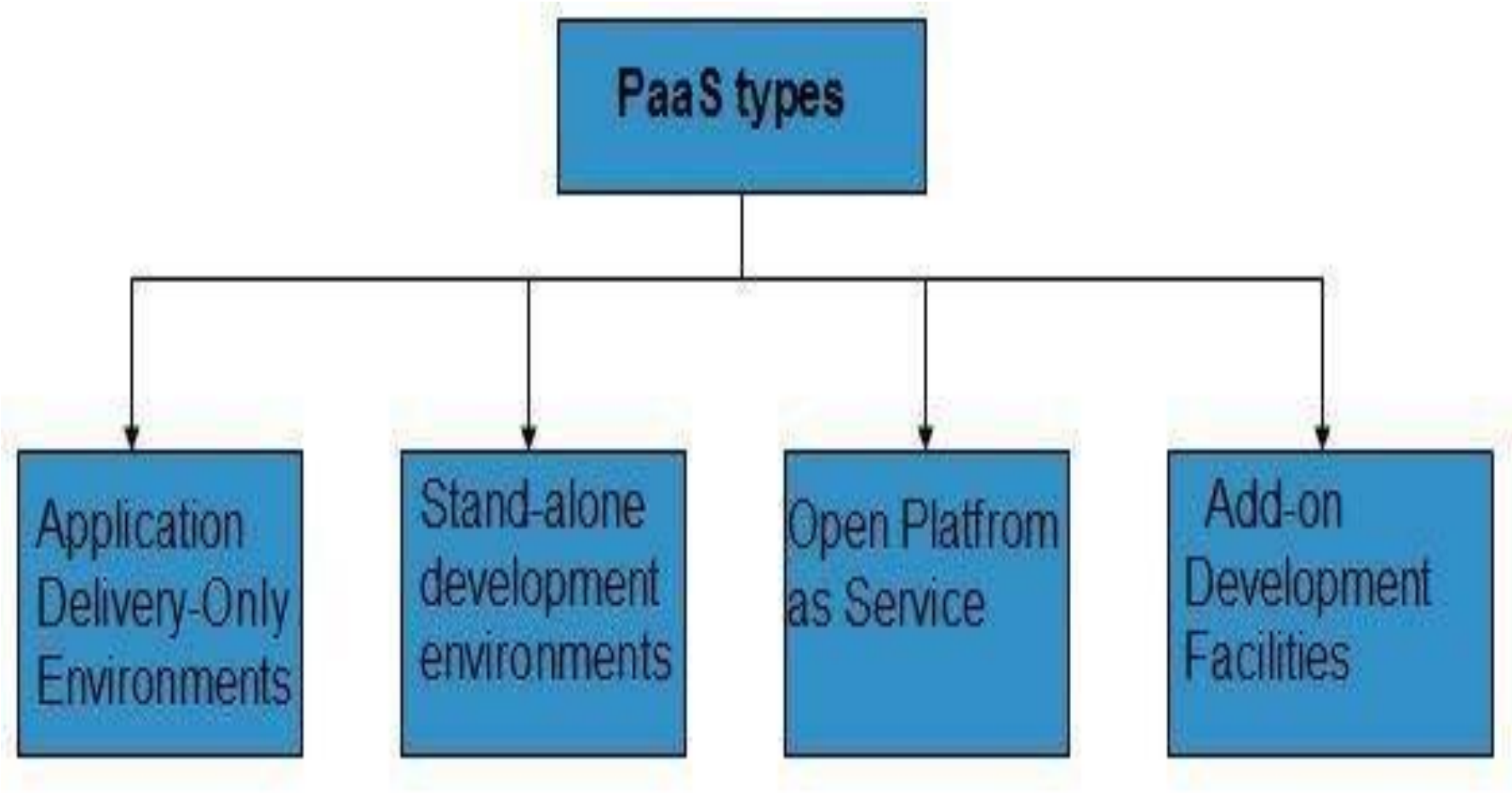
- PaaS provides **built-in security, scalability,** and **web service interfaces.**
- PaaS provides built-in tools for defining **workflow, approval processes,** and business rules.

- It is easy to integrate PaaS with other applications on the same platform.

- PaaS also provides web services interfaces that allow us to connect the applications outside the platform.

PaaS Types

Based on the functions, PaaS can be classified into four types as shown in the following diagram:



Stand-alone development environments

The **stand-alone PaaS** works as an independent entity for a specific function.

It does not include licensing or technical dependencies on specific SaaS applications.

Application delivery-only environments

The **application delivery PaaS** includes **on-demand scaling** and **application security.**

Open platform as a service

Open PaaS offers an **open source software** that helps a PaaS provider to run applications.

Add-on development facilities

The **add-on PaaS** allows to customize the existing SaaS platform.

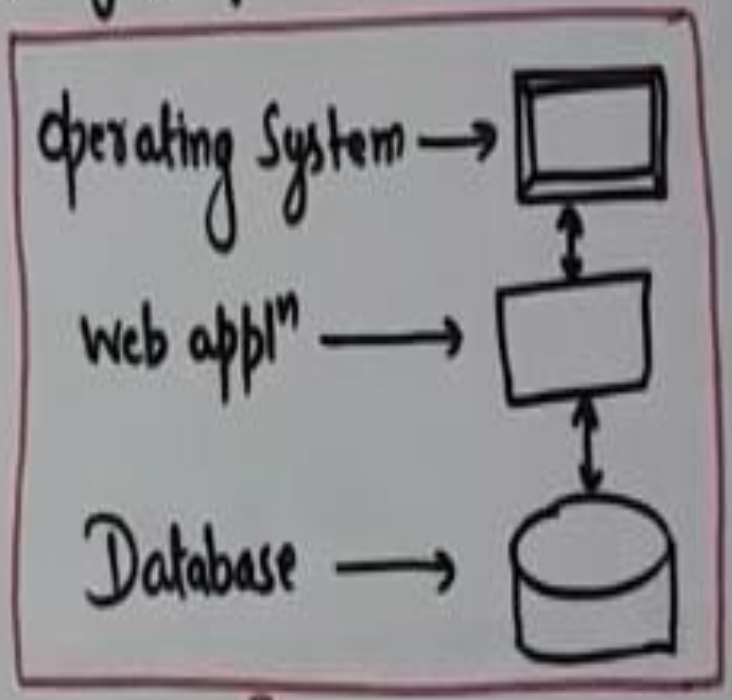
PAAS (Platform-as-a Service)

Platform ⇒ Computing platform [HW, OS, Libraries]

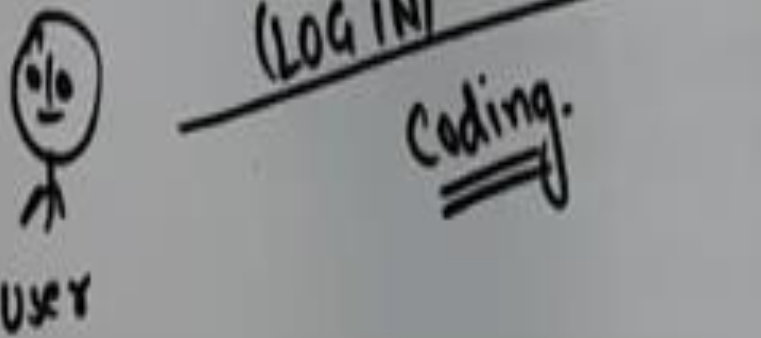
↳ It offers runtime environment for the applications.

↳ Basically provide platform to develop appl^n.

Eg:- Google App Engine, Force.com } Helping the user to Create web appl^n online.



PaaS (Cloud provider)



Benefits of PAAS:

- i) Lower cost] Customer doesn't need to purchase H/w, S/w.
- ii) SCALABILITY] resources can be scale up & Scale down easily.
- iii) Updated S/w System [S/w maintenance is the issue/res. of Vendor]
- iv) Less admin. overhead.
  - (administration is done by cloud provider)

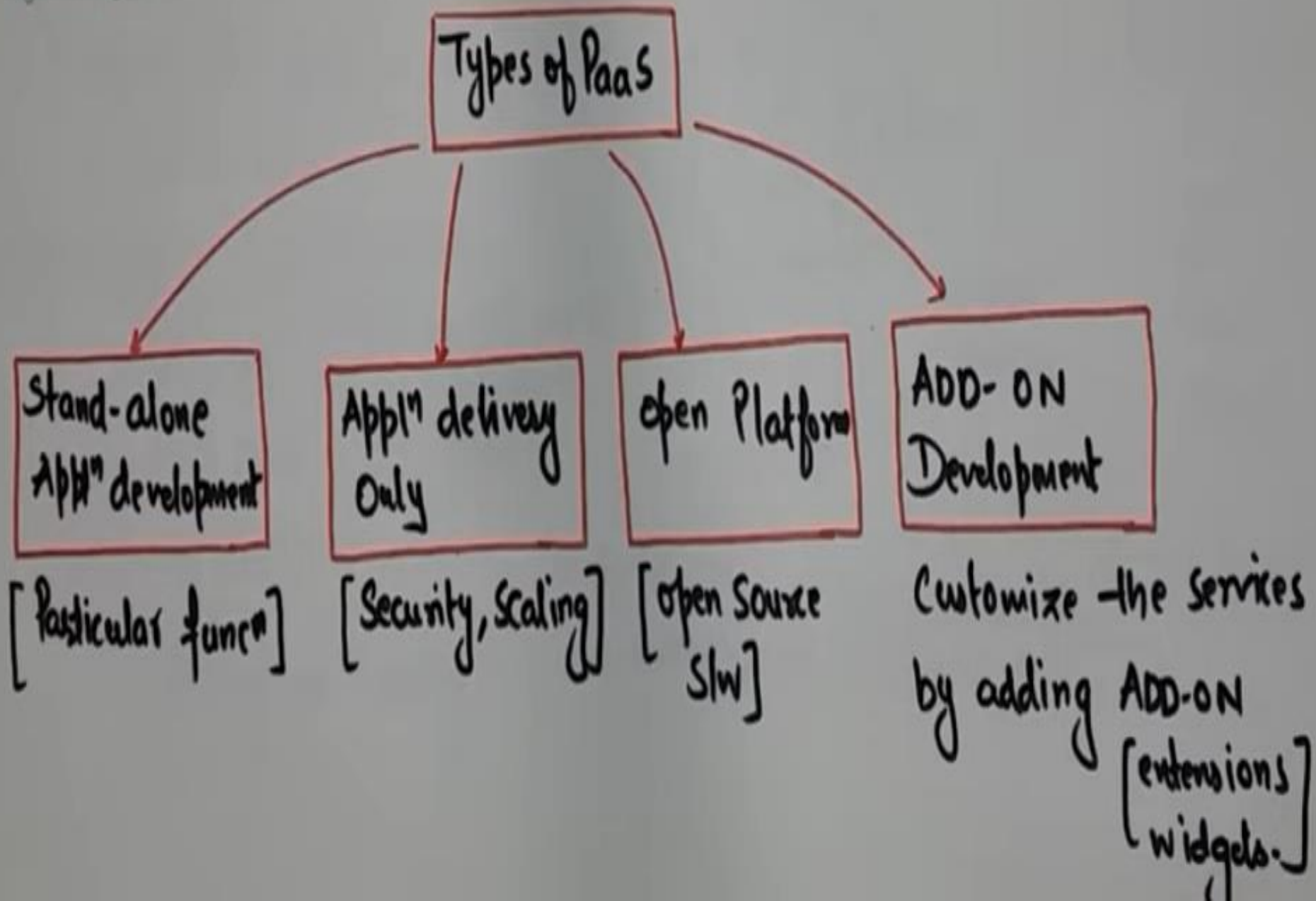
Issues of PAAS:

- i) Portability issue among Paas cloud providers.
- ii) Event based processor scheduling.
- iii) Security. [Latest Cryptographic ALGO should be used].

Characteristics of PAAS:

- i) Browser based environment for the development of appl".
- ii) Secured, Scalable web services
- iii) Easy workflow & Approval process.
- iv) Easy Integration with other applications.

Types of PAAS:-



Software-as–a-Service (SaaS) model allows to provide software application as a service to the end users.

It refers to a software that is deployed on a host service and is accessible via Internet.

There are several SaaS applications listed below:

Billing and invoicing system

- Customer Relationship Management (CRM) applications
- Help desk applications
- Human Resource (HR) solutions

Some of the SaaS applications are not customizable such as **Microsoft Office Suite.**

But SaaS provides us **Application Programming Interface (API),** which allows the developer to develop a customized application.

Characteristics

Here are the characteristics of SaaS service model:

- SaaS makes the software available over the Internet.
- The software applications are maintained by the vendor.
- The license to the software may be subscription based or usage based. And it is billed on recurring basis.
- SaaS applications are cost-effective since they do not require any maintenance at end user side.

- They are available on demand.
- They can be scaled up or down on demand.
- They are automatically upgraded and updated.
- SaaS offers shared data model.
  - Therefore, multiple users can share single instance of infrastructure.
  - It is not required to hard code the functionality for individual users.
- All users run the same version of the software.

Benefits

Using SaaS has proved to be beneficial in terms of scalability, efficiency and performance. Some of the benefits are listed below:

Modest software tools

- Efficient use of software licenses
- Centralized management and data
- Platform responsibilities managed by provider
- Multitenant solutions

Modest software tools

- The SaaS application deployment requires a little or no client side software installation, which results in the following benefits:

- No requirement for complex software packages at client side

- Little or no risk of configuration at client side

- Low distribution cost

Efficient use of software licenses

- The customer can have single license for multiple computers running at different locations which reduces the licensing cost.

- Also, there is no requirement for license servers because the software runs in the provider's infrastructure.

Centralized management and data

- The cloud provider stores data centrally.
- However, the cloud providers may store data in a decentralized manner for the sake of redundancy and reliability.

Platform responsibilities managed by providers

- All platform responsibilities such as backups, system maintenance, security, hardware refresh, power management, etc. are performed by the cloud provider.
- The customer does not need to bother about them.

Multitenant solutions

- Multitenant solutions allow multiple users to share single instance of different resources in virtual isolation.
- Customers can customize their application without affecting the core functionality.

Issues

There are several issues associated with SaaS, some of them are listed below:

- Browser based risks
- Network dependence
- Lack of portability between SaaS clouds

Browser based risks

If the customer visits malicious website and browser becomes infected, the subsequent access to SaaS application might compromise the customer's data.

To avoid such risks, the customer can use multiple browsers and dedicate a specific browser to access SaaS applications or can use virtual desktop while accessing the SaaS applications.

Network dependence

The SaaS application can be delivered only when network is continuously available.

Also network should be reliable but the network reliability cannot be guaranteed either by cloud provider or by the customer.

Lack of portability between SaaS clouds

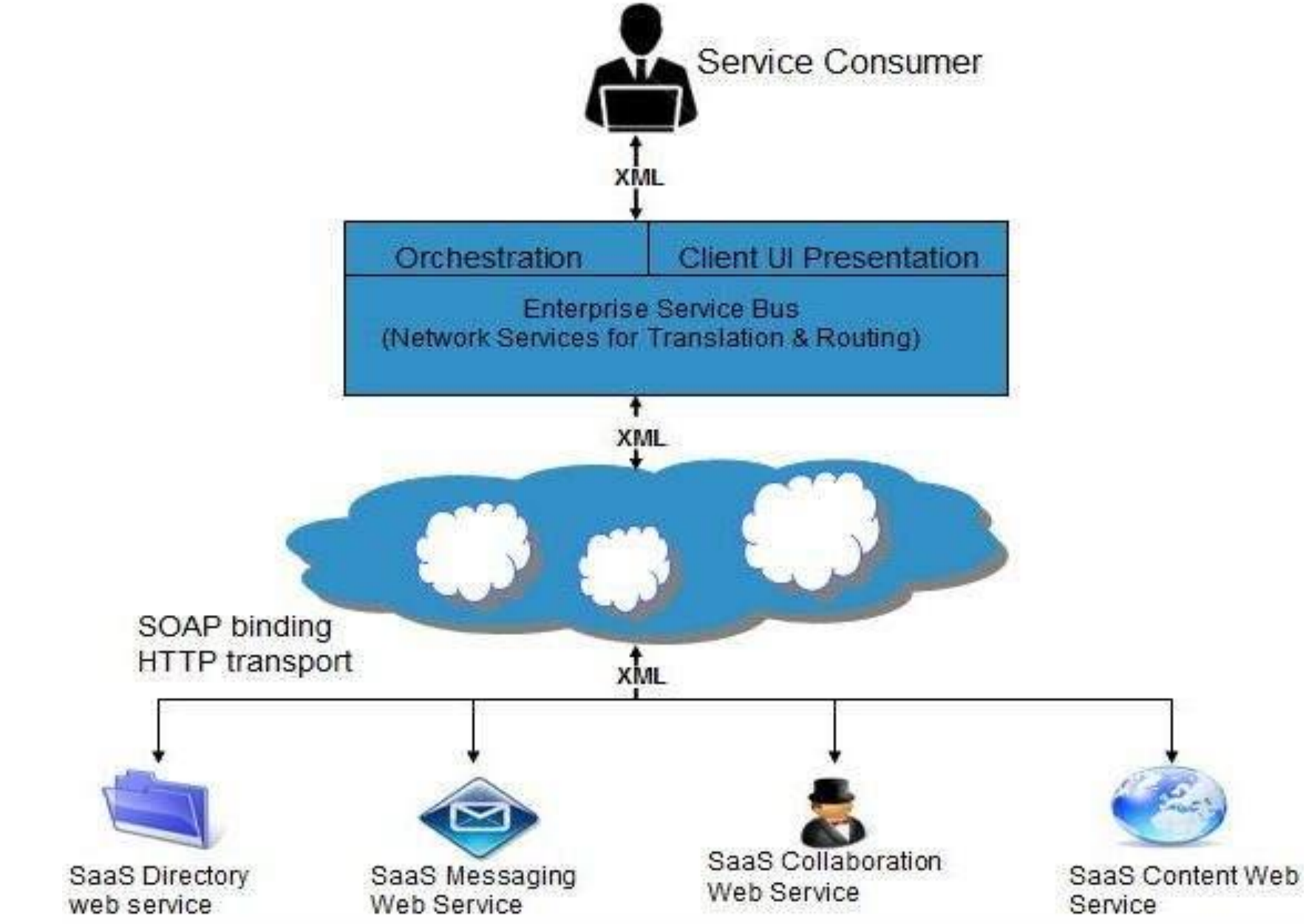
Transferring workloads from one SaaS cloud to another is not so easy because work flow, business logics, user interfaces, support scripts can be provider specific.

Open SaaS and SOA

Open SaaS uses those SaaS applications, which are developed using open source programming language. These SaaS applications can run on any open source operating system and database. Open SaaS has several benefits listed below:

- No License Required
- Low Deployment Cost
- Less Vendor Lock-in
- More portable applications
- More Robust Solution

The following diagram shows the SaaS implementation based on SOA:



Software-as-a-Service: (SaaS)

↳ offers S/W appl" as a Service to the users.

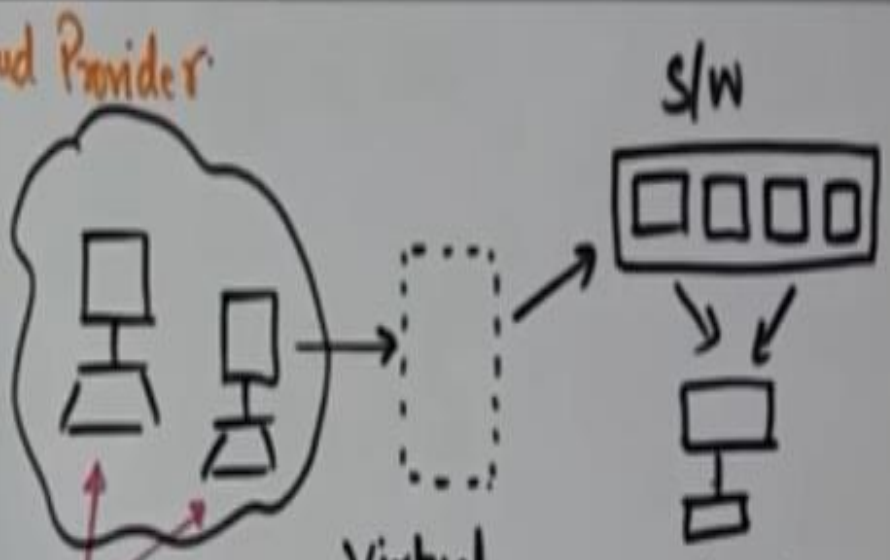
Applications: → (Sales Force)

↳ i) CRM appl". [Customer rel" mgmt]

ii) Help Desk

iii) HR sol"

iv) Billing and Invoicing.



Client-Server technology.

May Pay low cost to use -the S/W.

Characteristics of SAAS:

→ word, excel.

Availability of s/w over internet.

Maintenance of s/w by Vendor.] wfg xaclatio

Subscription or Usage based license.

Cost effective] Pay as per use.

On-demand availability.] anywhere, anytime

Easily scalable as per need.

Works on Shared model. client 1 2 3

Automatic updation of s/w.

↳ Client will always gets to work on the latest version of the s/w.

Benefits of SAAS:

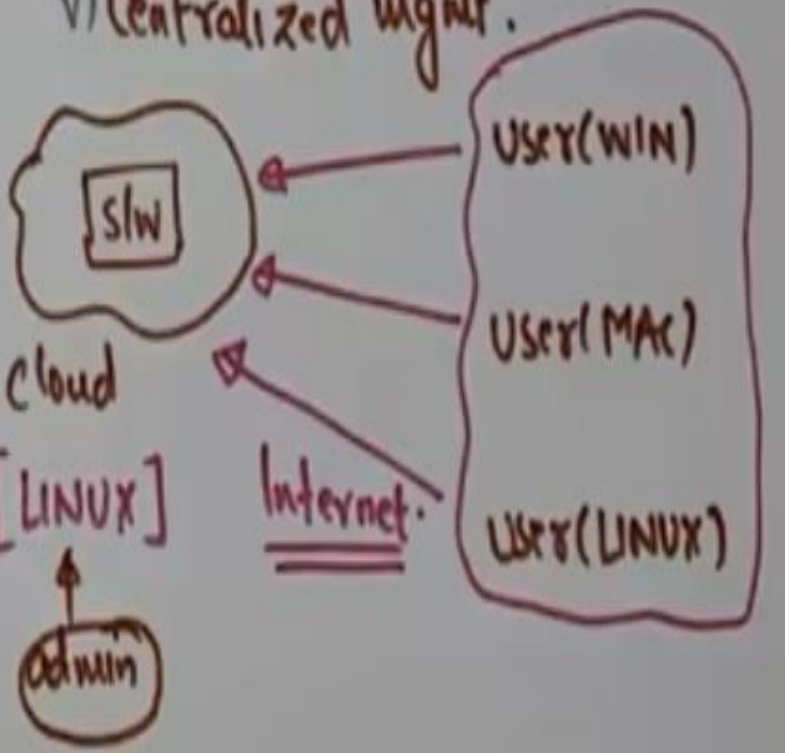
↳ i) Modern s/w tools.

ii) Platform independence to user.

iii) Efficient use of s/w License.

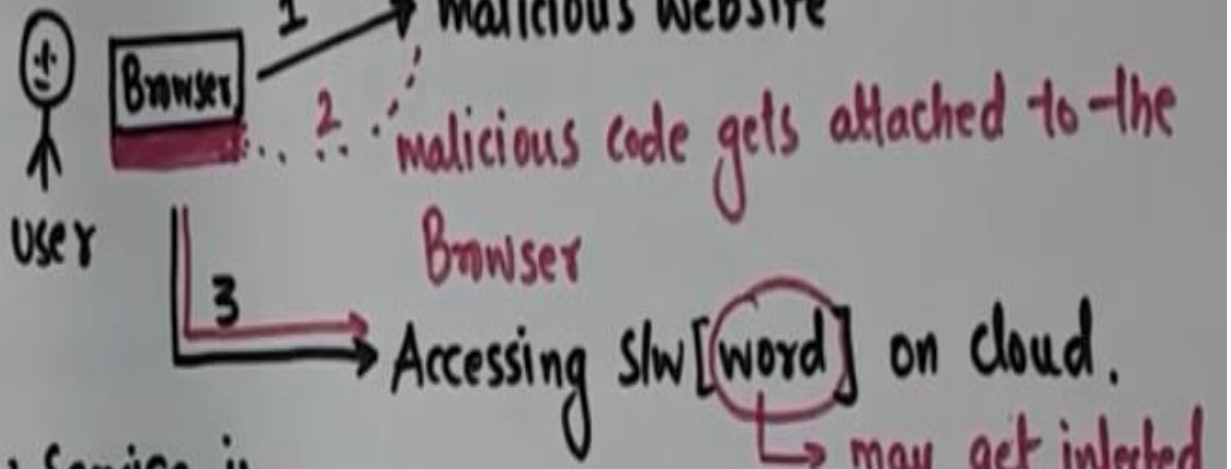
iv) Multitenant sol^{n}.

v) Centralized mgnt.



SAAS ISSUES:-

↳ i) Browser based risks



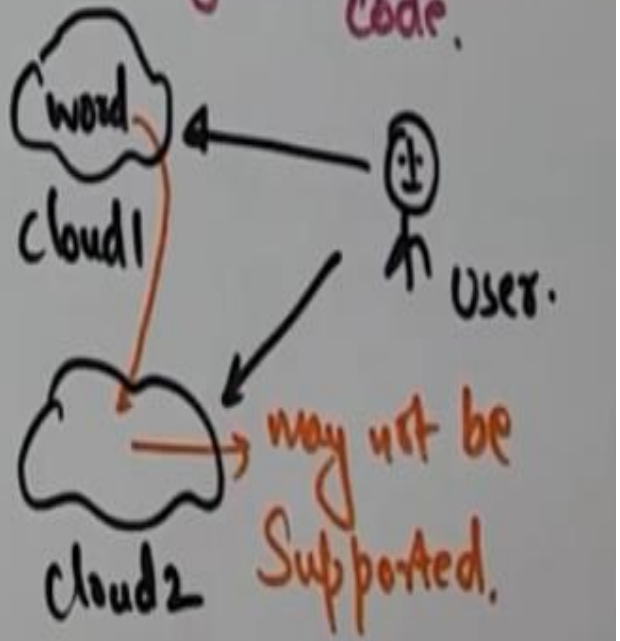
ii) N/w dependence :- S/w Service is available till there is internet Conn^n.

↳ Continuous.

iii) Portability Issues.

↳ among diff. Saas Clouds.

Eg:- NetSuite
ATLT
Intacct



What Is IaaS?

- Infrastructure as a service (IaaS) is a type of cloud computing model that allocates virtualized computing resources to the user through the internet.

- IaaS is one of the main components of cloud computing along with software as a service (SaaS) and platform as a service (PaaS).

- IaaS is completely provisioned and managed over the internet.

- The IaaS technology helps the users to avoid the cost and complexity of purchasing and managing their own physical servers.

- Every resource of IaaS is offered as an individual service component and the users only have to use the particular one they need.

- The cloud service provider manages the IaaS infrastructure while the users can concentrate on installing, configuring and managing their software.

- As the cloud buyers rent a space in the virtual data center of the IaaS provider, they get the access to the virtual data center through the internet.

- IaaS provides the raw materials and basic infrastructure for IT and ensures affordability as the users only have to pay or the resources they use.

- The cloud service providers enable the users to rent the virtual servers and storage while forming networks in order to tie them all together.

- While renting from a cloud IaaS provider, users are essentially renting hardware along with the provisioning software that automates it.

How It Works?

- In the IaaS technology, the cloud service provider hosts the IaaS infrastructure components that are traditionally present in a data center including network hardware, servers, storage and the virtualization of the hypervisor layer.

- The IaaS provider also provides a wide range of services to accompany the infrastructure components.

The Cloud

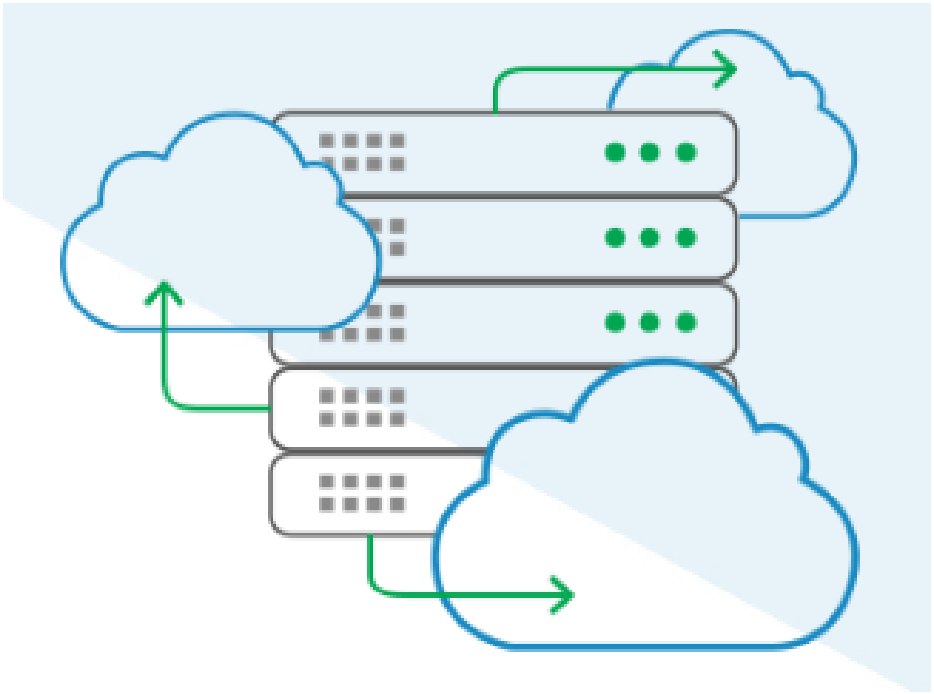
•Just like all the cloud computing services, IaaS provides the users the access to computing resources in a virtualized environment.

•This is done through a public connection usually through the internet.

•IaaS provides the users the access to the virtualized environment for establishing their own IT platforms.

- **Virtualized Hardware**
- IaaS provides resources that are especially belonging to virtualized hardware which is also known as the computing infrastructure.

- The offerings in an IaaS environment include network connections, virtual server space, load balancers and IP addresses.

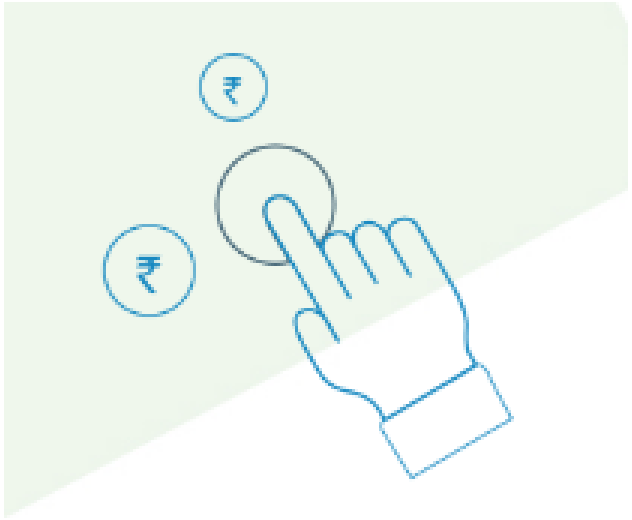


- **Cloud Servers**
- In physical terms, the cloud service provider extracts the pool of hardware resource from a group of servers and networks that are usually spread across various data centers and the cloud service provider is responsible for managing all the resources.

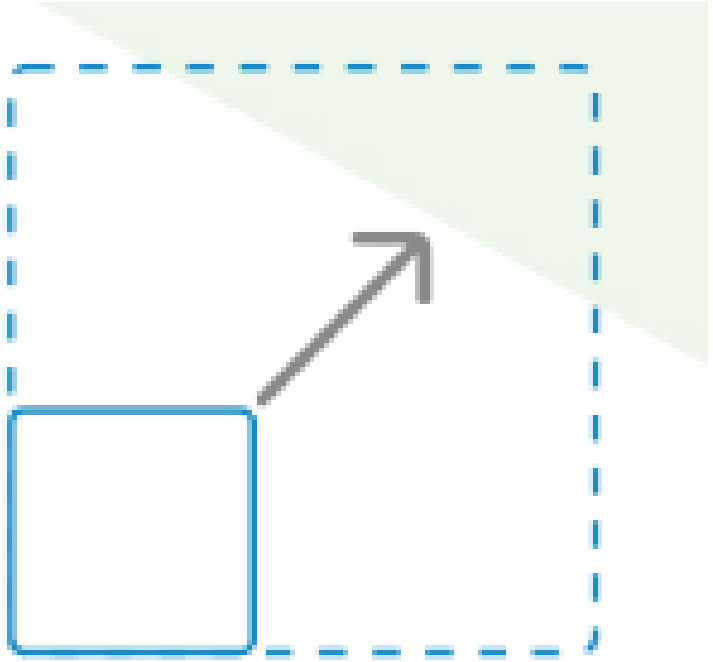
- IaaS provider also offers relative services to the users for supporting the infrastructure components that include
  - monitoring,
  - detailed billing,
  - security,
  - load balancing,
  - clustering along with storage services like data backup, replication and recovery.

- IaaS technology is focused at enabling the users to implement higher levels of automation for the crucial infrastructure tasks.

- Benefits Of IaaS
- IaaS offers many impressive benefits to the customers for ensuring affordability and for easily scaling the IT infrastructure.
- Benefits of implementing the IaaS environment include:
- **Pay Per Use**
  - The IaaS service can be used on demand and the users only have to pay for the resources that are actually used.



- **Scalability**
- The IaaS infrastructure makes sure that the resources are available to the users when they need them.
- Therefore, there are no delays caused in the expansion of capacity and there is no wastage of the unused capacity.

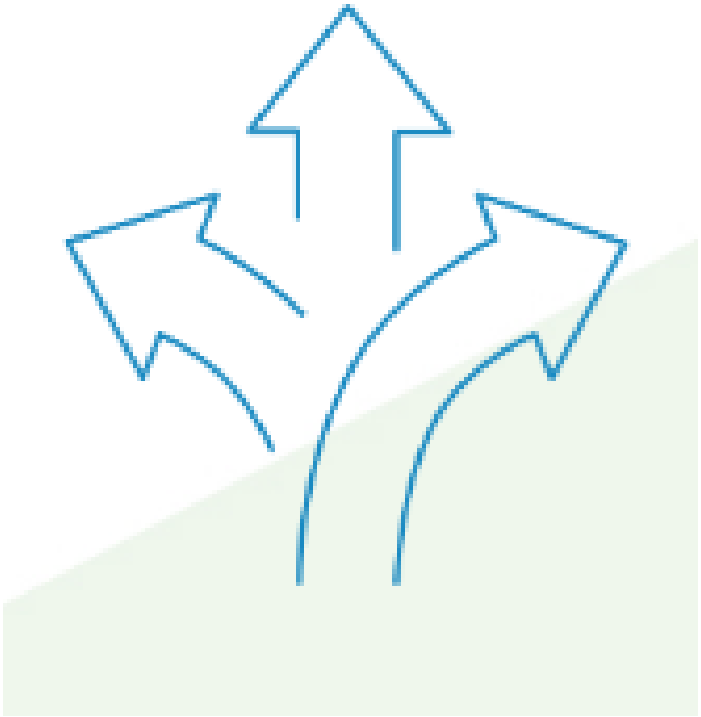


- **Save Time And Cost**
- As the cloud service provider is responsible for setting up and maintaining the underlying physical hardware required for supporting the IaaS environment it saves a lot of time and effort of the users and ensures affordability.

- **Location Independence**
- Users working on the IaaS environment can access it from anywhere in the world through the internet; however, they have to abide by the security protocol of the cloud network.

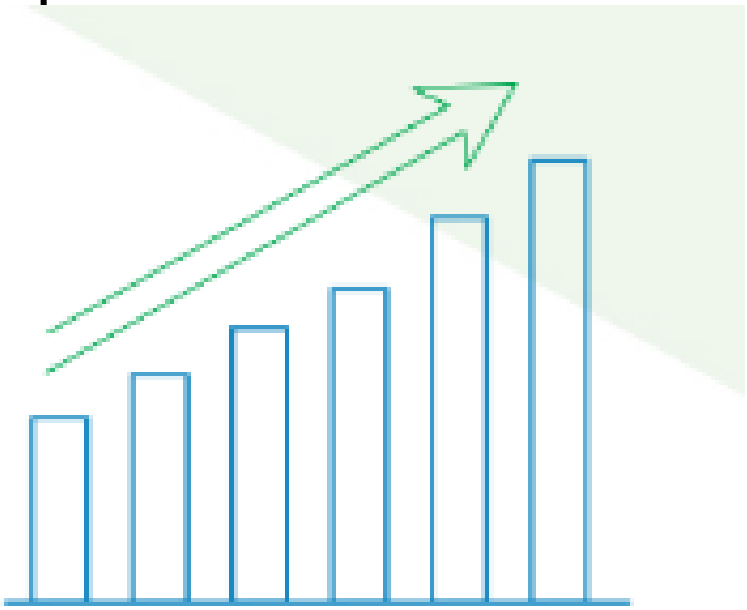
- **Unaffected Service**
- There is no single point of failure in IaaS. Even though any one aspect of the hardware resources fail, the service will remain constant and unaffected.

- **Flexibility**
- One of the greatest benefits of IaaS include the ability to scale the resources up and down quickly according to the needs of the customers.



- **Faster Time To Market**
- Competition is an important factor in every business sector and faster time to market is one of the best ways to stay ahead of the competition.
- As the IaaS environment ensures flexibility and scalability, the business organizations can gear up and get their work done faster.

- **Focus On Business Growth**
- Business owners usually have to spend a lot of time, money and energy on making technology related decisions and recruiting staff for managing and maintaining their IT infrastructure.
- By opting for a service based IaaS model, business organizations can concentrate their time and resources where they are required.



- **Examples Of IaaS**
- **Internal Business Networks**
- Utilization of a pooled server and networking resources is done through which a business can store data and run applications.
- Growing businesses get the ability to scale their infrastructure according to the business growth.

- **Cloud Hosting**
- Hosting websites on virtual severs that are created on the pooled resources on the basis of the underlying physical servers.

- **Virtual Data Centers**
- A virtualized network is established that consists of virtual servers that can be used for offering advanced cloud hosting capabilities, enabling enterprise IT infrastructure or for integrating the operations.

- **What does *Database (DB)* mean?**

- A database (DB), in the most general sense, is an organized collection of data.

- More specifically, a database is an electronic system that allows data to be easily accessed, manipulated and updated.

- In other words, a database is used by an organization as a method of storing, managing and retrieving information.

- Modern databases are managed using a database management system (DBMS).

- ***Database (DB)***
- Software programmers are well acquainted with database concepts through relational databases like Oracle, SQL SERVER and MySQL, etc.

- Typically, a database structure stores data in a tabular format.

- Database architecture may be external, internal or conceptual.

- The external level specifies the way in which every end-user type comprehends the organization of its corresponding relevant data in the database.

- The internal level deals with the performance, scalability, cost and other operational matters.

- The conceptual level perfectly unifies the different external views into a defined and wholly global view.

- It consists of every end-user required generic data.

- Database-as-a-Service (DBaaS) is a service managed by either public or private cloud operators

- Supports data driven applications without having to manage database administration functions.

- Application developers do not have to rely on a database administrator for maintaining the database.

- **Virtualized DBaaS**
- Database functions like server instances, networking and storage are automatic.

- Enables companies to offer a variety of online services to clients whilst automating a significant part of the conventional tasks of purchasing, installing and managing cloud database solutions.

Oracle DBaaS

- Oracle's DBaaS gives their customers the ability to access their Oracle database from anywhere in the world, with full administrative control and managed service options.

- Helps clients develop and use applications by providing full control over dedicated database instances, supporting all database applications and offering users more flexibility and options over their database services.

Getting Started with DBaaS

- Businesses of all sizes are using DBaaS.
- Main advantages are ease of use and scalability that make it easier to deploy and manage the growing demand of data-driven apps.
- In addition, DBaaS can significantly reduce operational overhead.

Database as a Service (DBaaS)

- Database as a service (DBaaS) is a cloud computing service model that provides users with some form of access to a database without the need for setting up physical hardware, installing software or configuring for performance.

- All of the administrative tasks and maintenance are taken care of by the service provider so that all the user or application owner needs to do is use the database.

- If the customer opts for more control over the database, this option is available and may vary depending on the provider.

- Database as a service is one of cloud computing's secondary service models and a key component of XaaS.

- This may be considered a subspecialty under the bigger software as a service model umbrella.

- In essence, DBaaS is a managed service offering access to a database to be used with applications and their related data.

- This is a more structured approach compared to storage as a service, and at its core it is really a software offering.

- In this model, payment may be charged according to the capacity used as well as the features and use of the database administration tools.

- DBaaS consists of a database manager component, which controls all underlying database instances via an API.

- This API is accessible to the user via a management console, usually a web application, which the user may use to manage and configure the database and even provision or deprovision database instances.

- Database-as-a-Service (DBaaS) more commonly known as “Managed Databases”, took off when AWS introduced its Relational Database Service (RDS) in 2009.
- Since then it has become the fastest growing cloud service with some estimates projecting a market of $320 billion by 2025.
- The reason for this meteoric growth is the proven value of Database-as-a-Service in enabling a fast time-to market by improving productivity, standardization and data security.

- Database-as-a-Service defined as

- The term “Database-as-a-Service” (DBaaS) refers to software that enables users to setup, operate and scale databases using a common set of abstractions (primitives), without having to either know nor care about the exact implementations of those abstractions for the specific database.

- For example, a developer could instantiate a database instance using the same set of API calls or UI clicks regardless of whether the database was MySQL, Oracle or MongoDB.

- Similarly, the IT admin user could request a backup of the database, or create and resize a database cluster using the same call regardless of the particular database being used.
- It’s the platform’s responsibility to implement backup, cluster resizing or any other abstract operation correctly for each of the underlying databases that the platform supports

- Setup
- Setting up a database involves provisioning a VM on which to run it, installing the database, and configuring it according to a set of parameters.
- IT administrators managing the platform can choose to setup databases for their consumers, or enable a self-service model in which developers and DevOps create databases either through an enterprise portal, an SDK, or even using automation tools like Terraform.
- The self-service model has the advantage of zero IT intervention, freeing up IT admins for more important tasks.
- Using DBaaS, the time required to setup a database can be reduced from weeks to minutes.

- Operate
- Once a database has been setup, the platform is responsible for all the back end operations to maintain it in good health.

- These include configuration management, automating backups (and enabling easy restore when needed), patches and upgrades, DR, service monitoring (both for the database and the underlying infrastructure) and more.

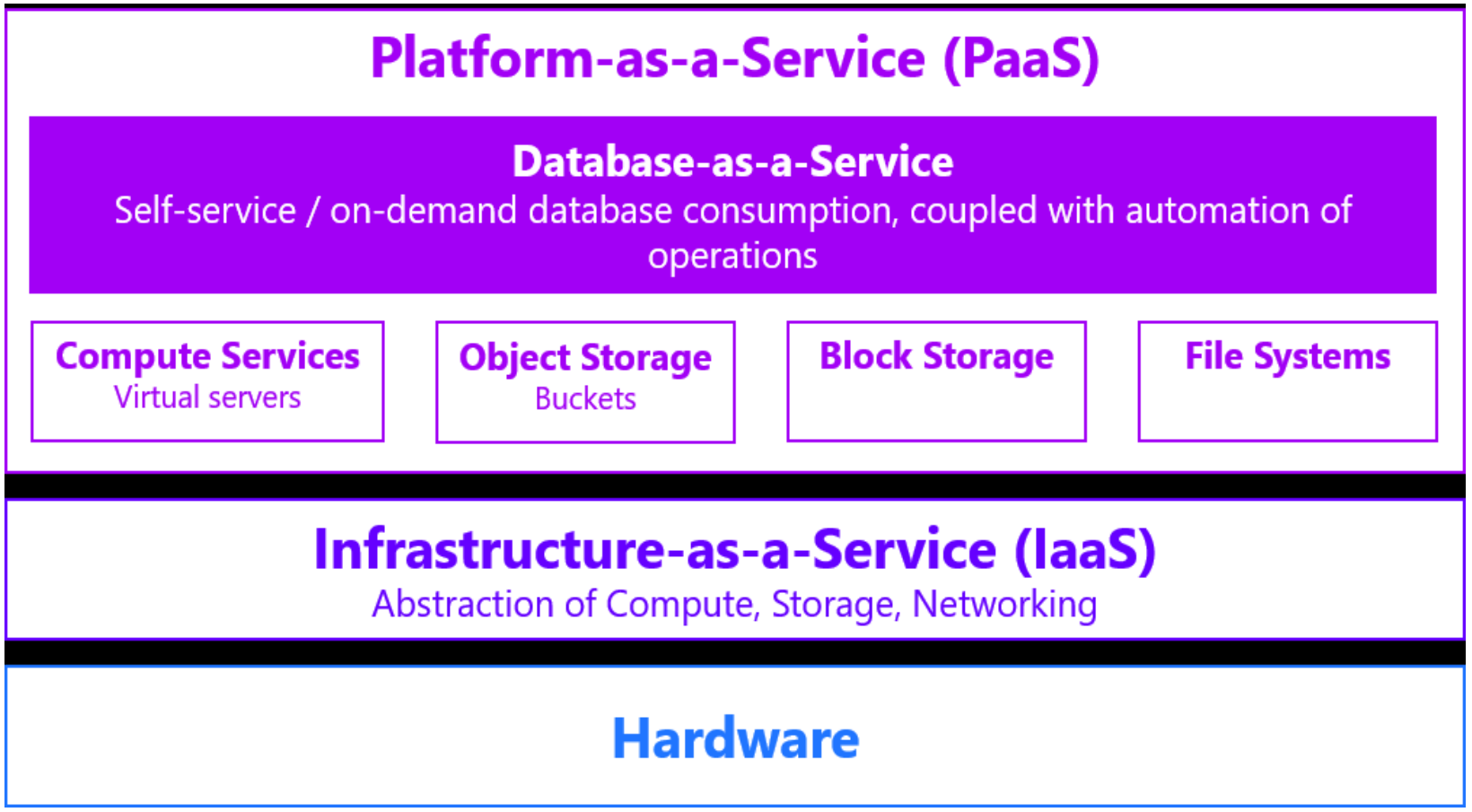
- All of these capabilities are provided to the IT administrator as easy single-click operations rather than the complex procedures they would have been without a DBaaS platform.

- Scale
- To accommodate increased usage of an application as it evolves and matures, the platform should automatically scale up database instances as needed according to a set of policies.

- For example, as usage grows beyond a certain threshold, data from a master instance can be automatically distributed to one or more read replica instances.

- Once data has been distributed over multiple instances, one of the read replicas can also be used for failover.

- DBaaS on IaaS
- DBaaS is often delivered as a component of a more comprehensive platform, which may provide additional services such as Infrastructure-as-a-Service (IaaS).
-
- The DBaaS solution would request resources from the underlying IaaS, which would automatically manage the provisioning compute, storage and networking as needed essentially removing the need for IT to be involved.



- Database as a Service Metrics: Assessing the Value of DBaaS

- Who uses DBaaS
- It is important to understand that like other cloud technologies, DBaaS has two primary consumers:
  - The IT organization which manages and maintains the cloud
  - The end user who consumes the cloud resources, typically, developers and DevOps.

- The IT organization deploys the DBaaS solution enabling end users (developers and DevOps) to provision a database of their choice, on-demand, from a catalog of supported databases, which could include both relational and non-relational databases.

- The IT organization can configure the DBaaS to support specific releases of these software titles, and can further restrict the configurations that specific users can provision.

- For example, developers may only be allowed to provision databases with a small memory footprint using traditional disks while DevOps could provision higher capacity servers with SSD's.

- Finally, the IT organization can setup policies for standard database operations like backups, DR and security policies to ensure that the data is properly saved from time to time to allow for recovery when required.

- Typically, an end user would access the DBaaS system through a portal that offers a selection of different database titles, and in a variety of different configuration options.

- With a few clicks, the user specifies the required database and its corresponding configuration for provisioning.

- The benefits of DBaaS
  - A DBaaS solution provides an organization a number of benefits, the main ones being:
  - Developer agility
  - IT productivity
  - Application reliability and performance
  - Application security

- Developer agility
- Deploying a database is a multi-step process including the provisioning of compute, storage and networking components, configuring them properly and installing the database software.

- In most enterprises, this process must go through the organization's IT department and is typically, something like the following:

1. Developer opens a request in the IT ticketing system

2. Ticket sits in the queue until it gets to the top of the list according to IT priorities

3. IT evaluates ticket, and if the request is approved goes about allocating the required compute, storage and networking resources needed for the developer's database (in some cases, each of these is also handled by a separate sub-department which has its own ticketing system and set of priorities)

4. IT configures the allocated resource
5. IT installs and configures the database to utilize the underlying infrastructure according to its internal policies
6. IT provides the developer with an entry point to the database and the developer takes it from there.

- IT productivity
- IT is responsible for the day-two operations of the enterprise's databases including things like tuning, configuration, monitoring, patching, upgrading, resizing periodic backups, and so on;

- all the things that must be done to keep databases in proper working order.

- As enterprises grow, and with them, the number and types of databases that must be managed and maintained, IT resources get stretched very thin (explaining the long lead time that developers have to wait before IT provisions them with a database).

- Application reliability and performance
- Modern DBaaS solutions make it easy to keep your databases highly available and running at peak performance.

- Through support for read replicas, in the event of a failure, the system automatically reroutes traffic to a replica ensuring system availability at all times.

- The system also monitors your databases to identify increased demand on resources.

-

- Using scaling policies based on resource usage thresholds, you can configure the system to automatically scale out by provisioning additional resources as demand increases, and then scale back in once demand is reduced releasing resources for other applications.

- Application security
- Many database engines natively provide security features such as data encryption both at rest and in transit, each using its own data structures and APIs.

- A DBaaS solution provides consistent management of security for all the different types of databases you might use in your organization, while adding some security features of its own.

- In addition to native data encryption, you might look for things like end-to-end network security with micro-segmentation, virtual private networks and security groups.

- A DBaaS solution might also integrate with common enterprise user stores such as LDAP and Active Directory for user authentication, and then apply fine-grained access control via different permission policies.

- Solving cloud challenges with on-premises DBaaS
- While anything that is “as-a-Service” is immediately associated with the public cloud, you shouldn’t automatically jump to that conclusion.

- While most DBaaS offerings will provide things like self-service provisioning, lifecycle management and autoscaling, there are some challenges with public cloud DBaaS solutions that are solved when you go on-premises.

- Public cloud data costs can be high and unpredictable
- If you keep your data on the public cloud, estimating the costs associated with that data can be a bit of a crap-shoot.

- Rates on everything from data overage to data transfer frequently change.

- Not only that, prices can vary between the different availability regions of a public cloud provider.

- Then there's the phenomenon of "data gravity" – the larger the body of data you store on the cloud, the larger the number of applications and services that will use it – and those all come at more unpredictable cost.

- These costs can easily spiral out of control to the extent that some companies are finding themselves spending hundreds of millions of dollars a year to have their data with public cloud providers.

- While maintaining the storage and compute power needed to maintain your databases on-premises does have associated costs, these costs are much easier to predict and control compared to public cloud DBaaS solutions.

- DBaaS empowers both developers and IT
- Most enterprises today operate applications that require several different database technologies, a departure from recent years where the ‘corporate standard’ mandated a single database solution for all application needs.

- Database-as-a-Service provides a framework within which enterprises can operate all these different databases.

- It provides end users with improved agility through simplified provisioning and operation, and the flexibility to choose from a number of pre-configured options established by the IT organization.

- DBaaS also improves the operation of fleets of diverse databases through automation and standardization allowing IT organizations
  - to cost-effectively offer their users a number of database choices
  - while also ensuring that these databases are operated in a safe and secure way and in compliance with established best practices.

•Challenges With Cloud

–Defining Cloud Security

- It is a set of control-based technologies & policies adapted to stick to regulatory compliances, rules & protect data application and cloud technology infrastructure.

- Because of cloud's nature of sharing resources, cloud security gives particular concern to identity management, privacy & access control.

- So the data in the cloud should have to be stored in an encrypted form.

- With the increase in the number of organizations using cloud technology for a data operation, proper security and other potentially vulnerable areas became a priority for organizations contracting with cloud providers.

- Cloud computing security processes the security control in cloud & provides customer data security, privacy & compliance with necessary regulations.

•Security Planning for Cloud

- Before using cloud technology, users should need to analyze several aspects.

- <u>These are:</u>
  - Analyze the sensitivity to risks of user's resources.
  - The cloud service models require the customer to be responsible for security at various levels of service.
  - Understand the data storage and transfer mechanism provided by the cloud service provider.
  - Consider proper cloud type to be used

•Cloud Security Controls

- Cloud security becomes effective only if the defensive implementation remains strong.

- There are many types of control for cloud security architecture; the categories are listed below:
  - Detective Control: are meant to detect and react instantly & appropriately to any incident.
  - Preventive Control: strengthen the system against any incident or attack by actually eliminating the vulnerabilities.
  - Deterrent Control is meant to reduce attack on cloud system; it reduces the threat level by giving a warning sign.
  - Corrective Control reduces the consequences of an incident by controlling/limiting the damage. Restoring system backup is an example of such type.

•Understand the data security

- As we all know the data is transferred via the internet, so one of the major concerns is data security.
- The major points that one should adopt to secure cloud data are:
  - Access Control
  - Auditing
  - Authentication
  - Authorization

•Cloud Security Alliance(CSA) Model

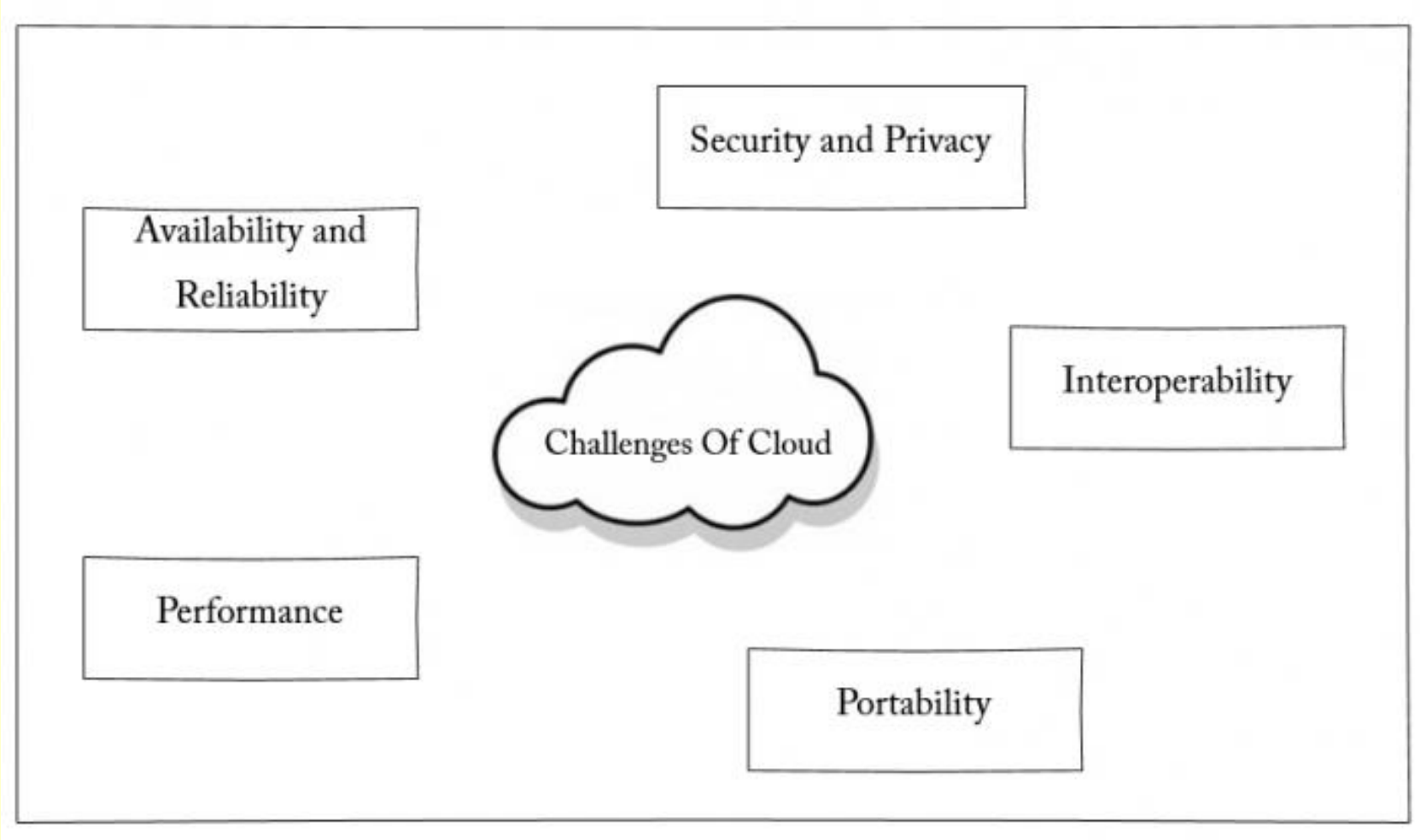
- This stack model defines the boundaries of each service model & shows with how much variation the functional units relate to each other.
- It is responsible for creating the boundary between the service provider & the customer.

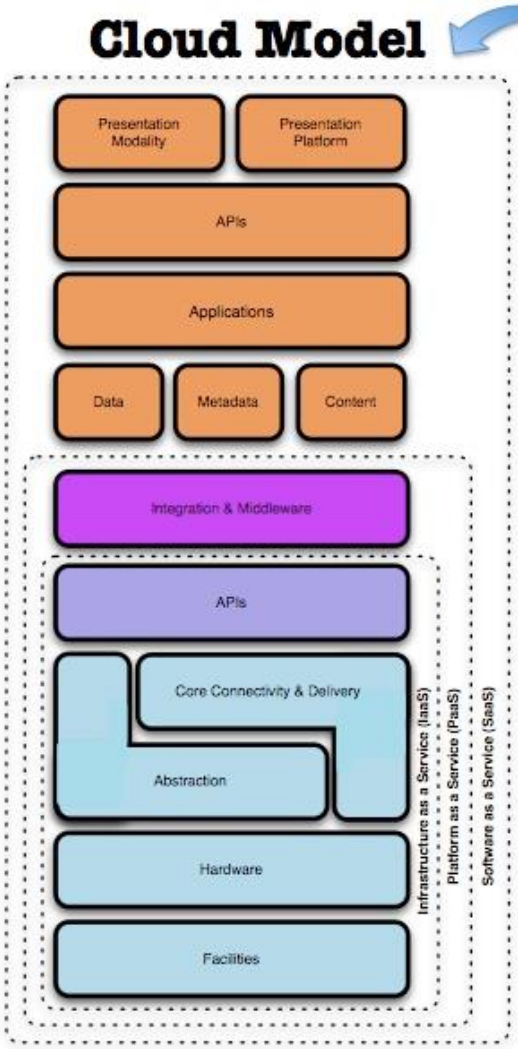
- <u>CSA Model's Key Points:</u>
  - IaaS is the most basic level among all services.
  - Each of the services inherits the capabilities and security concerns of the model beneath.
  - The infrastructure, platform for development & software operating environment are provided by IaaS, PaaS & SaaS respectively.
  - The security mechanism below the security boundary must be built into the system that is required to be maintained by the customer.

- **Encrypt Cloud Data**
- Encryption protects data from being compromised.
- It helps in protecting data that is being transferred & stored in the cloud.
- Encryption helps both protect unauthorized access along with the prevention of data loss.

- **Challenges of Cloud Computing**
- This emergent cloud technology is facing many technological challenges in different aspects of data & information handling & storage.
- Some of the challenges are as follows:
  - Availability & reliability
  - Security & Privacy
  - Interoperability
  - Performance
  - Portability

Challenges of Cloud Computing





Find the Gaps!

Security Control Model

Applications	SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
Information	DLP, CMF, Database Activity Monitoring, Encryption
Management	GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
Network	NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
Trusted Computing	Hardware & Software RoT & API's
Compute & Storage	Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
Physical	Physical Plant Security, CCTV, Guards

Compliance Model

PCI

- ☑ Firewalls
- ☑ Code Review
- ☑ WAF
- ☑ Encryption
- ☑ Unique User IDs
- ☑ Anti-Virus
- ☑ Monitoring/IDS/IPS
- ☑ Patch/Vulnerability Management
- ☑ Physical Access Control
- ☑ Two-Factor Authentication...

HIPAA

GLBA

SOX

- **Security Threats and Vulnerabilities**
- Basic Security Risk Considerations
  - Organizational Security Risks
    - Organizational risks are categorized as the risks that may impact the structure of the organization or the business as an entity.
    - If a CSP goes out of business or gets acquired by another entity, this may negatively affect their CSPs since any Service Level Agreements (SLA) they had may have changed and they would then have to migrate to another CSP that more closely aligns with their needs.
    - In addition to this, there could be the threat of malicious insiders in the organization who could do harm using the data provided by their CSCs.

- Physical Security Risks
  - The physical location of the cloud datacenter must be secured by the CSP in order to prevent unauthorized on-site access of CSC data.
  - Even firewalls and encryption cannot protect against the physical theft of data.
  - Since the CSP is in charge of the physical infrastructure, they should implement and operate appropriate infrastructure controls including staff training, physical location security, network firewalls.
  - It is also important to note that the CSP is not only responsible for storing and process data in specific jurisdictions but is also responsible for obeying the privacy regulations of those jurisdictions.

- Technological Security Risks
  - These risks are the failures associated with the hardware, technologies and services provided by the CSP.
  - In the public cloud, with its multi tenancy features, these include resource sharing isolation problems, and risks related to changing CSPs, i.e. portability.
  - Regular maintenance and audit of infrastructure by CSP is recommended.
- Compliance and Audit Risks
  - These are risks related to the law.
  - That is, risks related to lack of jurisdiction information, changes in jurisdiction, illegal clauses in the contract and ongoing legal disputes.
  - For example, depending on location, some CSPs may be mandated by law to turn over sensitive information if demanded by government.

- Data Security Risks
  - There are a variety of data security risks that we needto take into account.
  - The three main properties that we need to ensure are data integrity, confidentiality and availability.
  - We will go more into depth on this in the next subsection since this is the area most at risk of being compromised and hence where the bulk of cloud security efforts are focused.

- These risk categories have been split between CSPs and CSCs and are illustrated in the following diagram.
- 1. CSP(Cloud Service Provider)

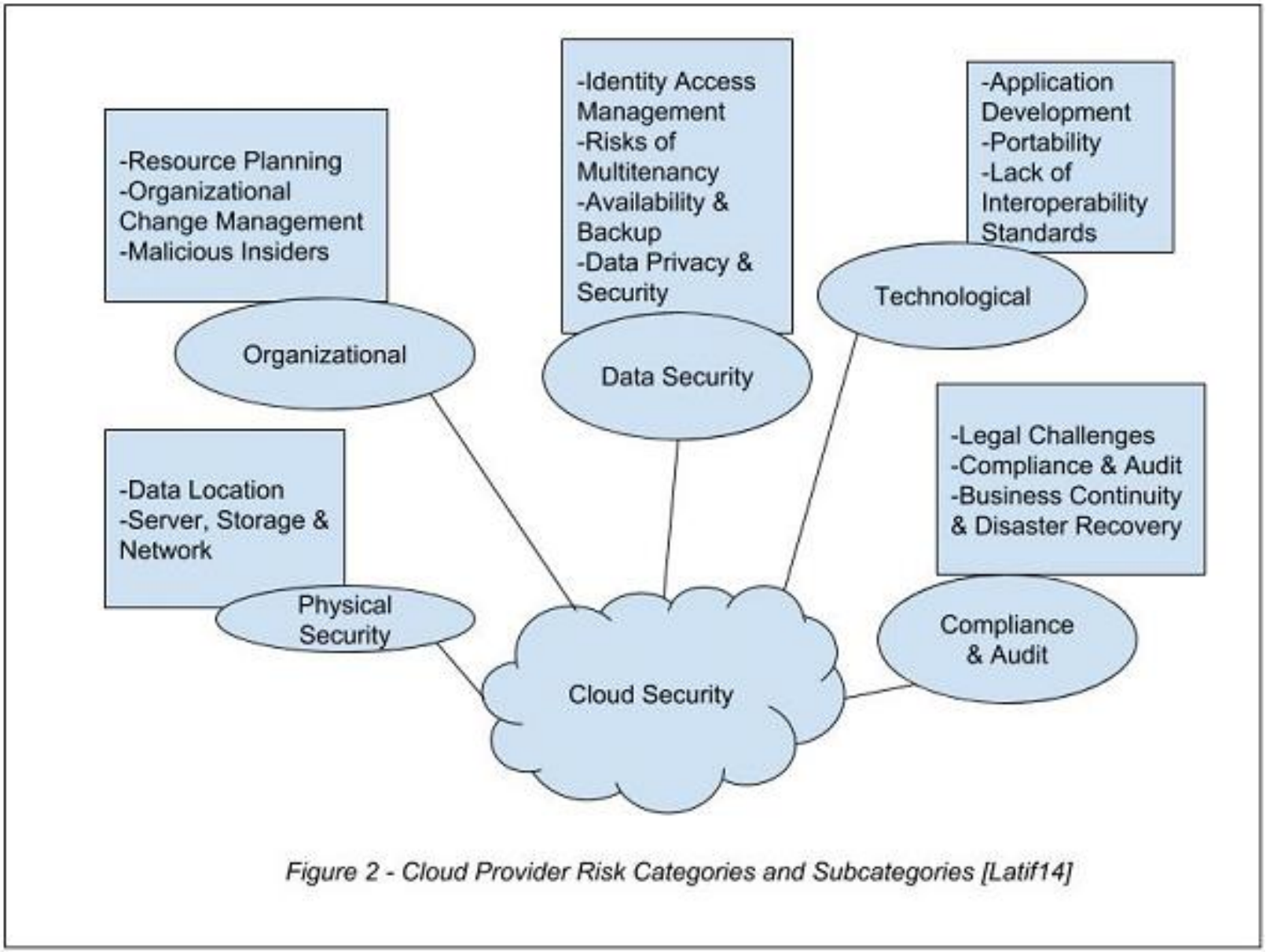


Figure 2 - Cloud Provider Risk Categories and Subcategories [Latif14]

2. CSC(Cloud Service Customer)

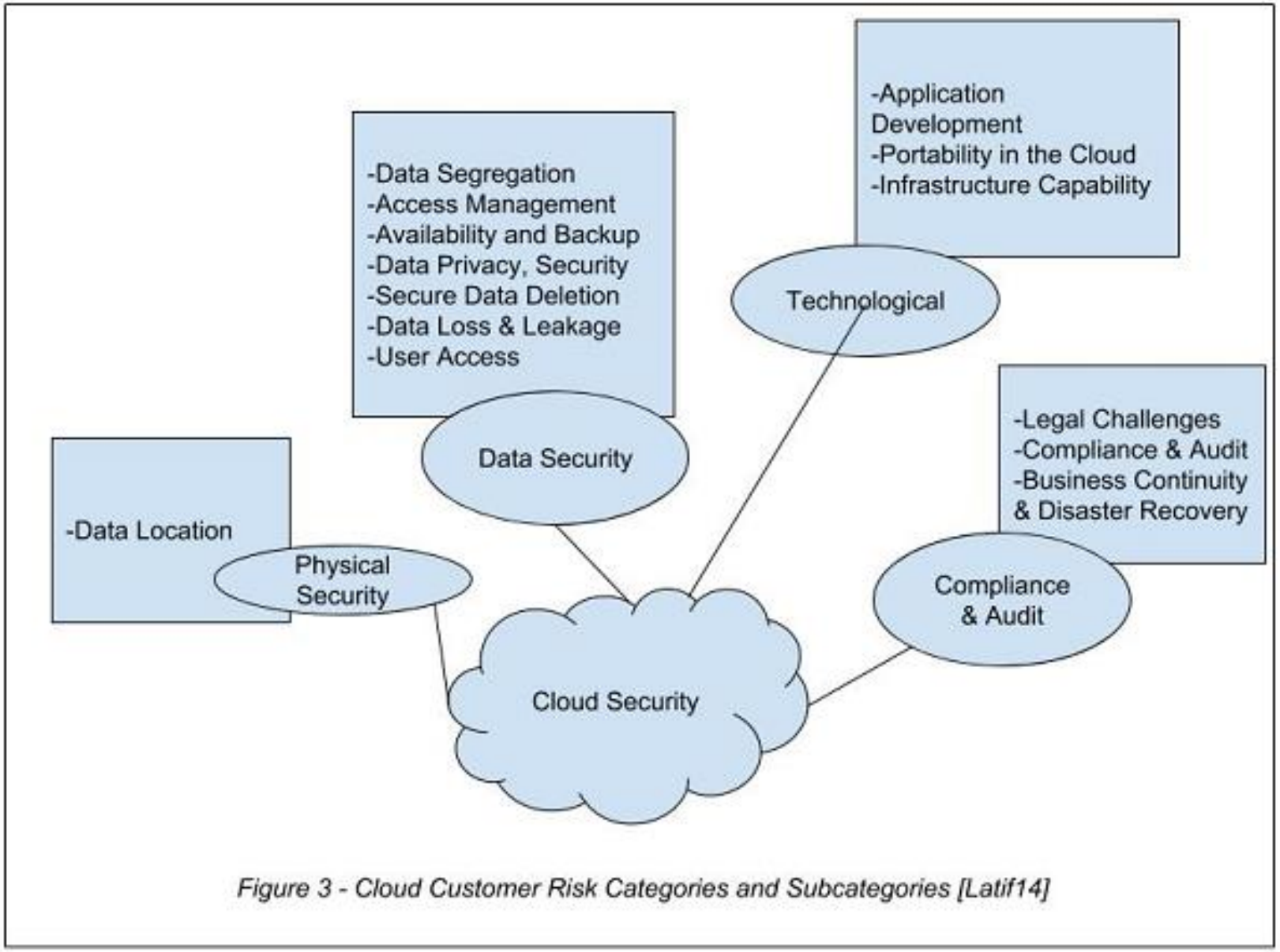


Figure 3 - Cloud Customer Risk Categories and Subcategories [Latif14]

- Data Security Considerations
  - At the heart of all computing is arguably the processing of data into meaningful information.
  - As such, when the processing and storage of such data is outsourced to infrastructure owned and maintained by a third party, this leads to a host of issues to consider when securing said data.
  - These issues are especially more pronounced in the public cloud, since multiple parties, some of which could be malicious, have to share this aforementioned infrastructure.

- Data Security Properties
- Privacy
- Confidentiality
- Integrity
- Availability

– Privacy

- Privacy is one of the more important issues to deal with in the cloud and in network security in general.
- Privacy ensures that the personal information and identity of a CSC are not revealed to unauthorized users.
- This property is most important to the CSC, especially when they deal with sensitive data.

- Confidentiality
  - This is related to data privacy since this is the property ensuring that the data that belongs to a CSC is not revealed to any unauthorized parties.
  - In public clouds, the CSP is mainly responsible for securing the CSC's data.
  - This is particularly difficult due to multi tenancy, since multiple customers have access to the same hardware that a CSC stores its data.
  - Some providers use job scheduling and resource management, but most providers employ virtualization to maximize the use of hardware
  - These two methods allow attackers to have full access to the host and cross- VM side channel attacks to extract information from a target VM on the same machine.

- Integrity
  - The integrity of data refers to the confidence that the data stored in the cloud is not altered in any way by unauthorized parties when it's being retrieved, i.e. you get out what you put in.
  - To ensure this, CSPs must make sure that no third party has access to data in transit or data in storage. Only authorized CSCs should be able to change their data.
- Availability
  - This property ensures that the CSC has access to their data, and are not denied access erroneously or due to malicious attacks by any entity.
  - Attacks like denial-of-service are typically used to deny availability of data.

- Data Stages
  - The flow of data through a cloud goes through various distinct stages, with each stage requiring one or more of the previous properties to be maintained.
  - These stages are as follows
  - Data-in-transit
  - Data-at-rest
  - Data-in-use

  - Data-in-transit
    - This is when data is in the process of being transmitted either to the cloud infrastructure or to the computing device used by the CSC.
    - Here, data is most at risk of being intercepted, hence violating confidentiality.

    - Encryption is generally used here to prevent this, along with other methods we shall detail later.

– Data-at-rest

- This is when data has been stored in the cloud infrastructure.
- The main issue with this stage for the CSC is their loss of control over the data.
- The onus of defending against attacks at this stage hence fall on the CSP.
- They have to ensure that all 4 of the data security properties outlined are upheld at this stage.

– Data-in-use

- This is when data is being processed into information.
- Here, the issues might lie with the corruption of data while it is being processed.
- In order to prevent this the integrity of data going into a process must be ensured using any one of the applicable methods

- Methods to Ensure Security in Cloud
- Countermeasures for Security Risks
  - Organizational Security Risks
  - Physical Security Risks
  - Technological Security Risks
  - Compliance and Audit Risks

  - Organizational Security Risks
    - Malicious Insiders - The risk of having malicious personnel in a CSPs staff can be mitigated by putting strict legal constraints in contracts when hiring personnel.
    - A comprehensive assessment of the CSP by a third party, as well as a robust security breach notification process will also go a long way to preventing this.

– Physical Security Risks

- Physical Breach - The risk of intruders gaining physical access to devices used in the provision of cloud services can be reduced by having strong physical security deterrents in place such as armed guards, keycard access and biometric scans to restrict access to sensitive locations in the data center.

– Technological Security Risks

- Virtualized defense and reputation based trust management - CSP could use the following structure:
- a hierarchy of DHT-based overlay networks, with specific tasks to be performed by each layer.
- The lowest layer deals with reputation aggregation and probing colluders.
- The highest layer deals with various attacks.
- Reputation aggregation here is related to utilizing various sources to verify certain connections, and probing colluders refers to checking if any sources are associated with known malignant parties.

- Secure virtualization - CSP can use an Advanced Cloud Protection system (ACPS) to ensure the security of guest virtual machines and of distributed computing middleware.

- Behavior of cloud components can also be monitored by logging and periodic checking of executable system files.

- Trust model for interoperability and security - There should be separate domains for providers and users, each with a special trust agent.

- A trust agent is an independent party that collects security information used to verify an endpoint [Wiki1] .

- There should also be different trust strategies for service providers and customers.

– Compliance and Audit Risks

- This area primarily deals with legal issues and as such, both CSPs and CSCs need to understand legal and regulatory obligations and ensure that any contracts made meet these obligations.

- The CSP should also ensure that its discovery capabilities do not compromise security and privacy of data .

- Having seen some methods used to prevent lapses in security from the other four areas,

- Methods to ensure Data security
  - Authentication in the Cloud
  - Encryption techniques in the cloud

  - Authentication in the Cloud
    - Since cloud computing is associated with having users‘ sensitive data stored both with a CPC and a CSP, identity and access management (IAM), a form of access control, is very crucial.
    - Authentication for the CPC can be done either by the CSP or outsourced to third party specialists.
    - Some methods for authentication include the identity-based hierarchical model for cloud computing (IBHMCC) and the SSH Authentication Protocol (SAP).
    - This is used mainly to protect data privacy and confidentiality.

- IAM ensures regulatory compliance by managing the major security concerns - authentication, automated provisioning and authorization services.

- Other underlying technologies usedfor authentication, authorization and access control services are OpenID, OAuth, SAML, XACML.

- The trusted computing group‘s (TCG's) IF-MAP standard further allows for real-time communication between a cloud service provider and the customer about authorized users and other security issues

– Encryption techniques in the cloud

- For securing data both at rest and in transit, cryptographic encryption mechanisms are certainly the best options.
- In transit, homomorphic encryption is one such mechanism.
- This involves processing on an encryption domain.
- Other methods such as searchable encryption are also employed, so that data does not need to be decrypted to be accessed unlike with homomorphic encryption.
- Sample Encryption Algorithms
  - Caesar Cipher
  - S-DES
  - RSA
  - Secure Socket Layer (SSL)

Top Security Threats

- Abuse and nefarious use of cloud computing
- Insecure interfaces & API’s
- Unknown risk profile
- Malicious insiders
- Shared technology issues
- Data loss or leakage
- Account or service hijacking

Threat Mitigation

Abuse and nefarious use of cloud computing	▪ Stricter initial registration and validation processes. ▪ Enhanced credit card fraud monitoring and coordination. ▪ Comprehensive introspection of customer network traffic. ▪ Monitoring public blacklists for one's own network blocks.
Insecure interfaces & API's	▪ Analyze the security model of cloud provider interfaces. ▪ Ensure strong authentication and access controls are implemented in concert with encrypted transmission. ▪ Understand the dependency chain associated with the API.
Unknown risk profile	▪ Disclosure of applicable logs and data. Partial/full disclosure of infrastructure details ▪ Monitoring and alerting on necessary information.

Threat Mitigation

Malicious insiders	▪ Enforce strict supply chain management and conduct a comprehensive supplier assessment. ▪ Specify human resource requirements as part of legal contracts. ▪ Require transparency into overall information security and management practices, as well as compliance reporting. ▪ Determine security breach notification processes.
Shared technology issues	▪ Implement security best practices for installation and configuration. ▪ Monitor environment for unauthorized changes/activity. ▪ Promote strong authentication and access control for administrative access and operations. ▪ Enforce service level agreements for patching and vulnerability remediation. ▪ Conduct vulnerability scanning and configuration audits.

Threat Mitigation

Data loss or leakage	▪ Implement strong API access control. ▪ Encrypt and protect integrity of data in transit. ▪ Analyze data protection at both design and run time. ▪ Implement strong key generation, storage and management, and destruction practices. ▪ Contractually demand providers wipe persistent media before it is released into the pool. ▪ Contractually specify provider backup and retention strategies.
Account or service hijacking	▪ Prohibit the sharing of account credentials between users and services. ▪ Leverage strong two-factor authentication techniques where possible. ▪ Employ proactive monitoring to detect unauthorized activity. ▪ Understand cloud provider security policies and SLAs(Service level Agreement).

Google Security Practices

- Organizational and Operational Security
- Data Security
- Threat Evasion
- Safe Access
- Privacy

Google Organizational and Operational Security

- Holistic approach to security
- Security team
- Develop with security in mind
- Regularly performs security audits and threat assessments
- Employees screened, trained
- Works with security community and advisors

Google Data Security

- Google Code of Conduct – “Don’t be evil.”
- Physical security
- Logical Security
- Accessibility
- Redundancy

Google Threat Evasion

- Spam and virus protection built into products
- Protects against application & network attacks

Google Safe Access

- Avoids local storage
- Access controls
- Encrypted connections
- Integrated security

Google Privacy

- Privacy policy
- Does not access confidential user data
- Does not alter data
- Maintain own IP rights
- Indemnification, liability
- End of use

Cloud Data 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.
- Cloud security concerns arising which both customer data and program are residing in provider premises.
- While cost and ease 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.

Cloud Data Security

- To address these concerns, the cloud provider must develop sufficient controls to provide the same or a greater.
- level of security than the organization would have if the cloud were not used.
- There are three types of data in cloud computing
  - Data in transit (transmission data)
  - Data at rest (storage data)
  - Data in processing (processing data).
- Clouds are massively complex systems can be reduced to simple primitives that are replicated thousands of times and common functional units.
- These complexities create many issues related to security as well as all aspects of Cloud computing.

Cloud Data Security

- Security of data and trust problem has always been a primary and challenging issue in cloud computing.
- focuses on enhancing security by using…
  - OTP authentication system.
  - Check data integrity by using hashing algorithms.
  - Encrypt data automatically with the highest strong/ fast encryption algorithm and finally ensure the fast recovery of data.
- Most cloud computing providers..
  - Authenticates (e.g., Transfer usernames and password) via secure connections and secondly,
  - 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.
- The authorization, the process of granting access to requested resources, is pointless without suitable authentication.

Cloud Data Security

- 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.
- When organizations begin to utilize applications in the cloud, authenticating users in a trustworthy and manageable manner becomes an additional challenge.
- Organizations must address authentication-related challenges such as credential management, strong authentication, delegated authentication, and trust across all types of cloud delivery models (SPI).

Cloud Data Security

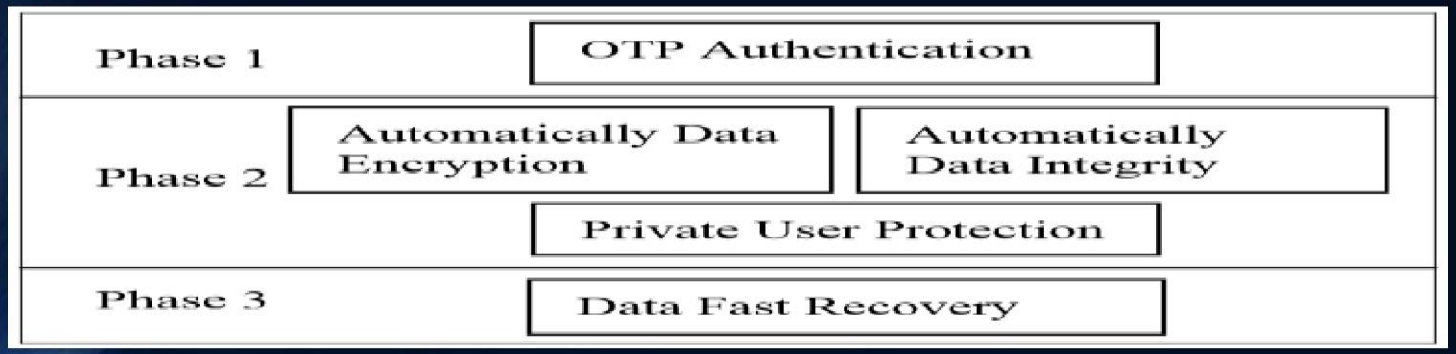
- data security model must ensure…
  - Data must be encrypted automatically
  - Use a strong encryption algorithm.
  - Use the strong encryption algorithm that must be fast to retrieve data faster.
  - Use strong authentication.
  - Ensure file integrity.
- Amazon web services encourage user's to encrypt sensitive data by using TrueCrypt software.
- TrueCrypt is an outstanding encryption solution for anyone familiar with managing volumes and a slight knowledge of encryption technology.

Cloud Data Security

- Any organization planning to deploy TrueCrypt as a cloud-data protection solution must consider the cost and logistics of training and supporting users, managing versions, and recovering damages.
- 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.

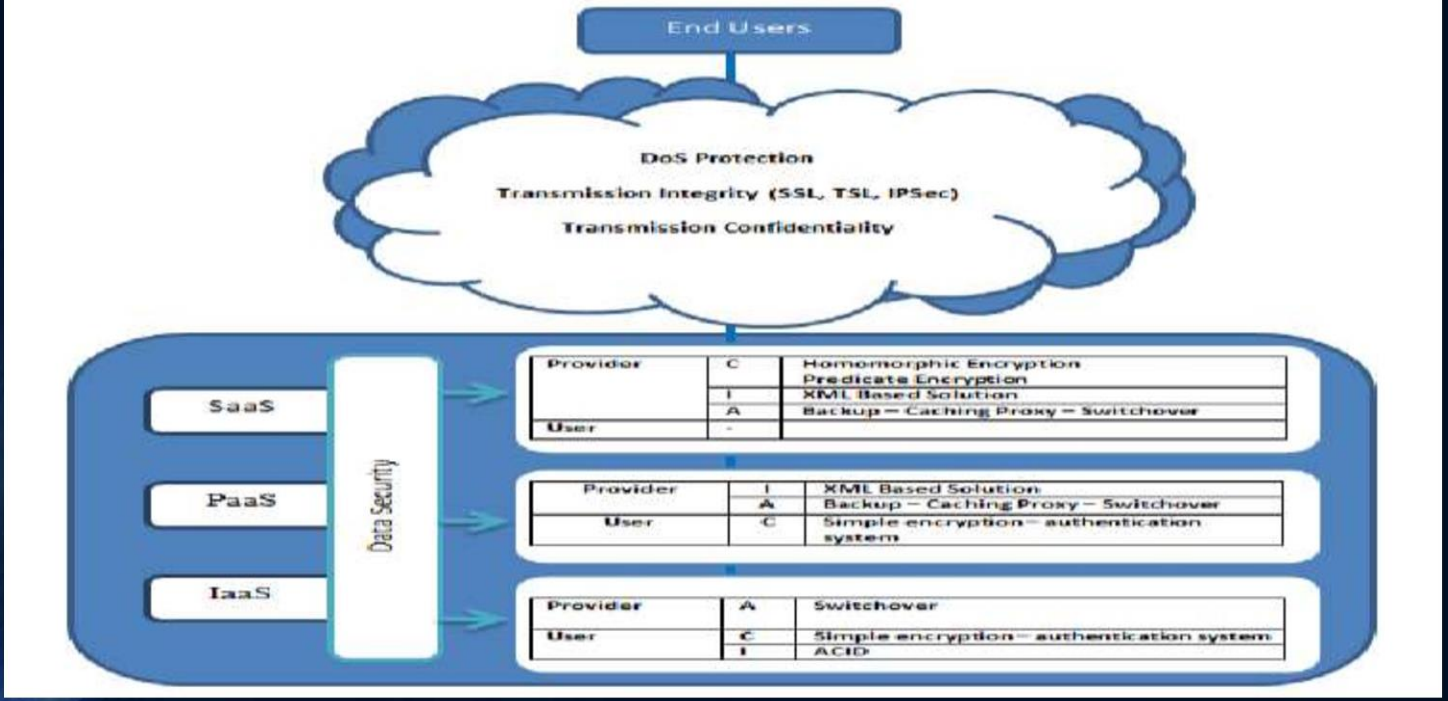
Cloud Data Security

- 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

Data Security Model In Cloud Computing



Cloud Data Security

- OTP Authentication:
  - The users connect to the cloud provider. Then the user gets the username (e-mail), password and finally account password.
  - Users login to the cloud provider website by getting username (e-mail), password and account password. Cloud node controller verifies user info.
  - If user info is true, controller-node send that login authentication success and require OTP.
  - Users generate OTP by using MD5 hash function and sequence number based on user name, password and account password.
  - Then users login to cloud website with OTP .
  - The cloud controller node generates 1000 OTP based on user info by using the MD5 hash function. Then the cloud controller saves 1000 OTP in the temporary OTP database.

Cloud Data Security

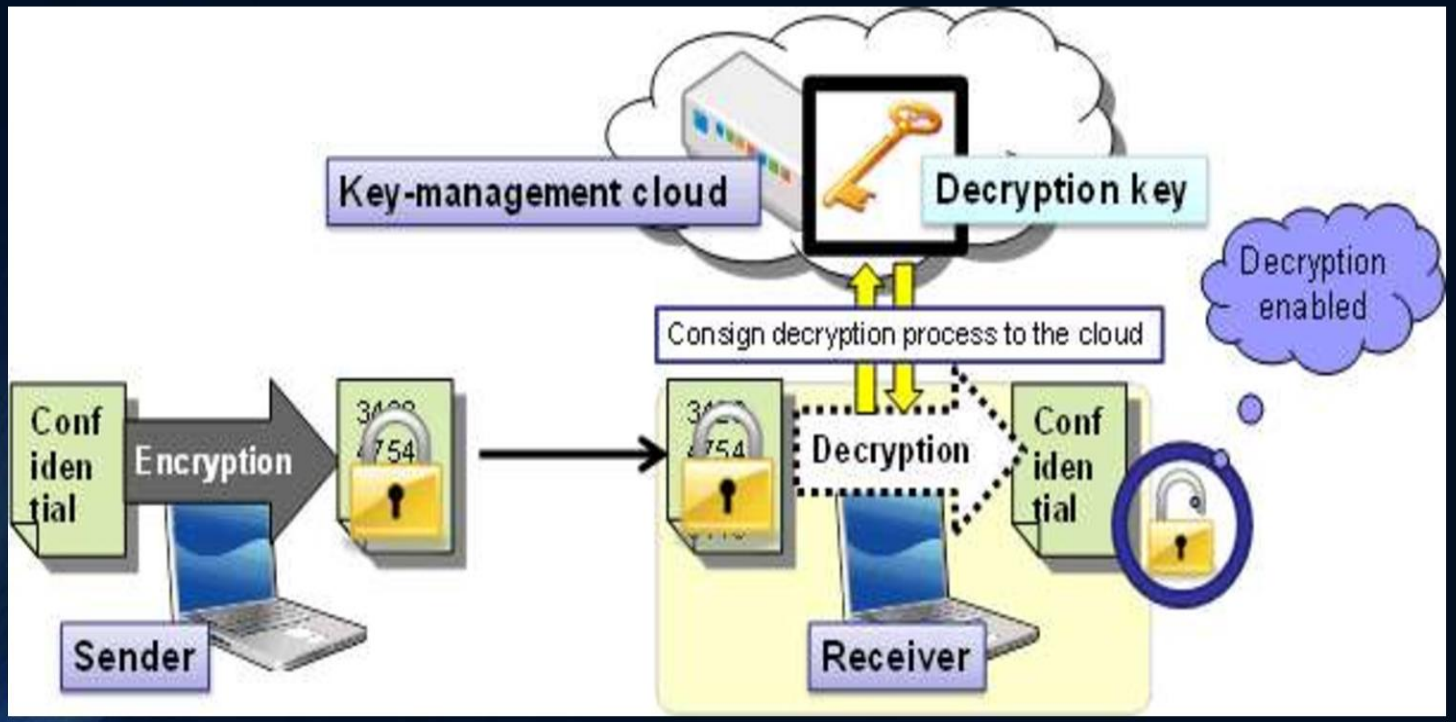
- OTP Authentication:
  - The cloud controller verifies user OTP from the temporary OTP database.
  - If OTP is true, send OTP login success.

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



Cloud Data Security

- 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.
  - For integrity check, we have to think about a simple solution that is feasible and easy to implement for a common user.
  - The trust problem between Cloud storage and customer can be solved, if users can check the integrity of data themselves instead of renting an auditing service to do the same.
  - This can be achieved by hashing the data on user's side and storing the hash values in the cloud with the original data.

Cloud Data Security

- Ensuring Integrity:
  - Hashing technique steps…
    - The program takes file path which has to be accessed through cloud.
    - The program computes a four-hash values in this file based on the four hash functions (MD_4, MD_5, SHA-1 and SHA-2).
    - When users store data in cloud storage devices, server stores four hash values.
    - When a user retrieve data file from cloud, server generate four hash values.
    - Server check integrity by comparing new four hash values with stored four hash values.

Cloud Data Security

High Level Summary of Cloud Data Security Features

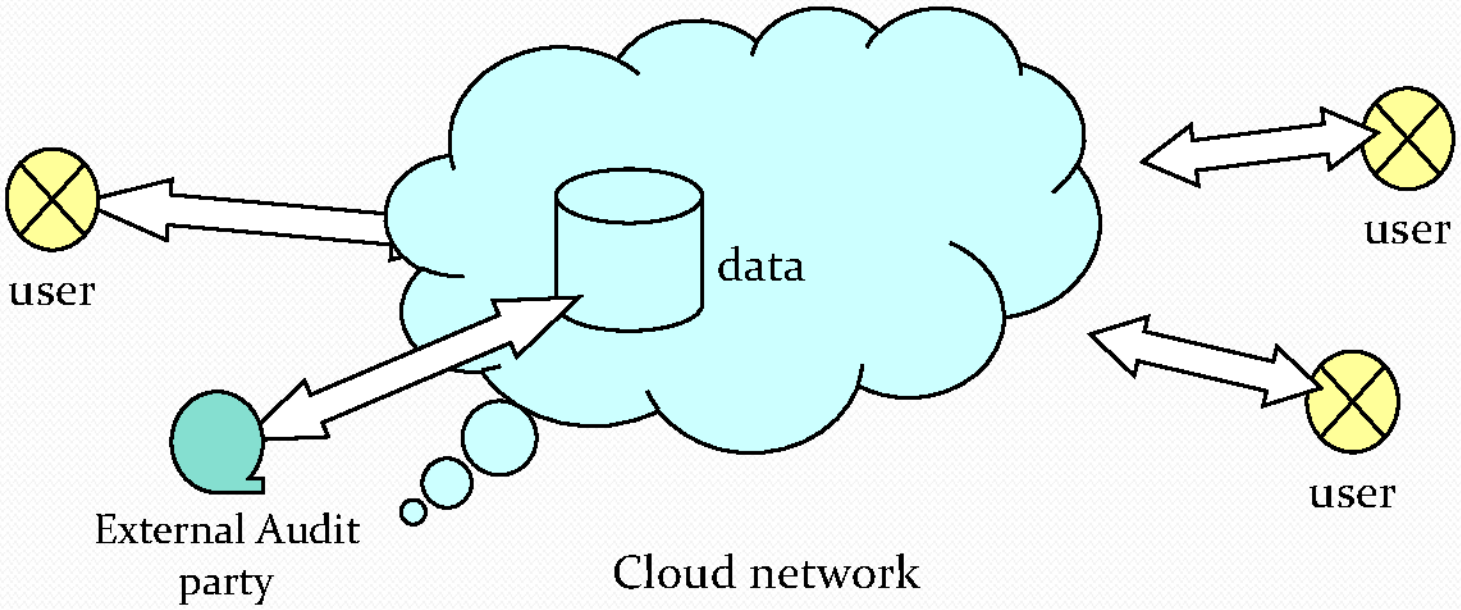
Features	Description
Authentication	OTP Authentication System (mathematical generation).
Provider encryption	Software implemented to select the highest security and faster encryption algorithm based on NIST statistical tests.
Private user encryption	TrueCrypt system or proposed software CloudCrypt v.10.
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.

DATA SECURITY IN CLOUD COMPUTING:

Data outsourcing: users are relieved from the burden of data storage and maintenance

When users put their data (of large size) on the cloud, the data integrity protection is challenging

Enabling public audit for cloud data storage security is important



- cloud computing is built on top of virtualization, if there are security issues with virtualization, then there will also security issues with cloud computing.

- Data segregation. Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists.

- A data center full of servers supporting cloud computing is internally and externally indistinguishable from a data center full of "regular" servers. In each case, it will be important for the data center to be physically secure against unauthorized access

- Computer and network security is fundamentally about three goals/objectives:

-- confidentiality (C)
-- integrity (I), and
-- availability (A).

- *Confidentiality* refers to keeping data private. Privacy is of the amount importance as data leaves the borders of the organization. Not only must internal secrets and sensitive personal data be safeguarded, but metadata and transactional data can also leak important details about firms or individuals. Confidentiality is supported by, among other things, technical tools such as encryption and access control, as well as legal protections

- *Integrity* is a degree confidence that the data in the cloud is what is supposed to be there, and is protected against accidental or intentional alteration without authorization. It also extends to the hurdles of synchronizing multiple databases. Integrity is supported by well audited code, well-designed distributed systems, and robust access control mechanisms.

➢ *Availability* means being able to use the system as anticipated. Cloud technologies can increase availability through widespread internet-enabled access, but the client is dependent on the timely and robust provision of resources. Availability is supported by capacity building and good architecture by the provider, as well as well-defined contracts and terms of agreement

Reduces the exposure of sensitive data
Simplifies security auditing & testing
Enables automated security management
Improves redundancy & disaster recovery
.

Latest technologies used in data security in cloud computing:

•Latest Training Program on Cloud Computing and Windows Azure In order to address the aforementioned challenges, Fujitsu Laboratories developed new cloud information gateway technology that can flexibly control data, including data content, transmitted from the inside of a company to a cloud and between multiple clouds.

•In addition to the option of blocking confidential data, the data gateway also includes the following three features.

Data Masking Technology
Secure Logic Migration and Execution Technology
Data Traceability Technology

Data Masking Technology :

• Using masking technology, when data passes through the information gateway, confidential parts of the data can be deleted or changed before the data are transmitted to an external cloud.

Secure Logic Migration and Execution Technology:

- For confidential data that cannot be released outside of the company, even formed by concealing certain aspects of the data, by simply defining the security level of data, the information gateway can transfer the cloud-based application to the in-house sandbox for execution.

- The sandbox will block access to data or networks that lack pre-authorized access, so even applications transferred from the cloud can be safely executed.

Data Traceability Technology :

- The information gateway tracks all information flowing into and out of the cloud, so these flows and their content can be checked.

- Data traceability technology uses the logs obtained on data traffic as well as the characteristics of the related text to make visible the data used in the cloud.

Latest techniques used data security in cloud computing:

Authentication and Identity:

- Maintaining confidentiality, integrity, and availability for data security is a function of the correct application and configuration of familiar network, system, and application security mechanisms at various levels in the cloud infrastructure.
- Authentication of users takes several forms, but all are based on a combination of authentication factors: something an individual knows (such as a password), something they possess (such as a security token), or some measurable quality that is intrinsic to them (such as a fingerprint).

Application of Encryption for Data in Motion:

•Encryption is used to assure that if there was a breach of communication integrity between the two parties that the data remains confidential.

•Authentication is used to assure that the parties communicating data are who they say they are.

• Common means of authentication themselves employ cryptography in various ways.

Data Masking:

•Data masking is a technique that is intended to remove all identifiable and distinguishing characteristics from data in order to render it anonymous and yet still be operable.

•This technique is aimed at reducing the risk of exposing sensitive information.

•Data masking has also been known by such names as data obfuscation, de-identification, or depersonalization.

Advantages:

- Reduces the exposure of sensitive data
- Simplifies security auditing & testing
- Enables automated security management
- Improves redundancy & disaster recovery
- Access to highly qualified IT security personnel
- Prevent or curtail viruses and malware infection
- Secure sensitive or confidential information in motion
- Achieve compliance with leading self-regulatory frameworks
- Conduct training and awareness for all system users
- In contrast, cloud providers are least confident about the following security requirements:
- Identify and authenticate users before granting access
- Secure vendor relationships before sharing information assets
- Prevent or curtail external attacks
- Encrypt sensitive or confidential information assets whenever feasible
- Determine the root cause of cyber attacks

Platforms:

Amazon's Elastic Compute Cloud, or EC2, is probably the most generalized and best-known of the cloud computing service offerings.

IBM Computing on Demand or Blue Cloud is a highly enterprise-focused cloud computing offering that, because it is related to and built with the same technology sold to enterprises, can cross over between public and private cloud applications.

Microsoft's Azure cloud computing, based on Microsoft Vista and .NET technology, includes both cloud computing and cloud-hosted extension

Causes of Problems Associated with Cloud Computing

- Most security problems stem from:
  - Loss of control
  - Lack of trust (mechanisms)
  - Multi-tenancy

- These problems exist mainly in 3rd party management models
  - Self-managed clouds still have security issues, but not related to above

Loss of Control in the Cloud

- Consumer's loss of control
  - Data, applications, resources are located with provider
  - User identity management is handled by the cloud
  - User access control rules, security policies and enforcement are managed by the cloud provider
  - Consumer relies on provider to ensure
    - Data security and privacy
    - Resource availability
    - Monitoring and repairing of services/resources

Lack of Trust in the Cloud

- Trusting a third party requires taking risks

- Defining trust and risk
  - Opposite sides of the same coin (J. Camp)
  - People only trust when it pays (Economist's view)
  - Need for trust arises only in risky situations

- Defunct third party management schemes
  - Hard to balance trust and risk
  - e.g. Key Escrow (Clipper chip)
  - Is the cloud headed toward the same path?

Multi-tenancy Issues in the Cloud

- Conflict between tenants' opposing goals
  - Tenants share a pool of resources and have opposing goals
- How does multi-tenancy deal with conflict of interest?
  - Can tenants get along together and 'play nicely' ?
  - If they can't, can we isolate them?
- How to provide separation between tenants?

- Cloud Computing brings new threats
  - Multiple independent users share the same physical infrastructure
  - Thus an attacker can legitimately be in the same physical machine as the target

Taxonomy of Fear

- Confidentiality
  - Fear of loss of control over data
    - Will the sensitive data stored on a cloud remain confidential?
    - Will cloud compromises leak confidential client data
  - Will the cloud provider itself be honest and won't peek into the data?

- Integrity
  - How do I know that the cloud provider is doing the computations correctly?
  - How do I ensure that the cloud provider really stored my data without tampering with it?

Taxonomy of Fear (cont.)

- Availability
  - Will critical systems go down at the client, if the provider is attacked in a Denial of Service attack?
  - What happens if cloud provider goes out of business?
  - Would cloud scale well-enough?
  - Often-voiced concern
    - Although cloud providers argue their downtime compares well with cloud user's own data centers

Taxonomy of Fear (cont.)

- Privacy issues raised via massive data mining
  - Cloud now stores data from a lot of clients, and can run data mining algorithms to get large amounts of information on clients
- Increased attack surface
  - Entity outside the organization now stores and computes data, and so
  - Attackers can now target the communication link between cloud provider and client
  - Cloud provider employees can be phished

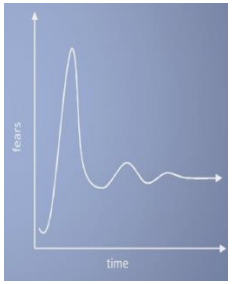
Taxonomy of Fear (cont.)

- Auditability and forensics (out of control of data)
  - Difficult to audit data held outside organization in a cloud
  - Forensics also made difficult since now clients don't maintain data locally
- Legal dilemma and transitive trust issues
  - Who is responsible for complying with regulations?
    - e.g., SOX, HIPAA, GLBA ?
  - If cloud provider subcontracts to third party clouds, will the data still be secure?

Taxonomy of Fear (cont.)

Cloud Computing is **a security nightmare** and it can't be handled in traditional ways.

John Chambers
CISCO CEO



- Security is one of the most difficult task to implement in cloud computing.
  - Different forms of attacks in the application side and in the hardware components
- Attacks with catastrophic effects only needs one security flaw

Threat Model

• A threat model helps in analyzing a security problem, design mitigation strategies, and evaluate solutions

•Steps:

- Identify attackers, assets, threats and other components
- Rank the threats
- Choose mitigation strategies
- Build solutions based on the strategies

Threat Model

- Basic components
  - Attacker modeling
    - Choose what attacker to consider
      - insider vs. outsider?
      - single vs. collaborator?
    - Attacker motivation and capabilities
  - Attacker goals
  - Vulnerabilities / threats

What is the issue?

- The core issue here is the levels of trust
  - Many cloud computing providers trust their customers
  - Each customer is physically commingling its data with data from anybody else using the cloud while logically and virtually you have your own space
  - The way that the cloud provider implements security is typically focused on they fact that those outside of their cloud are evil, and those inside are good.
- But what if those inside are also evil?

Attacker Capability: Malicious Insiders

- At client
  - Learn passwords/authentication information
  - Gain control of the VMs
- At cloud provider
  - Log client communication
  - Can read unencrypted data
  - Can possibly peek into VMs, or make copies of VMs
  - Can monitor network communication, application patterns
  - Why?
    - Gain information about client data
    - Gain information on client behavior
    - Sell the information or use itself

Attacker Capability: Outside attacker

- What?
  - Listen to network traffic (passive)
  - Insert malicious traffic (active)
  - Probe cloud structure (active)
  - Launch DoS
- Goal?
  - Intrusion
  - Network analysis
  - Man in the middle
  - Cartography

Challenges for the attacker

- How to find out where the target is located?
- How to be co-located with the target in the same (physical) machine?
- How to gather information about the target?

Data Security and Storage

- Several aspects of data security, including:
  - Data-in-transit
    - Confidentiality + integrity using secured protocol
    - Confidentiality with non-secured protocol and encryption
  - Data-at-rest
    - Generally, not encrypted , since data is commingled with other users' data
    - Encryption if it is not associated with applications?
      - But how about indexing and searching?
  - Processing of data, including multitenancy
    - For any application to process data

Data Security and Storage (cont.)

- Data lineage
  - Knowing when and where the data was located w/i cloud is important for audit/compliance purposes
  - e.g., Amazon AWS
    - Store <d1, t1, ex1.s3.amazonaws.com>
    - Process <d2, t2, ec2.compute2.amazonaws.com>
    - Restore <d3, t3, ex2.s3.amazonaws.com>
- Data provenance
  - Computational accuracy (as well as data integrity)
  - E.g., financial calculation: sum ((((2*3)*4)/6) -2) = **$**2.00 ?
    - How about dollars of different countries?
    - Correct exchange rate?
- Data remanence
  - Inadvertent disclosure of sensitive information is possible

What is Privacy?

- The concept of privacy varies widely among (and sometimes within) countries, cultures, and jurisdictions.
- It is shaped by public expectations and legal interpretations;
  - as such, a concise definition is elusive if not impossible.
- Privacy rights or obligations are related to the collection, use, disclosure, storage, and destruction of personal data
- At the end of the day, privacy is about the accountability of organizations to data subjects, as well as the transparency to an organization's practice around personal information.

What Are the Key Privacy Concerns?

- Typically mix security and privacy

- Some considerations to be aware of:
  - Storage
  - Retention
  - Destruction
  - Auditing, monitoring and risk management
  - Privacy breaches
  - Who is responsible for protecting privacy?

Security Issues in the Cloud

- In theory, minimizing any of the issues would help:
  - Third Party Cloud Computing
  - Loss of Control
    - Take back control
      - Data and apps may still need to be on the cloud
      - But can they be managed in some way by the consumer?
  - Lack of trust
    - Increase trust (mechanisms)
      - Technology
      - Policy, regulation
      - Contracts (incentives)
  - Multi-tenancy
    - Private cloud
      - Takes away the reasons to use a cloud in the first place
    - VPC: its still not a separate system
    - Strong separation

Third Party Cloud Computing

- Known issues: Already exist

- Confidentiality issues
- Malicious behavior by cloud provider
- Known risks exist in any industry practicing outsourcing
- Provider and its infrastructure needs to be trusted

New Vulnerabilities & Attacks

- Threats arise from other consumers
- Due to the subtleties of how physical resources can be transparently shared between VMs
- Such attacks are based on placement and extraction
- A customer VM and its adversary can be assigned to the same physical server
- Adversary can penetrate the VM and violate customer confidentiality

More on attacks…

- Collaborative attacks
- Mapping of internal cloud infrastructure
- Identifying likely residence of a target VM
- Instantiating new VMs until one gets co-resident with the target
- Cross-VM side-channel attacks
- Extract information from target VM on the same machine

More on attacks…

1. Can one determine where in the cloud infrastructure an instance is located?
2. Can one easily determine if two instances are co-resident on the same physical machine?
3. Can an adversary launch instances that will be co-resident with other user instances?
4. Can an adversary exploit cross-VM information leakage once co-resident?

Answer: Yes to all

Minimize Lack of Trust: Policy Language

- Consumers have specific security needs but don't have a say-so in how they are handled
  - Currently consumers cannot dictate their requirements to the provider (SLAs are one-sided)
- Standard language to convey one's policies and expectations
  - Agreed upon and upheld by both parties
  - Standard language for representing SLAs
- Create policy language with the following characteristics:
  - Machine-understandable (or at least processable),
  - Easy to combine/merge and compare

Minimize Lack of Trust: Certification

- Certification
  - Some form of reputable, independent, comparable assessment and description of security features and assurance
    - Sarbanes-Oxley, DIACAP, DISTCAP, etc
- Risk assessment
  - Performed by certified third parties
  - Provides consumers with additional assurance

Minimize Loss of Control: Monitoring

- Cloud consumer needs situational awareness for critical applications
  - When underlying components fail, what is the effect of the failure to the mission logic
  - What recovery measures can be taken
    - by provider and consumer
- Requires an application-specific run-time monitoring and management tool for the consumer
  - The cloud consumer and cloud provider have different views of the system
  - Enable both the provider and tenants to monitor the components in the cloud that are under their control

Minimize Loss of Control: Monitoring (Cont.)

- Provide mechanisms that enable the provider to act on attacks he can handle.
  - infrastructure remapping
    - create new or move existing fault domains
  - shutting down offending components or targets
    - and assisting tenants with porting if necessary
  - Repairs
- Provide mechanisms that enable the consumer to act on attacks that he can handle
  - application-level monitoring
  - RAdAC (Risk-adaptable Access Control)
  - VM porting with remote attestation of target physical host
  - Provide ability to move the user's application to another cloud

Minimize Loss of Control: Utilize Different Clouds

- The concept of 'Don't put all your eggs in one basket'
  - Consumer may use services from different clouds through an intra-cloud or multi-cloud architecture
  - A multi-cloud or intra-cloud architecture in which consumers
    - Spread the risk
    - Increase redundancy (per-task or per-application)
    - Increase chance of mission completion for critical applications
  - Possible issues to consider:
    - Policy incompatibility (combined, what is the overarching policy?)
    - Data dependency between clouds
    - Differing data semantics across clouds
    - Knowing when to utilize the redundancy feature
      - monitoring technology
    - Is it worth it to spread your sensitive data across multiple clouds?
      - Redundancy could increase risk of exposure

Minimize Loss of Control: Access Control

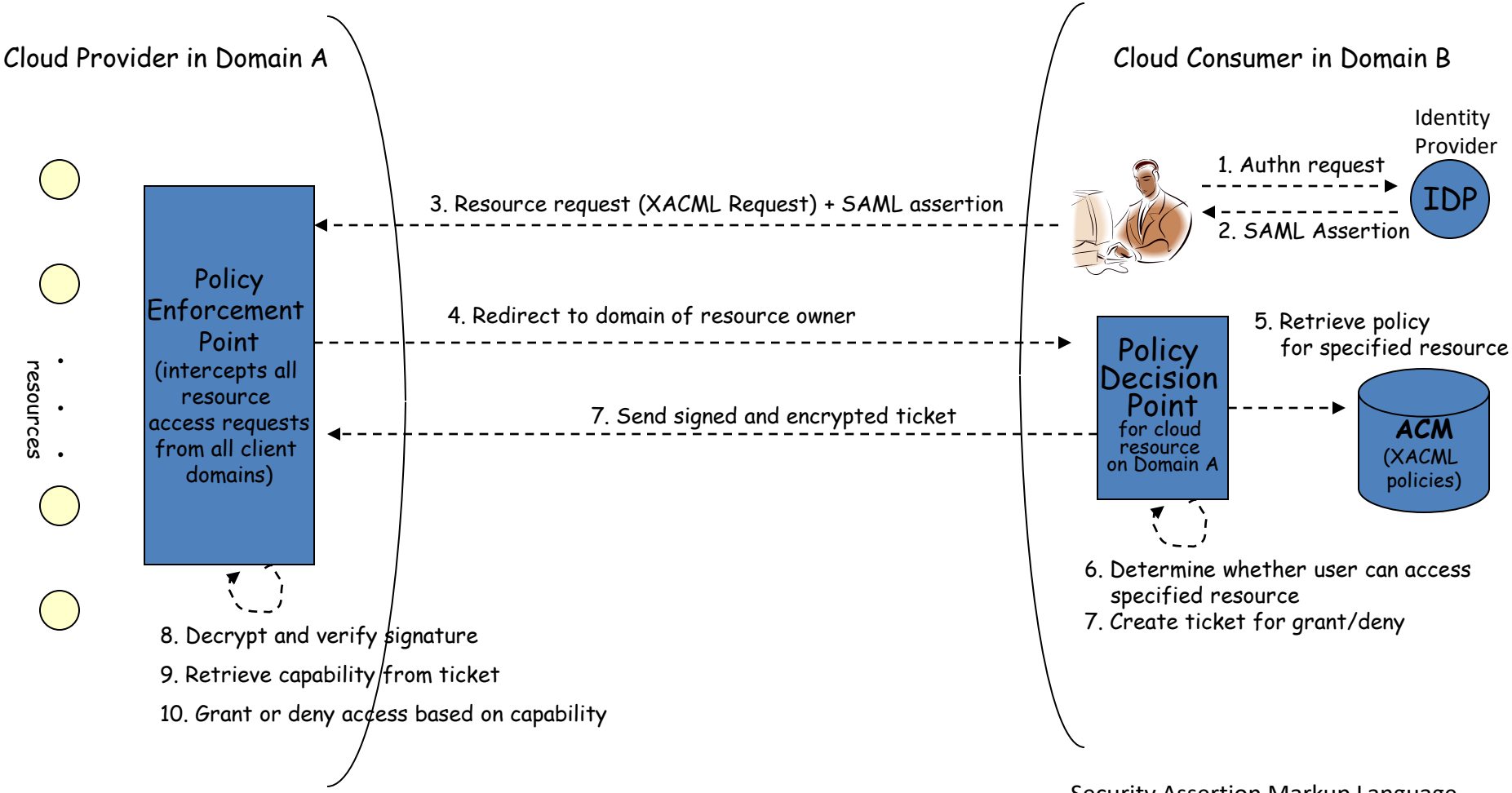
- Many possible layers of access control
  - E.g. access to the cloud, access to servers, access to services, access to databases (direct and queries via web services), access to VMs, and access to objects within a VM
  - Depending on the deployment model used, some of these will be controlled by the provider and others by the consumer

- Regardless of deployment model, provider needs to manage the user authentication and access control procedures (to the cloud)
  - Federated Identity Management: access control management burden still lies with the provider
  - Requires user to place a large amount of trust on the provider in terms of security, management, and maintenance of access control policies.
    - This can be burdensome when numerous users from different organizations with different access control policies, are involved

Minimize Loss of Control: Access Control (Cont.)

- Consumer-managed access control
  - Consumer retains decision-making process to retain some control, requiring less trust of the provider
  - Requires the client and provider to have a pre-existing trust relationship, as well as a pre-negotiated standard way of describing resources, users, and access decisions between the cloud provider and consumer.
    - It also needs to be able to guarantee that the provider will uphold the consumer-side's access decisions.
  - Should be at least as secure as the traditional access control model.

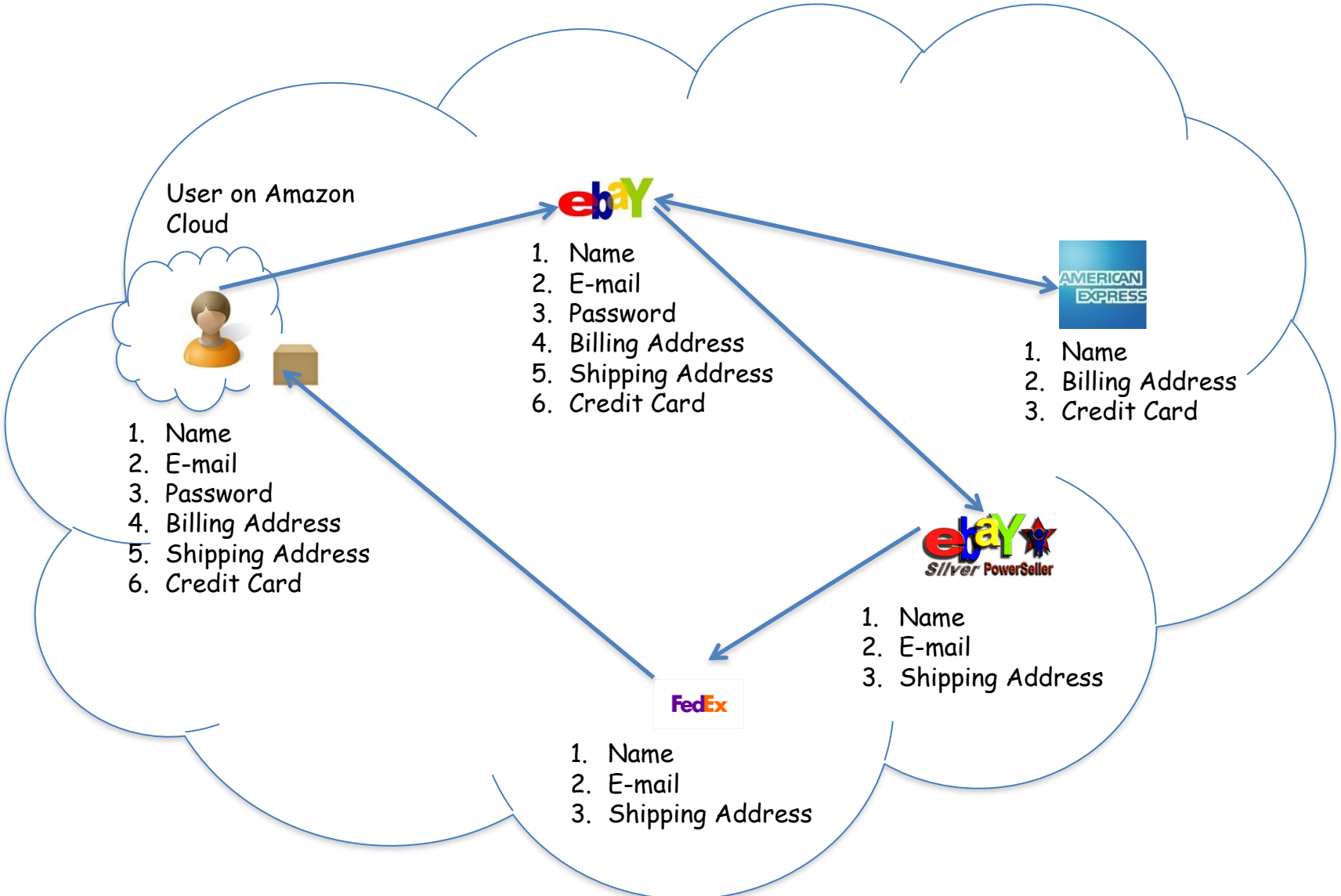
Minimize Loss of Control: Access Control



Security Assertion Markup Language

eXtensible Access Control Markup Language

Minimize Loss of Control: IDM Motivation



Minimize Loss of Control: IDM Identity in the Cloud

Minimize Loss of Control: IDM Issues in Cloud Computing

- Cloud introduces several issues to IDM
  - Users have **multiple accounts** associated with **multiple service providers.**
  - Present IDMs require a **trusted third party** and do not work on an **untrusted host**.
  - Lack of trust
    - Use of Trusted Third Party is not an option
    - Cloud hosts are untrusted
  - Loss of control
    - Collusion between Cloud Services
      - Sharing sensitive identity information between services can lead to undesirable **mapping of the identities to the user.**

IDM in Cloud needs to be user-centric

Minimize Multi-tenancy

- Can't really force the provider to accept less tenants
  - Can try to increase isolation between tenants
    - Strong isolation techniques (VPC to some degree)
    - QoS requirements need to be met
    - Policy specification
  - Can try to increase trust in the tenants
    - Who's the insider, where's the security boundary? Who can I trust?
    - Use SLAs to enforce trusted behavior

Conclusion

- Cloud computing is sometimes viewed as a reincarnation of the classic mainframe client-server model
  - However, resources are ubiquitous, scalable, highly virtualized
  - Contains all the traditional threats, as well as new ones
- In developing solutions to cloud computing security issues it may be helpful to identify the problems and approaches in terms of
  - Loss of control
  - Lack of trust
  - Multi-tenancy problems

- **Cloud Data Management Interface(CDMI)**

- A new standard to protect data is the cloud data management interface(CDMI) from storage networking Industry Association(SNIA).

- CDMI allows users to tag the data with special metadata.

- The metadata can be used to code services that must be provided such as encryption, backup, duplications, replication, compression, archiving etc.

- These services increase the value of user data existing in the cloud

- By implementing a well documented standard interface such as CDMI user can freely move the data from one cloud vendor to another without the problem of confirming or adjusting to different interfaces.

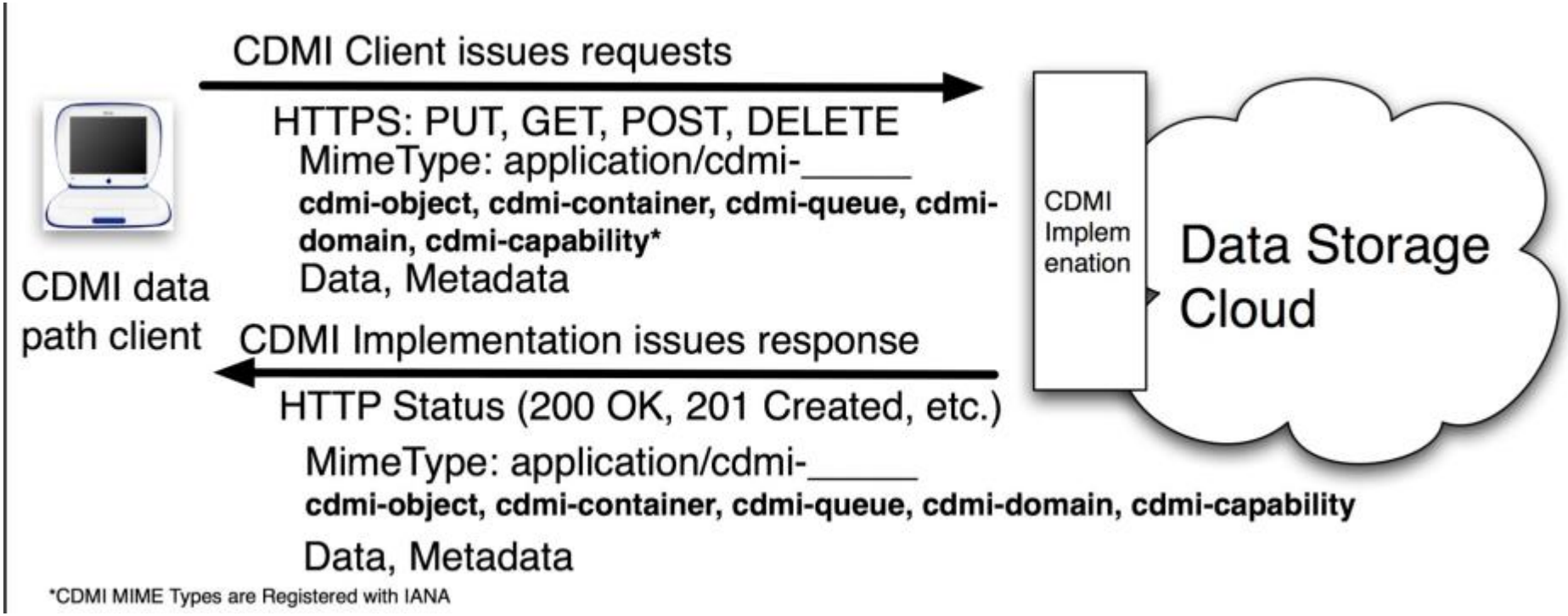
- CDMI is the first industry-developed open standard for cloud data.

- It enables interoperable cloud storage implementation from various cloud service providers and storage vendors.

- The CDMI standard is applicable to private, public, and hybrid clouds.

- It is a data path to the cloud and has the ability to manage service levels for cloud data.

- It includes common inter-operable data storage format for safely moving data and its requirements from one cloud provider to another.

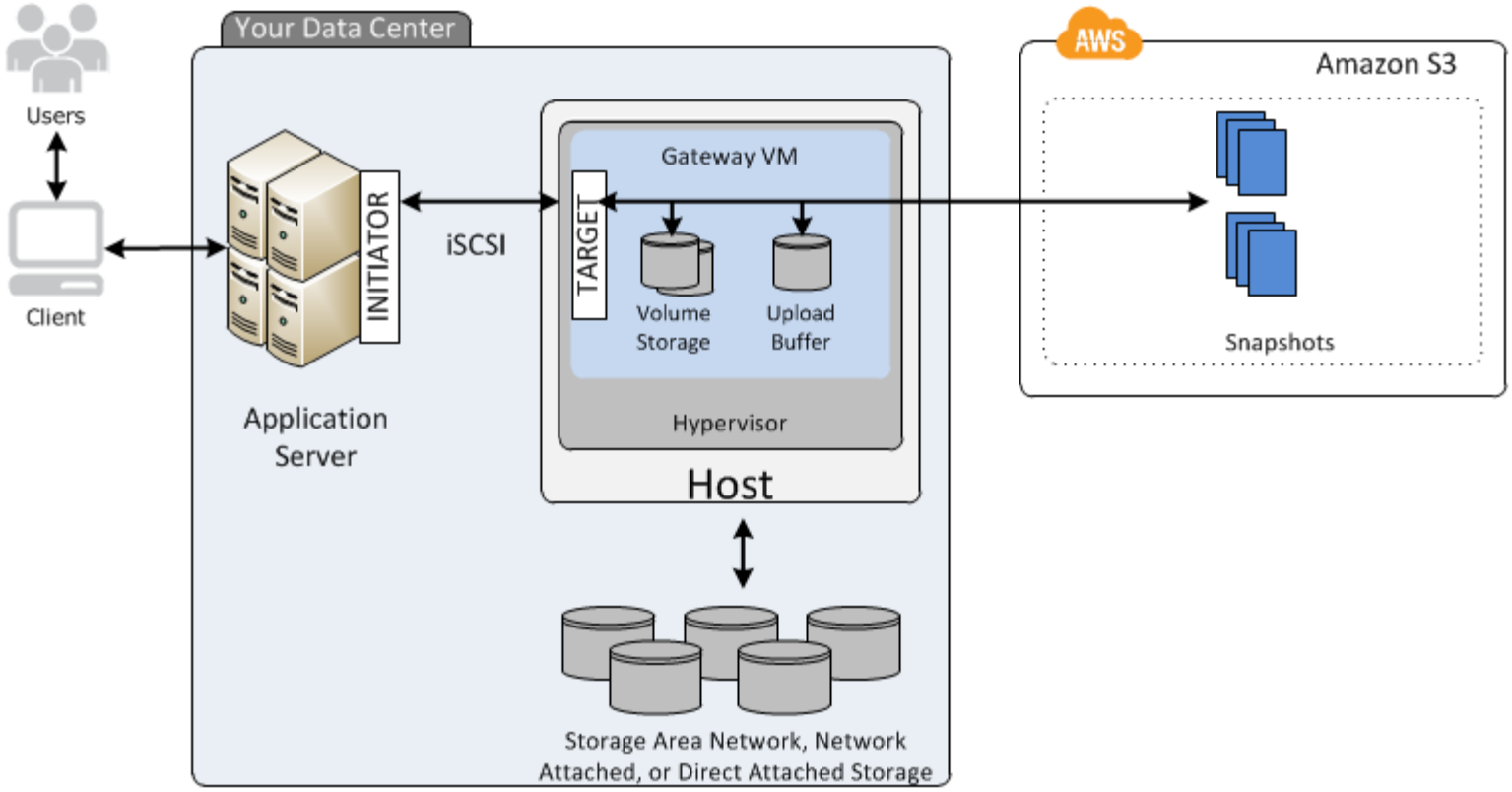


- # Cloud Storage Gateways
- A **cloud storage gateway** is a network appliance or server which resides at the customer premises and translates cloud storage APIs such as SOAP or REST to block-based storage protocols such as iSCSI or Fibre Channel or file-based interfaces such as NFS or SMB

- Cloud gateways were expected to increase the use of cloud storage by lowering monthly charges and eliminating the concern of data security

- To address the performance and security issues in public clouds consumer organizations can use CSGs.

- The CGS is an appliance residing in the consumers premises and provides data protection by encrypting compressing and archiving data sets before moving the data to a cloud.



- The CSG provides data protection in 4 steps:
  - The CSG cache accelerates I/O rates and enables convenient replication procedure.
  - Files that are to be copied to the cloud are first stored in the CSG cache.
  - After a certain pre-set time interval the cache data is pushed to the cloud.
  - Data that is read from the cloud is copied to the cache.

- To improve performance the CSG cache data as well as metadata
- The CSG must provide following features or benefits:
  - Caching Algorithm:

    The CSG must use certain algorithms such as LRU to enhance the cache hit rate.
  - Intelligent pre-fetching Algorithm:

    The CSG must monitor read patterns and intelligently pre-fetch data from the cloud to the cache before the user request the data
  - Caching time periods:

    Some CSG's allow users to setup a caching time duration.
  - Synchronous Snapshots:

    Ti allows the CSG to identify new and modified data which are tagged as dirty and moved to the cloud
  - Data Replication Process:

    The CSG must have an efficient data transfer mechanism.

- A cloud storage gateway is a hardware- or software-based appliance located on the customer premises that serves as a bridge between local applications and remote cloud-based storage.

- A cloud storage gateway provides basic protocol translation and simple connectivity to allow the incompatible technologies to communicate transparently.

- The gateway may be a stand-alone computing device or a virtual machine (VM) image that provides basic protocol translation and connectivity that allows incompatible technologies to communicate transparently.

- The need for a bridge between cloud storage systems and enterprise applications arose because of an incompatibility between the protocols used for public cloud technologies and legacy storage systems.

- Most public cloud providers rely on Internet protocols, usually a RESTful API over HTTP, rather than conventional storage area network (SAN) or network-attached storage (NAS) protocols.

- Many of today's cloud storage gateway products provide data de-duplication and compression capabilities to make use of available bandwidth efficiently and move data as quickly as possible.

- A cloud storage gateway is also known as a cloud storage controller or cloud storage appliance.

- A cloud storage gateway is designed to provide interoperability between different data protocols used in a client/server cloud architecture.

- It allows interoperability between the application programming interface (API) of a client's REST/SOAP-based data storage and Internet SCSI (iSCSI), Fiber Channel (FC).

- Generally, cloud storage gateways are implemented as software gateways that provide a suite of services to facilitate seamless data transfer and retrieval between remote cloud storage servers, data compression for faster transfer, version management and control of entire storage snapshots and run-time encryption, which ensures secure data transmission.

- Advantages of Using a CSG
  - Cloud storage gateway avoid the need to change existing applications by providing a standard interface.
  - We can make use of all advantages of object storage without re-writing our applications.
  - As well IT users are used to existing protocols – like SMB or NFS.
  - They can make use of cloud storage with the advantage of still using their existing infrastructures

- Cloud Firewall
- A cloud firewall is a network firewall appliance
- Explicitly built to work with other cloud based security solutions
- It serves the same purposes as traditional firewalls
- It is different from a traditional firewall on the following three aspects:
  - Scalability Cloud firewall are designed to scale as customer bandwidth increases or at the least any hardware upgrade has to be made transparent to customers.
  - Availability Cloud firewall providers offer extremely high availability through an infrastructure with fully redundant power and network services as well as backup strategies in the event of a site failure.
  - Extensibility Cloud firewalls are available in locations where the network manager can provide a protected communications path.

- Virtual Firewall
- A VF is a network firewall services running entirely within a virtualized environment.

- Like a physical firewall it provides the usual packet filtering and monitoring.

- VF provides an easy way to decrease investment expenses by consolidating multiple logical firewalls onto a single platform.

- Depending on the point of deployment VF can operate in two different modes namely bridge mode and hypervisor mode
  - In bridge mode the firewall acts like a physical firewall that works with a physical or virtual switch to intercept network traffic destined for other network segments.
  - In hypervisor mode the firewall service resides in the virtualization hypervisor where it can capture monitor and filter all the activities of all the virtual machines and logical resources.