UNIT 4: Resource Management and Security In Cloud:

What is Inter Cloud:
Intercloud is **an internet technology which is based on internet itself**. With the advent of cloud computing the scenario has changed a lot. The intercloud allows user to connect multiple cloud networks. This network allows users to share certain files and information in real time

Inter Cloud Resource Management:

The inter cloud resource management services are **build to perform resource discovery, match, select, composition, negotiate, schedule and monitor operations**.

1. **Extended Cloud Computing Services :**

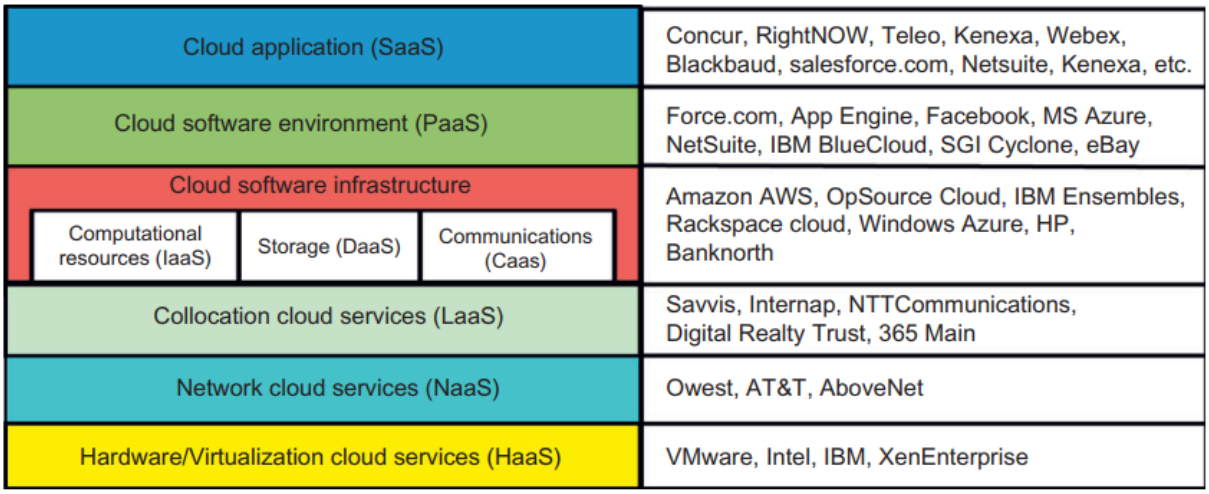

FIGURE 4.23
A stack of six layers of cloud services and their providers.

Figure 4.23 shows six layers of cloud services, ranging from hardware, network, and collocation to infrastructure, platform, and software applications.

The cloud platform provides PaaS, which sits on top of the IaaS infrastructure. The top layer offers SaaS. These must be implemented on the cloud platforms provided. Although the three basic models are dissimilar in usage, as shown in Table 4.7

They are built one on top of another. The implication is that one cannot launch SaaS applications with a cloud platform. The cloud platform cannot be built if compute and storage infrastructures are not there.

- The bottom three layers are more related to physical requirements. The bottommost layer provides Hardware as a Service (HaaS).
- The next layer is for interconnecting all the hardware components, and is simply called Network as a Service (NaaS). Virtual LANs fall within the scope of NaaS. The next layer up offers Location as a Service (LaaS), which provides a collocation service to house, power, and secure all the physical hardware and network resources.
- The cloud infrastructure layer can be further subdivided as Data as a Service (DaaS) and Communication as a Service (CaaS) in addition to compute and storage in IaaS.

Table 4.7 Cloud Differences in Perspectives of Providers, Vendors, and Users

Cloud Players	IaaS	PaaS	SaaS
IT administrators/cloud providers	Monitor SLAs	Monitor SLAs and enable service platforms	Monitor SLAs and deploy software
Software developers (vendors)	To deploy and store data	Enabling platforms via configurators and APIs	Develop and deploy software
End users or business users	To deploy and store data	To develop and test web software	Use business software

- As shown in Table 4.7, cloud players are divided into three classes: (1) cloud service providers and IT administrators, (2) software developers or vendors, and (3) end users or business users. These cloud players vary in their roles under the IaaS, PaaS, and SaaS models.
- The table entries distinguish the three cloud models as viewed by different players. From the software vendors' perspective, application performance on a given cloud platform is most important. From the providers' perspective, cloud infrastructure performance is the primary concern. From the end users' perspective, the quality of services, including security, is the most important.

1.1. Cloud Service Tasks and Trends:

- Cloud services are introduced in five layers. The top layer is for SaaS applications, as further subdivided into the five application areas in Figure 4.23, mostly for business applications. For example, CRM is heavily practiced in business promotion, direct sales, and marketing services. CRM offered the first SaaS on the cloud successfully.
- PaaS is provided by Google, Salesforce.com, and Facebook, among others. IaaS is provided by Amazon, Windows Azure, and RackRack, among others. Collocation services require multiple cloud providers to work together to support supply chains in manufacturing. Network cloud services provide communications such as those by AT&T, Qwest, and AboveNet.

1.2. Software Stack for Cloud Computing:

- Despite the various types of nodes in the cloud computing cluster, the overall software stacks are built from scratch to meet rigorous goals (see Table 4.7).
- Developers have to consider how to design the system to meet critical requirements such as high throughput, HA, and fault tolerance. Even the operating system might be modified to meet the special requirement of cloud data processing.
- Based on the observations of some typical cloud computing instances, such as Google, Microsoft, and Yahoo!, the overall software stack structure of cloud computing software can be viewed as layers. Each layer has its own purpose and provides the interface for the upper layers just as the traditional software stack does.
- The platform for running cloud computing services can be either physical servers or virtual servers. By using VMs, the platform can be flexible, that is, the running services are not bound to specific hardware platforms. This brings flexibility to cloud computing platforms. The software layer on top of the platform is the layer for storing massive amounts of data.
- Other layers running on top of the file system are the layers for executing cloud computing applications. They include the database storage system, programming for large-scale clusters, and data query language support. The next layers are the components in the software stack.

1.3. Runtime Support Services:

- As in a cluster environment, there are also some runtime supporting services in the cloud computing environment. Cluster monitoring is used to collect the runtime status of the entire cluster. One of the most important facilities is the cluster job management system.
- The scheduler queues the tasks submitted to the whole cluster and assigns the tasks to the processing nodes according to node availability. The distributed scheduler for the cloud application has special characteristics that can support cloud applications, such as scheduling the programs written in MapReduce style.
- The runtime support system keeps the cloud cluster working properly with high efficiency. Runtime support is software needed in browser-initiated applications applied by thousands of cloud customers.
- The SaaS model provides the software applications as a service, rather than letting users purchase the software. As a result, on the customer side, there is no upfront investment in servers or software licensing. On the provider side, costs are rather low, compared with conventional hosting of user applications. The customer data is stored in the cloud that is either vendor proprietary or a publicly hosted cloud supporting PaaS and IaaS.

2. Resource Provisioning:

Resource Provisioning means the selection, deployment, and run-time management of software (e.g., database server management systems, load balancers) and hardware resources (e.g., CPU, storage, and network) for ensuring guaranteed performance for applications. Resource Provisioning is an important and challenging problem in the large-scale distributed systems such as Cloud computing environments.

2.1. Provisioning of Compute Resources (VMs):

- Providers supply cloud services by signing SLAs with end users. The SLAs must commit sufficient resources such as CPU, memory, and bandwidth that the user can use for a preset period.
- Underprovisioning of resources will lead to broken SLAs and penalties. Overprovisioning of resources will lead to resource underutilization, and consequently, a decrease in revenue for the provider.
- Deploying an autonomous system to efficiently provision resources to users is a challenging problem. The difficulty comes from the unpredictability of consumer demand, software and hardware failures, heterogeneity of services, power management, and conflicts in signed SLAs between consumers and service providers.
- Resource provisioning schemes also demand fast discovery of services and data in cloud computing infrastructures. In a virtualized cluster of servers, this demands efficient installation of VMs, live VM migration, and fast recovery from failures.

2.2. Resource Provisioning Methods:

Figure 4.24 shows three cases of static cloud resource provisioning policies.

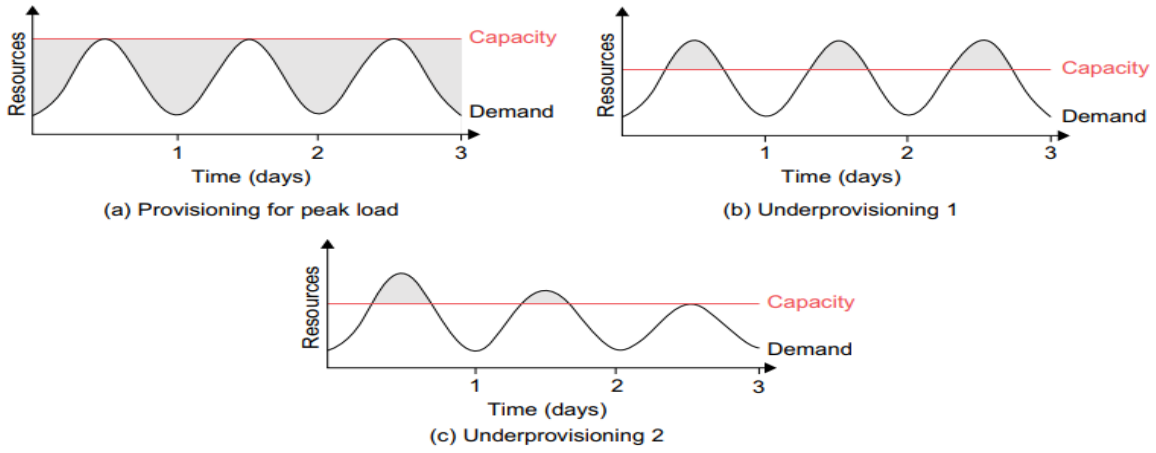

FIGURE 4.24

Three cases of cloud resource provisioning without elasticity: (a) heavy waste due to overprovisioning, (b) underprovisioning and (c) under- and then overprovisioning.

- In case (a), overprovisioning with the peak load causes heavy resource waste (shaded area).
- In case (b), underprovisioning (along the capacity line) of resources results in losses by both user and provider in that paid demand by the users (the shaded area above the capacity) is not served and wasted resources still exist for those demanded areas below the provisioned capacity.
- In case (c), the constant provisioning of resources with fixed capacity to a declining user demand could result in even worse resource waste. The user may give up the service by canceling the demand, resulting in reduced revenue for the provider. Both the user and provider may be losers in resource provisioning without elasticity.

Three resource-provisioning methods are presented in the following sections.

- The demand-driven method provides static resources and has been used in grid computing for many years.
- The event-driven method is based on predicted workload by time.
- The popularity-driven method is based on Internet traffic monitored.

(i) Demand-Driven Resource Provisioning:

- This method adds or removes computing instances based on the current utilization level of the allocated resources. The demand-driven method automatically allocates two Xeon processors for the user application, when the user was using one Xeon processor more than 60 percent of the time for an extended period.
- In general, when a resource has surpassed a threshold for a certain amount of time, the scheme increases that resource based on demand. When a resource is below a threshold for a certain amount of time, that resource could be decreased accordingly. Amazon implements such an auto-scale feature in its EC2 platform. This method is easy to implement. The scheme does not work out right if the workload changes abruptly.

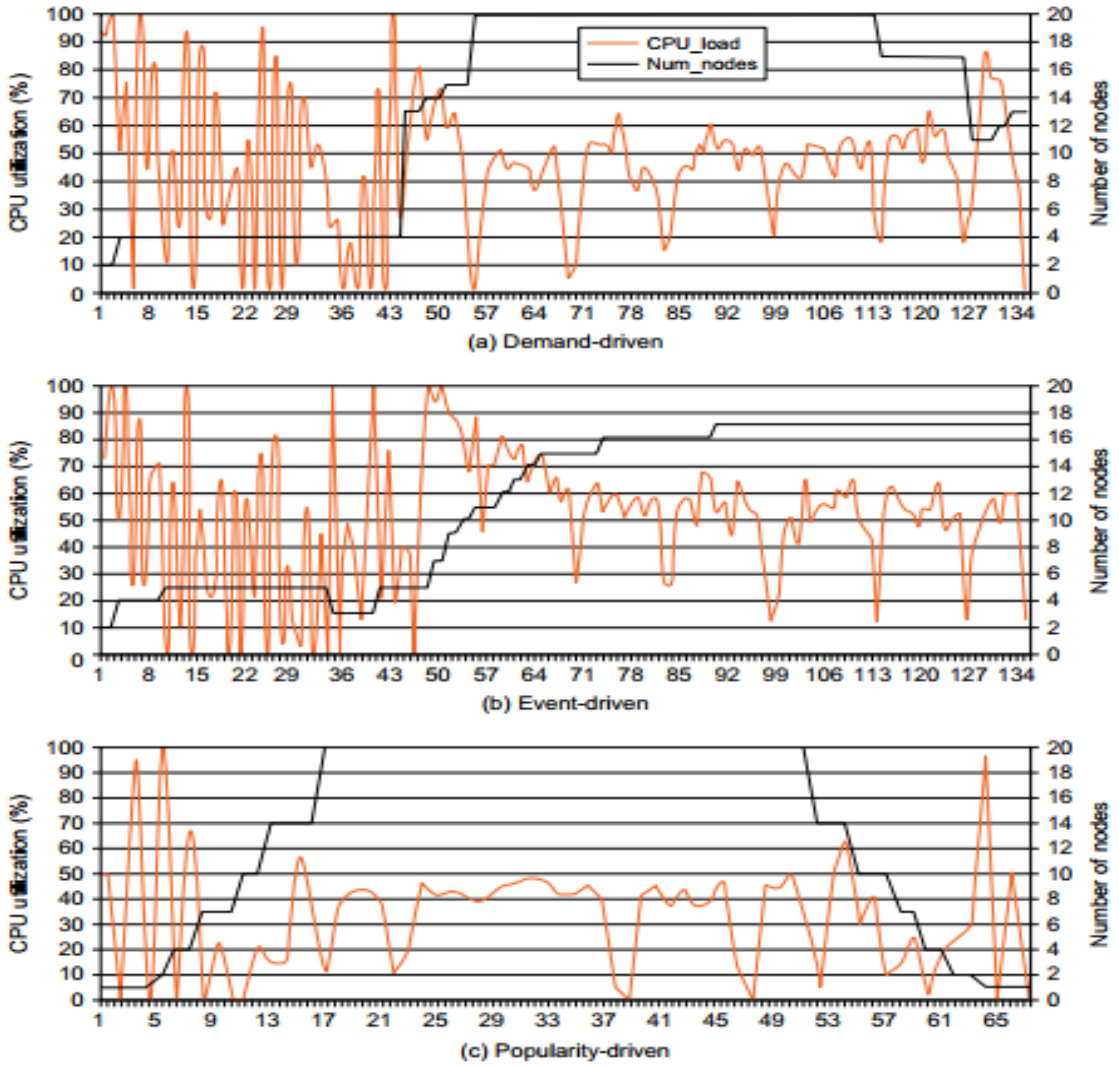

FIGURE 4.25

EC2 performance results on the AWS EC2 platform, collected from experiments at the University of Southern California using three resource provisioning methods.

- The x-axis in Figure 4.25 is the time scale in milliseconds. In the beginning, heavy fluctuations of CPU load are encountered. All three methods have demanded a few VM instances initially. Gradually, the utilization rate becomes more stabilized with a maximum of 20 VMs (100 percent utilization) provided for demand-driven provisioning in Figure 4.25(a).
- However, the event-driven method reaches a stable peak of 17 VMs toward the end of the event and drops quickly in Figure 4.25(b). The popularity provisioning shown in Figure 4.25(c) leads to a similar fluctuation with peak VM utilization in the middle of the plot.

(b) Event-Driven Resource Provisioning:

- This scheme adds or removes machine instances based on a specific time event. The scheme works better for seasonal or predicted events such as Christmastime in the West and the Lunar New Year in the East.
- During these events, the number of users grows before the event period and then decreases during the event period. This scheme anticipates peak traffic before it happens. The method results in a minimal loss of QoS, if the event is predicted correctly. Otherwise, wasted resources are even greater due to events that do not follow a fixed pattern.

(c) Popularity-Driven Resource Provisioning:

- In this method, the Internet searches for popularity of certain applications and creates the instances by popularity demand. The scheme anticipates increased traffic with popularity. Again, the scheme has a minimal loss of QoS, if the predicted popularity is correct.
- Resources may be wasted if traffic does not occur as expected. In Figure 4.25(c), EC2 performance by CPU utilization rate (the dark curve with the percentage scale shown on the left) is plotted against the number of VMs provisioned (the light curves with scale shown on the right, with a maximum of 20 VMs provisioned).

Global Exchange of Cloud Resources:

- In order to support a large number of application service consumers from around the world, cloud infrastructure providers (i.e., IaaS providers) have established data centers in multiple geographical locations to provide redundancy and ensure reliability in case of site failures.
- For example, Amazon has data centers in the United States (e.g., one on the East Coast and another on the West Coast) and Europe. However, currently Amazon expects its cloud customers (i.e., SaaS providers) to express a preference regarding where they want their application services to be hosted. Amazon does not provide seamless/automatic mechanisms for scaling its hosted services across multiple geographically distributed data centers.
- This approach has many shortcomings. First, it is difficult for cloud customers to determine in advance the best location for hosting their services as they may not know the origin of consumers of their services. Second, SaaS providers may not be able to meet the QoS expectations of their service consumers originating from multiple geographical locations. This necessitates building mechanisms for seamless federation of data centers of a cloud provider or providers supporting dynamic scaling of applications across multiple domains in order to meet QoS targets of cloud customers.

Figure 4.30 shows the high-level components of the Melbourne group's proposed InterCloud architecture

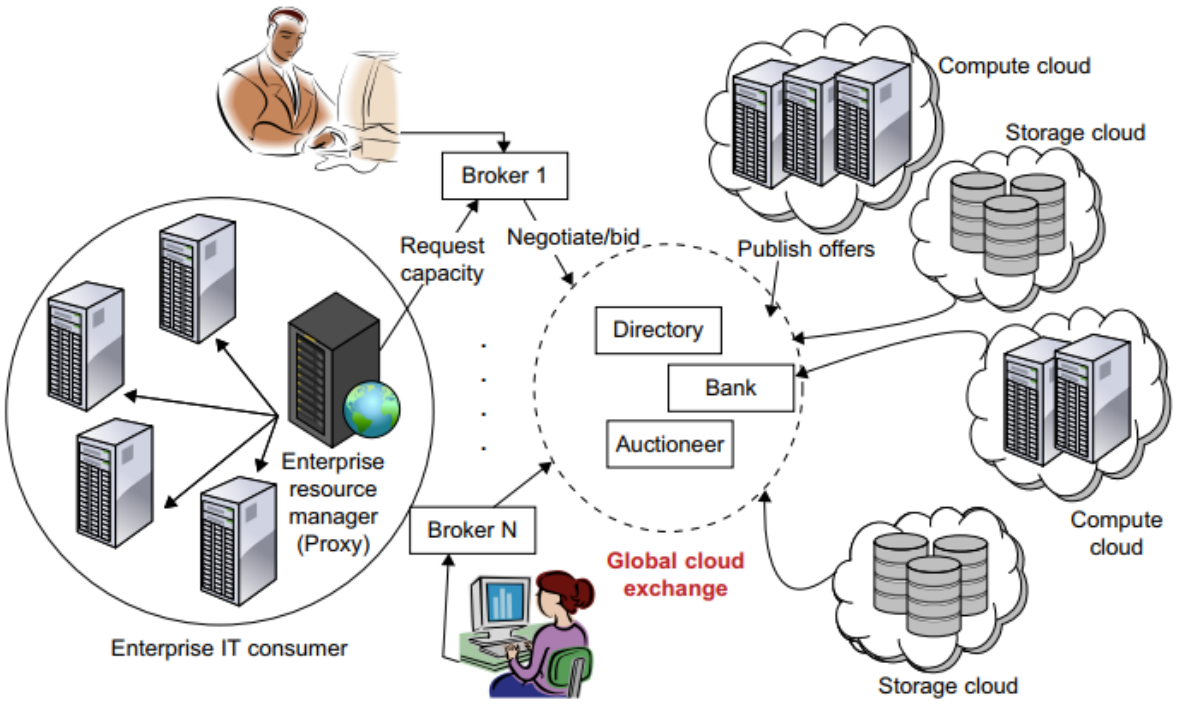

FIGURE 4.30

Inter-cloud exchange of cloud resources through brokering.

- The Cloudbus Project at the University of Melbourne has proposed InterCloud architecture supporting brokering and exchange of cloud resources for scaling applications across multiple clouds.
- By realizing InterCloud architectural principles in mechanisms in their offering, cloud providers will be able to dynamically expand or resize their provisioning capability based on sudden spikes in workload demands by leasing available computational and storage capabilities from other cloud service providers; operate as part of a market-driven resource leasing federation, where application service providers such as Salesforce.com host their services based on negotiated SLA contracts driven by competitive market prices; and deliver on-demand, reliable, cost-effective, and QoS-aware services based on virtualization technologies while ensuring high QoS standards and minimizing service costs.

Security Overview:

- Lacking trust between service providers and cloud users has hindered the universal acceptance of cloud computing as a service on demand. In the past, trust models have been developed to protect mainly e-commerce and online shopping provided by eBay and Amazon.

- For web and cloud services, trust and security become even more demanding, because leaving user applications completely to the cloud providers has faced strong resistance by most PC and server users. Cloud platforms become worrisome to some users for lack of privacy protection, security assurance, and copyright protection.
- Trust is a social problem, not a pure technical issue. However, the social problem can be solved with a technical approach. Common sense dictates that technology can enhance trust, justice, reputation, credit, and assurance in Internet applications. As a virtual environment, the cloud poses new security threats that are more difficult to contain than traditional client and server configurations.

Cloud Security Challenges:

Security has been one of the most challenging issues for the IT executives particularly in cloud implementation. There exist numerous security anxieties that are preventing companies from captivating advantages of the cloud.

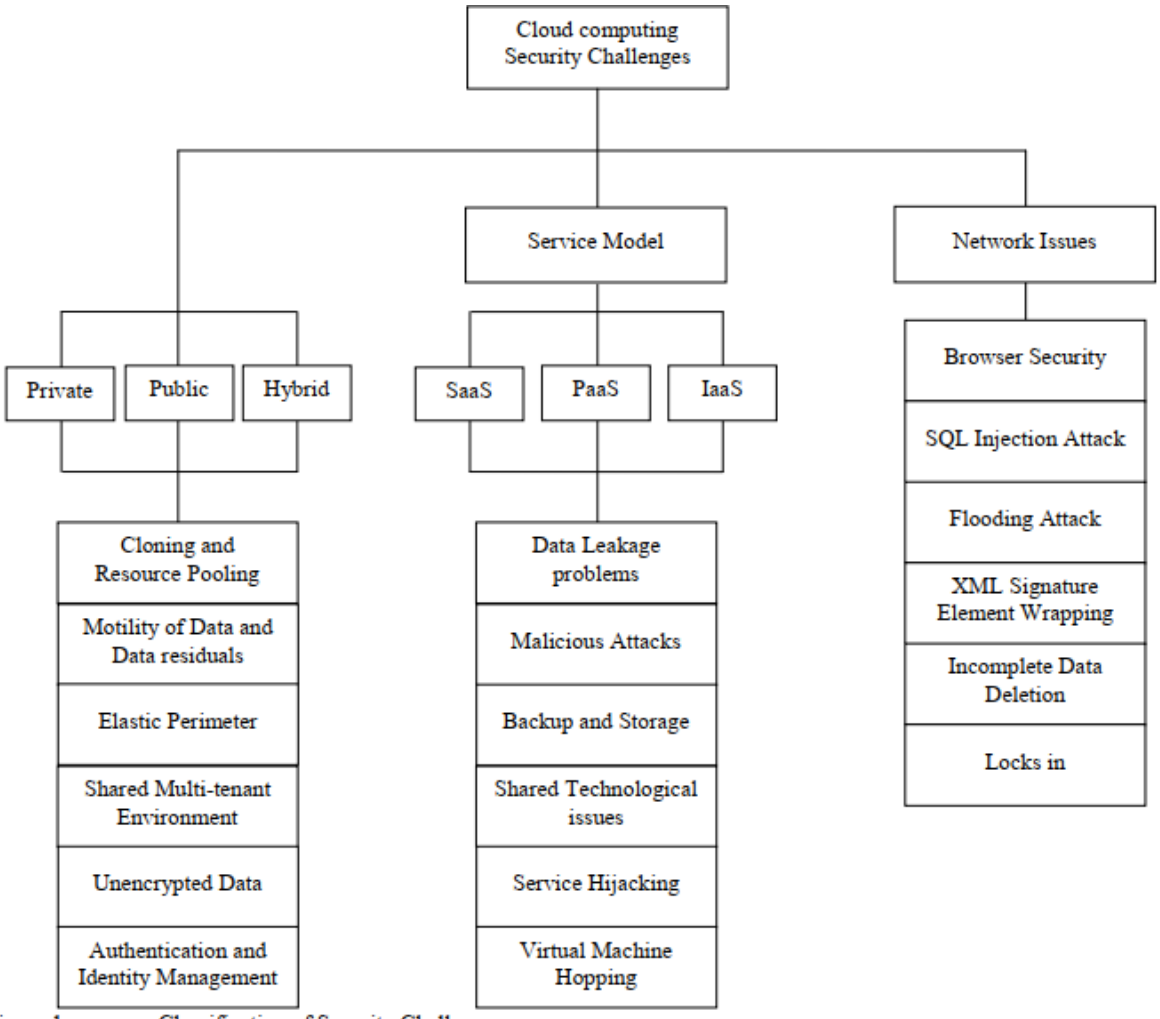

Figure 1: Classification of Security Challenge

- Fig. 1 represents the schematic diagram showing the hierarchy of the cloud computing, with security challenges on both the cloud computing models: Deployment and Service models and also the issues related to Networks.
- The classification provided above reveals various common challenges under cloud computing. The Deployment model is classified further as Private, Public and Hybrid Cloud and the security issues of the same have been exposed in common. Further, the Service model is classified into the SaaS, PaaS and IaaS briefing its security challenges in common.
- The security challenges with respect to network is also shown as for any internet based service, network is considered as the backbone for cloud computing.

Various security challenges related to these deployment models are as follows:

1. **Cloning and Resource Pooling:**
    - Cloning deals with replicating or duplicating the data. It leads to data leakage problems revealing the machine's authenticity. Resource pooling as a service

provided to the users by the provider to use various resources and share the same according to their application demand.

- Resource Pooling relates to the unauthorized access due to sharing through the same network. While the study on Virtual and Cloud Computing by various researches states that a Virtual Machine can easily be provisioned, they can also be inversed to previous cases, paused, easily restarted, readily cloned and migrated between two physical servers, leading to non-auditable security threats.

2. **Motility of Data and Data residuals:**
    - For the best use of resources, data often is moved to cloud infrastructure. As a result the enterprise would be devoid of the location where data is put on the cloud. This is true with public cloud.
    - With this data movement, the residuals of data is left behind which may be accessed by unauthorized users. Data-remnant causes very less security threats in private cloud but severe security issues may evolve in public cloud donations. This again may lead to data security threats like data leakage, data remnants and inconsistent data.

3. **Elastic Perimeter:**
    - A cloud infrastructure, particularly comprising of private cloud, creates an elastic perimeter. Various departments and users throughout the organization allow sharing of different resources to increase facility of access but unfortunately lead to data breach problem.
    - In private clouds, the resources are centralized and distributed as per demand. The resource treatment transfers resources based on the requirements of the users thus leading to problems of data loss, where any user may try to access secure data with ease.

4. **Shared Multi-tenant Environment:**
    - Multi-tenancy is defined as one of the very vital attribute of cloud computing, which allows multiple users to run their distinct applications concurrently on the same physical infrastructure hiding user data from each other. But the shared multi-tenant character of public cloud adds security risks such as illegal access of data by other renter using the same hardware.
    - A multi-tenant environment might also depict some resource contention issues when any tenant consumes some unequal amount of resources. This might be either due to genuine periodic requirements or any hack attack.

5. **Unencrypted Data:**
    - Data encryption is a process that helps to address various external and malicious threats. Unencrypted data is vulnerable for susceptible data, as it does not provide any security mechanism. These unencrypted data can easily be accessed by unauthorized users.

- Unencrypted data risks the user data leading cloud server to escape various data information to unauthorized users. For example, the famous file sharing service Dropbox was accused for using a single encryption key for all user data the company stored.

6. **Authentication and Identity Management:**

- With the help of cloud, a user is facilitated to access its private data and make it available to various services across the network.
- Identity management helps in authenticating the users through their credentials. But, a key issue, concerned with Identity Management (IDM), is the disadvantage of interoperability resulting from different identity tokens and identity negotiation protocols as well as the architectural pattern.
- IDM leads to a problem of intrusion by unauthorized users. They even discussed that in order to serve authentication, apart from providing a password, a multi-factor authentication using smart card and fingerprint must be implemented for attaining higher level of security.

Service models and its security challenges:

Various cloud services like Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) are delivered and used in real time over the cloud. SaaS as a multi tenant platform which is commonly referred to as Application Service Provider aiding distribution of services across cloud users. While the PaaS provides the developers a platform to work with all the environments and systems for the developing, testing and deploying web applications through the cloud service. The computer infrastructure needed for this application to run on a particular platform is provided by IaaS which may give more flexibility and pay-as-you-go scheme.

Various security challenges with the service models are discussed below:

1. Data Leakage and consequent problems:

- Data deletion or alteration without backup leads to certain drastic data related problems like security, integrity, locality, segregation and breaches. This would lead to sensitive data being accessed by the unauthorized users. Cloud platforms should provide new services in order to collect context information and to perform analysis and manage data privacy so as to support applications requesting the information.
- One solution to this data leakage problem is de duplication with allowing a limitation on number of user uploads per time window. The term deduplication means storing only a single copy of redundant data and providing just a link to this copy rather than storing actual copies of this data.

2. Malicious Attacks:

- The threat of malicious attackers is augmented for customers of cloud services by the use of various IT services which lacks the lucidity between the procedure and process relating to service providers.
- Malicious users may gain access to certain confidential data and thus leading to data breaches. Malicious attacks by the unauthorized users on the victim's IP address and physical server. An access control mechanism tool can be thought of to control unauthorized user in accessing secured data.

3. Backup and Storage:

- The cloud vendor must ensure that regular backup of data is implemented that even ensure security with all measures. But this backup data is generally found in unencrypted form leading to misuse of the data by unauthorized parties. Thus data backups lead to various security threats.

4. Shared Technological issues:

- IaaS vendors transport their services in a scalable way by contributing infrastructure. But this structure does not offer strong isolation properties for a multi-tenant architecture. Hence in order to address this gap, a virtualization hypervisor intercede the access between guest operating systems and the physical compute resources.

5. Service Hijacking:

- Service hijacking is associated with gaining an illegal control on certain authorized services by various unauthorized users. It accounts for various techniques like phishing, exploitation of software and fraud. This is considered as one of the top most threats.
- Account hijacking has been pointed as one of the severe threats. The chances of hijacking ones account increases considerably as no native API's are used for registering various cloud services.

6. VM Hopping:

- With VM hopping, an attacker on one VM gains rights to use another victim VM. The attacker can check the victim VM's resource procedure, alter its configurations and can even delete stored data, thus, putting it in danger the VM's confidentiality, integrity, and availability.
- A requirement for this attack is that the two VMs must be operating on the same host, and the attacker must recognize the victim VM's IP address. Although PaaS and IaaS users have partial authority, an attacker can get hold of or decide the IP address using benchmark customer capabilities on the basis of various tricks and combinational inputs

to fetch user's IP. Thus it can be inferred that VM hopping is a rational threat in cloud computing.

7. VM Mobility:

- The contents of VM virtual disks are saved as files such that VMs can be copied from one host to another host over the system or via moveable storage devices with no physically pilfering a hard drive.
- VM mobility might offer quick use but could show the way to security problems likewise, the rapid spread of susceptible configurations that an attacker could make use of to endanger the security of a novel host.

8. VM Denial of Service:

- Virtualization lets numerous VMs split physical resources like CPU, network bandwidth and memory or disk.
- A Denial-of-Service or DoS attack in virtualization takes place when one VM occupies all the obtainable physical resources such that the hypervisor cannot hold up more VMs and accessibility is endangered.
- The most excellent move towards preventing a DoS attack is to bound resource allocation using correct configurations.

Network issues on Cloud:

Cloud computing mainly depends upon internet and remote computers or servers in maintaining data for running various applications.

Various security challenges with the network models are discussed below:

1. Browser Security:

- Every client uses browser to send the information on network. The browser uses SSL technology to encrypt user's identity and credentials. But hackers from the intermediary host may acquire these credentials by the use of sniffing packages installed on the intermediary host.
- In order to overcome this, one should have a single identity but this credential must allow various levels of assurance which can be achieved by obtaining approvals digitally.

2. SQL Injection Attack:

- These attacks are malicious act on the cloud computing in which a spiteful code is inserted into a model SQL code. This allows the invader to gain unauthorized access to a database and eventually to other confidential information. Further, SQL injection attacks.

3. Flooding Attacks:

- In this attack the invader sends the request for resources on the cloud rapidly so that the cloud gets flooded with the ample requests.
- As per the study carried out by IBM, cloud has a property to expand on the basis of large amount of request. It will expand in order to fulfil the requests of invader making the resources inaccessible for the normal users.

4. XML Signature Element Wrapping:

- It is found to be a very renowned web service attack. It protects identity value and host name from illegal party but cannot protect the position in the documents.
- The attacker simply targets the host computer by sending the SOAP messages and putting any scrambled data which the user of the host computer cannot understand.

5. Incomplete Data Deletion:

- Incomplete data deletion is treated as hazardous one in cloud computing. when data is deleted, it does not remove the replicated data placed on a dedicated backup server. The operating system of that server will not delete data unless it is specifically commanded by network service provider.
- Precise data deletion is majorly impossible because copies of data are saved in replica but are not available for usage.

6. Locks in:

- Locks in is a small tender in the manner of tools, standard data format or procedures, services edge that could embark on data, application and service portability, not leading to facilitate the customer in transferring from one cloud provider to another or transferring the services back to home IT location.

Software-as-a-Service Security:

SaaS security is the managing, monitoring, and safeguarding of sensitive data from cyber-attacks. With the increase in efficiency and scalability of cloud-based IT infrastructures, organizations are also more vulnerable.

SaaS maintenance measures such as SaaS security posture management ensure privacy and safety of user data. From customer payment information to inter-departmental exchange of information, strengthening the security of SaaS applications is vital to your success.

To help this cause, regulatory bodies worldwide have issued security guidelines such as GDPR (General Data Protection Regulation of EU), EU-US and the Swiss-US Privacy Shield Frameworks.

Every SaaS business must adopt these guidelines to offer safe and secure services. Whether you are starting anew or adding an aspect to your IT arsenal, SaaS security is essential for successful ventures.

SaaS providers handle much of the security for a cloud application. The SaaS provider is responsible for securing the platform, network, applications, operating system, and physical infrastructure. However, providers are not responsible for securing customer data or user access to it. Some providers offer a bare minimum of security, while others offer a wide range of SaaS security options.

Below are SaaS security practices that organizations can adopt to protect data in their SaaS applications.

- **Detect rogue services and compromised accounts**: Organizations can use tools, such as cloud access security brokers (CASB) to audit their networks for unauthorized cloud services and compromised accounts.
- **Apply identity and access management (IAM)**: A role-based identity and access management solution can ensure that end users do not gain access to more resources than they require for their jobs. IAM solutions use processes and user access policies to determine what files and applications a particular user can access. An organization can apply role-based permissions to data so that end users will see only the data they're authorized to view.
- **Encrypt cloud data**: Data encryption protects both data at rest (in storage) and data in transit between the end user and the cloud or between cloud applications. Government regulations usually require encryption of sensitive data. Sensitive data includes financial information, healthcare data, and personally identifiable information (PII). While a SaaS vendor may provide some type of encryption, an organization can enhance data security by applying its own encryption, such as by implementing a cloud access security broker (CASB).
- **Enforce data loss prevention (DLP)**: DLP software monitors for sensitive data within SaaS applications or outgoing transmissions of sensitive data and blocks the transmission. DLP software detects and prevents sensitive data from being downloaded to personal devices and blocks malware or hackers from attempting to access and download data.
- **Monitor collaborative sharing of data**: Collaboration controls can detect granular permissions on files that are shared with other users, including users outside the organization who access the file through a web link. Employees may inadvertently or intentionally share confidential documents through email, team spaces, and cloud storage sites such as Dropbox.
- **Check provider's security**: An audit of a SaaS provider can include checks on its compliance with data security and privacy regulations, data encryption policies, employee security practices, cybersecurity protection, and data segregation policies.

Security Governance:

- Cloud security governance refers to the management model that facilitates effective and efficient security management and operations in the cloud environment so that an enterprise's business targets are achieved.
- This model incorporates a hierarchy of executive mandates, performance expectations, operational practices, structures, and metrics that, when implemented, result in the optimization of business value for an enterprise.

Cloud Security Governance Challenges

Whether developing a governance model from the start or having to retrofit one on existing investments in cloud, these are some of the common challenges:

1. Lack of senior management participation and buy-in:

- The lack of a senior management influenced and endorsed security policy is one of the common challenges facing cloud customers. An enterprise security policy is intended to set the executive tone, principles and expectations for security management and operations in the cloud.
- However, many enterprises tend to author security policies that are often laden with tactical content, and lack executive input or influence. The result of this situation is the ineffective definition and communication of executive tone and expectations for security in the cloud.
- To resolve this challenge, it is essential to engage enterprise executives in the discussion and definition of tone and expectations for security that will feed a formal enterprise security policy. It is also essential for the executives to take full accountability for the policy, communicating inherent provisions to the enterprise, and subsequently enforcing compliance

2. Lack of embedded management operational controls

- Another common cloud security governance challenge is lack of embedded management controls into cloud security operational processes and procedures.
- Controls are often interpreted as an auditor's checklist or repackaged as procedures, and as a result, are not effectively embedded into security operational processes and procedures as they should be, for purposes of optimizing value and reducing day-to-day operational risks.
- This lack of embedded controls may result in operational risks that may not be apparent to the enterprise. For example, the security configuration of a device may be modified (change event) by a staffer without proper analysis of the business impact (control) of the modification. The net result could be the introduction of exploitable security weaknesses that may not have been apparent with this modification. The enterprise would now have

to live with an inherent operational risk that could have been avoided if the control had been embedded in the change execution process.

3. Lack of operating model, roles, and responsibilities

- Many enterprises moving into the cloud environment tend to lack a formal operating model for security, or do not have strategic and tactical roles and responsibilities properly defined and operationalized.
- This situation stifles the effectiveness of a security management and operational function/organization to support security in the cloud. Simply, establishing a hierarchy that includes designating an accountable official at the top, supported by a stakeholder committee, management team, operational staff, and third-party provider support (in that order) can help an enterprise to better manage and control security in the cloud, and protect associated investments in accordance with enterprise business goals.
- This hierarchy can be employed in an in-sourced, out-sourced, or co-sourced model depending on the culture, norms, and risk tolerance of the enterprise.

4. Lack of metrics for measuring performance and risk:

- Another major challenge for cloud customers is the lack of defined metrics to measure security performance and risks – a problem that also stifles executive visibility into the real security risks in the cloud.
- This challenge is directly attributable to the combination of other challenges discussed above. For example, a metric that quantitatively measures the number of exploitable security vulnerabilities on host devices in the cloud over time can be leveraged as an indicator of risk in the host device environment.
- Similarly, a metric that measures the number of user-reported security incidents over a given period can be leveraged as a performance indicator of staff awareness and training efforts. Metrics enable executive visibility into the extent to which security tone and expectations (per established policy) are being met within the enterprise and support prompt decision-making in reducing risks or rewarding performance as appropriate.

Key Objectives for Cloud Security Governance:

1. **Strategic Alignment**: Enterprises should mandate that security investments, services, and projects in the cloud are executed to achieve established business goals (e.g., market competitiveness, financial, or operational performance).

2. **Value Delivery**

   Enterprises should define, operationalize, and maintain an appropriate security function/organization with appropriate strategic and tactical representation, and charged

with the responsibility to maximize the business value (Key Goal Indicators, ROI) from the pursuit of security initiatives in the cloud.

3. Risk Mitigation: Security initiatives in the cloud should be subject to measurements that gauge effectiveness in mitigating risk to the enterprise (Key Risk Indicators). These initiatives should also yield results that progressively demonstrate a reduction in these risks over time.

4. Effective Use of Resources: It is important for enterprises to establish a practical operating model for managing and performing security operations in the cloud, including the proper definition and operationalization of due processes, the institution of appropriate roles and responsibilities, and use of relevant tools for overall efficiency and effectiveness.

5. Sustained Performance: Security initiatives in the cloud should be measurable in terms of performance, value and risk to the enterprise (Key Performance Indicators, Key Risk Indicators), and yield results that demonstrate attainment of desired targets (Key Goal Indicators) over time.

Virtual Machine Security:

- A virtual machine (VM) is a digital version of a physical computer. Virtual machine software can run programs and operating systems, store data, connect to networks, and do other computing functions, and requires maintenance such as updates and system monitoring.
- VMs are the basic building blocks of virtualized computing resources and play a primary role in creating any application, tool, or environment—for virtual machines online and on-premises.
- In the cloud environment, physical servers are consolidated to multiple virtual machine instances on virtualized servers. Not only can data center security teams replicate typical security controls for the data center at large to secure the virtual machines, they can also advise their customers on how to prepare these machines for migration to a cloud environment when appropriate.
- Firewalls, intrusion detection and prevention, integrity monitoring, and log inspection can all be deployed as software on virtual machines to increase protection and maintain compliance integrity of servers and applications as virtual resources move from on-premises to public cloud environments. By deploying this traditional line of defense to the virtual machine itself, you can enable critical applications and data to be moved to the cloud securely. To facilitate the centralized management of a server firewall policy, the security software loaded onto a virtual machine should include a bidirectional stateful firewall that enables virtual machine isolation and location awareness, thereby enabling a tightened policy and the flexibility to move the virtual machine from on-premises to cloud resources. Integrity monitoring and log inspection software must be applied at the virtual machine level.

- This approach to virtual machine security, which connects the machine back to the mother ship, has some advantages in that the security software can be put into a single software agent that provides for consistent control and management throughout the cloud while integrating seamlessly back into existing security infrastructure investments, providing economies of scale, deployment, and cost savings for both the service provider and the enterprise.

Identity and access management (IAM):

- It is a set of processes, policies, and tools for defining and managing the roles and access privileges of individual network entities (users and devices) to a variety of cloud and on-premises applications.
- Users include customers, partners, and employees; devices include computers, smartphones, routers, servers, controllers and sensors. The core objective of IAM systems is one digital identity per individual or item. Once that digital identity has been established, it must be maintained, modified, and monitored throughout each user's or device's access lifecycle.
- Thus, the overarching goal of identity management is to grant access to the enterprise assets that users and devices have rights to in a given context. That includes onboarding users and systems, permission authorizations, and the offboarding of users and devices in a timely manner.
- Top IAM tools include:

    1. CloudKnox Permissions Management Platform
    2. CyberArk
    3. ForgeRock
    4. Microsoft Azure Active Directory
    5. Okta
    6. OneLogin Trusted Experience Platform
    7. Ping Identity Intelligent Identity Platform
    8. SailPoint

Benefits of IAM:

1. Improved security:

IAM solutions help identify and mitigate security risks. You can use IAM to identify policy violations or remove inappropriate access privileges, without having to search through multiple distributed systems. You can also leverage IAM to ensure that security measures are in place to meet regulatory and audit requirements.

2. Information sharing

IAM provides a common platform for access and identity management information. You can apply the same security pollies across all the operating platforms and devices used by the organization. IAM frameworks can help you enforce policies related to user authentication, privileges, and validation, and attend to “privilege creep”.

3. Ease of use

IAM simplifies signup, sign-in and user management processes for application owners, end-users and system administrators. IAM makes it simple to provide and manage access, and this promotes user satisfaction.

4. Productivity gains

IAM centralizes and automates the identity and access management lifecycle, creating automated workflows for scenarios like a new hire or a role transition. This can improve processing time for access and identity changes and reduce errors.

5. Reduced IT Costs

IAM services can lower operating costs. Using federated identity services means you no longer need local identities for external uses; this makes application administration easier. Cloud-based IAM services can reduce the need to buy and maintain on-premise infrastructure.

Cloud Security Standards:

With the shift towards cloud infrastructure, compliance standards had to evolve. Cloud services and platforms are now required to maintain compliance with different federal, international, local, and state security laws, regulations and standards.

Compliance standards such as ISO, PCI DSS, HIPAA, and GDPR, have specific requirements for cloud environments. Where mandatory government regulations are concerned, violations may result in legal penalties such as fines.

In addition to general compliance standards, specialized standards have evolved, which can help organizations achieve a secure cloud environment. These include the Center for Internet Security (CIS) Cloud Security Benchmarks, the Cloud Security Alliance (CSA) Controls Matrix, and the Cloud Architecture Framework.

Following are some cloud security standards:

Following are the cloud security standards :

Information Technology Infrastructure Library (ITIL) :

i. It is a set of best practices and guidelines that define an integrated, process-based approach for managing information technology services.

ii. ITIL helps to make sure that proper security measures are taken at all important levels, namely strategic, tactical, and operational level.

iii. Many IT organizations employ security management framework- Information Technology Infrastructure Library (ITIL)

iv. This industry standard management framework provides guidance for planning and implementing a governance program with sustaining management processes that protect information assets and thus provide security.

v. Hence, it provides a framework with continuous improvement that is necessary to align and realign IT services to changing business needs.

Open Virtualization Format (OVF) :

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

ii. OVF thus provides customers, vendor and platform independence as it facilitates mobility of virtual machines.

iii. Across the cloud OVF plays a major role in providing cross-platform portability. It also helps to provide simplified deployment over multiple platforms.

iv. An OVF format virtual machine can be deployed easily by customers. They can do so on the platform of their choice. It helps to enhance customer experience as it provides customers with portability, platform independence, verification, signing, versioning, and licensing terms.

3. ITU-T X.1601 :

i. The ITU standard presents a sketch of issues pertaining to cloud computing and proposes a framework for cloud security.

ii. It talks in detail about various security challenges and ways to reduce these security risks in cloud computing. It also discusses a framework that provides an insight into what security capabilities are required for making the cloud secure and facing security challenges.

iii. ITU-T X.1601 starts by listing down major security threats that the cloud can encounter.

iv. The standard discusses the security challenges based on the nature of the role that an individual or an organization plays in the cloud computing paradigm.

v. The standard divides the roles of an individual or an organization into following three categories :

a. **Cloud Service Provider (CSP) :** An individual or an organization responsible for making cloud services available.

b. **Cloud Service Customer (CSC) :** An individual or an organization that uses cloud services.

c. **Cloud Service Partner (CSN) :** A partner that helps support the CSPs or the CSCs.

ISO Standards

The International Organization for Standardization (ISO) 27001 created a standard to assist organizations, helping them safeguard their information using best practices.

The ISO has created standards for many kinds of systems and technologies, such as:

- **ISO/IEC 17789 (2014)** — this standard outlines cloud computing activities, functional components, and roles, including the way they interact.
- **ISO/IEC 19944-1 (2020)** — this standard specifies how data is transported via cloud service centers and cloud service users.
- **ISO/IEC Technical Specification 23167 (2020)** — this standard specifies techniques and technologies employed in cloud computing, such as VMs, containers, and hypervisors.
- **ISO/IEC 27018 (2019)** — this document describes guidelines founded on ISO/IEC 27002, emphasising the safeguarding of personal identifiable information (PII) within the public cloud.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a series of security conditions for merchants who accept debit or credit cards. PCI DSS relates to organizations that store or process cardholder data.

If your organization retains and handles sensitive payment card details in the cloud, it is your responsibility to provide your IT team with advanced cloud expertise to create and upkeep your cloud environment safely. If you don't adhere to the PCI DSS Cloud Computing Guidelines, you may lose your capacity to process payment card transactions.

HIPAA

To safeguard the health-related data of individuals, the Health Insurance Portability and Accountability Act (HIPAA) features sections that directly relate to the security of information.

HIPAA is a law that relates to organizations that deal with personally identifiable medical information. In terms of information security, the HIPAA Security Rule (HSR) is the most applicable. The HSR provides guidelines for keeping an individual's electronic health details safe. This includes information that a covered entity uses, creates, maintains, or receives.

If your organization employs cloud-based services (IaaS, PaaS, SaaS) to oversee and move health information, it is your task to make sure the service provider is HIPAA-compliant. You also have to implement best practices for overseeing cloud configurations.

GDPR

One of the strictest and widely applicable information privacy laws, from around the globe, is the General Data Protection Regulation (GDPR). Its central aim is to safeguard the personal information of businesses and individuals in the European Union (EU).