INTER CLOUD

The idea behind an inter cloud is that a single common functionality would combine many different individual clouds into one seamless mass in terms of on-demand operations. To understand how this works, it's helpful to think about how existing cloud computing setups are designed.

Cloud hosting is largely intended to deliver on-demand services. Through careful use of scalable and highly engineered technologies, cloud providers are able to offer customers the ability to change their levels of service in many ways without waiting for physical changes to occur. Terms like rapid elasticity, resource pooling and on-demand self-service are already part of cloud hosting service designs that are set up to make sure the customer or client never has to deal with limitations or disruptions. Building on all of these ideas, the inter cloud would simply make sure that a cloud could use resources beyond its reach by taking advantage of pre-existing contracts with other cloud providers.

TYPES OF INTER CLOUD RESOURCE MANAGEMENT

Federation Clouds: A Federation cloud is an Inter-Cloud where a set of cloud providers willingly interconnect their cloud infrastructures in order to share resources among each other10. The cloud providers in the federation voluntarily collaborate to exchange resources. This type of Inter-Cloud is suitable for collaboration of governmental clouds (Clouds owned and utilized by nonprofit institution or government) or private cloud portfolios (Cloud is a part of a portfolio of clouds where the clouds belong to the same organization). Types of federation clouds are Peer to Peer and Centralized clouds.

Multi-Cloud: In a Multi-Cloud, a client or service uses multiple independent clouds. A multi-cloud environment has no volunteer interconnection and sharing of the cloud service providers' infrastructures. Managing resource provisioning and scheduling is the responsibility of client or their representatives. This approach is used to utilize resources from both governmental clouds and private cloud portfolios. Types of Multi-cloud are Services and Libraries.

CHALLENGES IN FEDERATIONS OF CLOUD INFRASTRUCTURE

1. Application Service Behavior Prediction: It is important that the system should be able to foresee the demands and the behavior of the services. Only when it can predict, it can take decisions intelligently to dynamically scale up and down. Prediction and forecasting models must be built. The challenge is to build such models that accurately learn and fit statistical functions suitable to different behaviors. It is more challenging to correlate between different behaviors of a service.

2. Flexible Mapping of Services to Resources: It is important to maximize the efficiency, cost-effectiveness and utilization because of high operating costs and energy requirements. The system has to compute the best software and hardware configurations which result in a complex process of mapping services to cloud resources. Mapping of services must guarantee that QoS targets are satisfied along with maximum system efficiency and utilization.

3. Economic Models Driven Optimization Techniques: Combinatorial optimization problem is a market driven decision making strategy which searches the optimal combinations of services and deployment plans. Optimization models must be developed which optimize both resource-centric and user-centric QoS targets.

4. Integration and Interoperability: SMEs have a large amount of IT assets like business applications in their premises and may not be migrated to the cloud. Sensitive data in an enterprise also may not be migrated to the cloud for security reasons and privacy. A need related to integration and interoperability arises between assets on premises and the cloud services. Issues related to identity management, data management, and business process orchestration need to be resolved.

5. Scalable Monitoring of System Components: The components in a federated system are distributed but the techniques employed for system monitoring and management use centralized approaches. Due to concerns of scalability, performance and reliability arising from the management of multiple service queues and large volume of service requests, centralized approaches are not suitable and architectures using service monitoring and management services based on decentralized messaging and indexing models are needed.

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.

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

RESOURCE PROVISIONING TYPES

They are of 3 Types:-

Static Provisioning: For applications that have predictable and generally unchanging demands/workloads, it is possible to use “static provisioning" effectively. With advance provisioning, the customer contracts with the provider for services and the provider prepares the appropriate resources in advance of start of service. The customer is charged a flat fee or is billed on a monthly basis. 2) Dynamic Provisioning: In cases where demand by applications may change or vary, “dynamic provisioning" techniques have been suggested whereby VMs may be migrated on-the-fly to new compute nodes within the cloud. With dynamic provisioning, the provider allocates more resources as they are needed and removes them when they are not. The customer is billed on a pay-per-use basis.

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

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

III. Parameters for Resource Provisioning

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

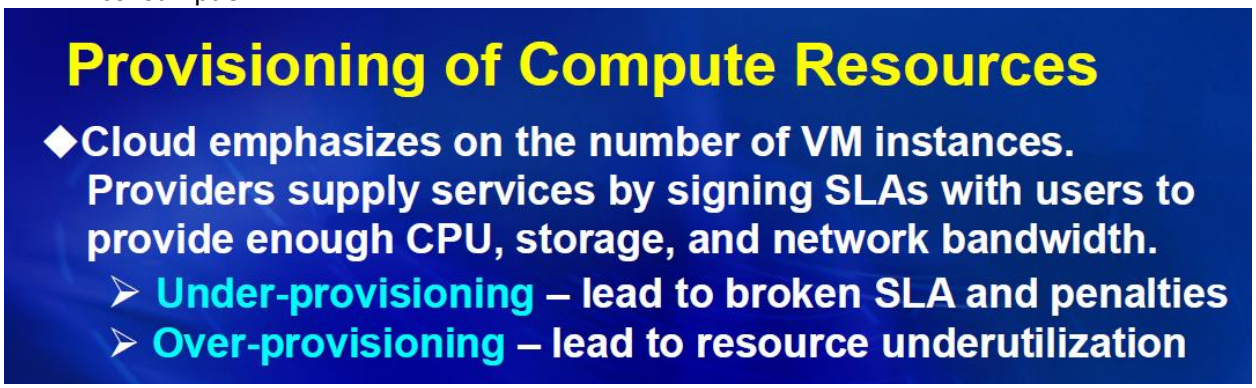
ii) Minimize Cost: From the Cloud user point of view cost should be minimized.

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

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

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

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



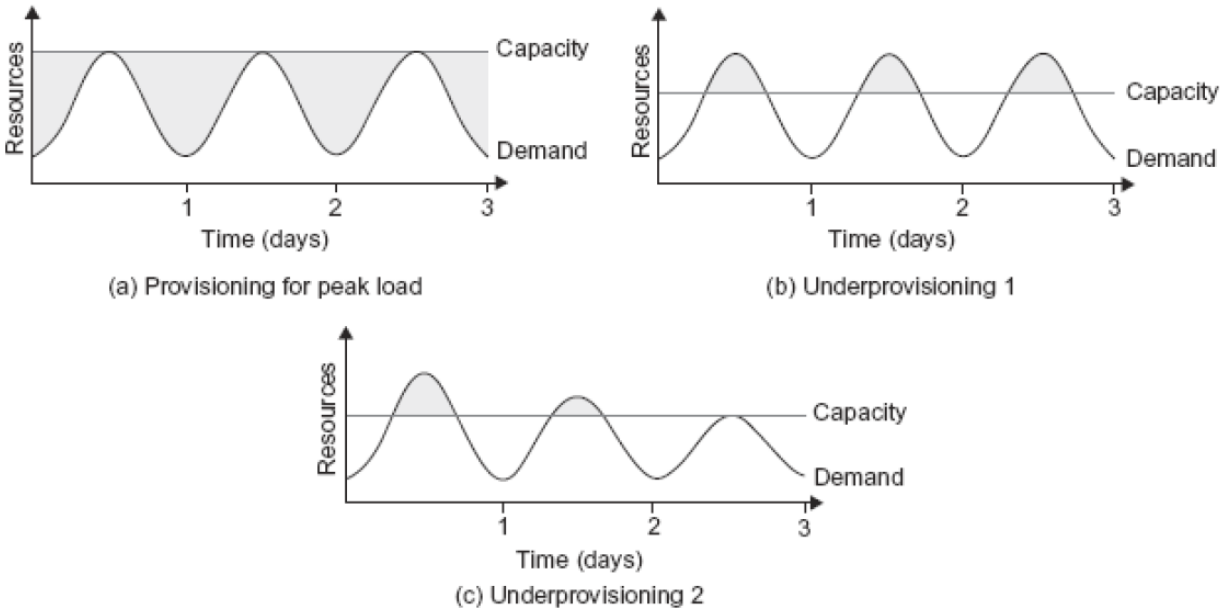


FIGURE 4.24

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

(Courtesy of Armbrust, et al., UC Berkeley, 2009 [4])

Resource Provisioning Methods

- **Demand-driven method** – add/remove computing instances based on the current utilization level of the allocated resources.
- **Event-driven method** – add/remove resources bases on a specific time event. This scheme anticipates peak traffic before it happens.
- **Popularity-driven method** – by searching for popularity of certain applications and creating the instances by popularity demand.

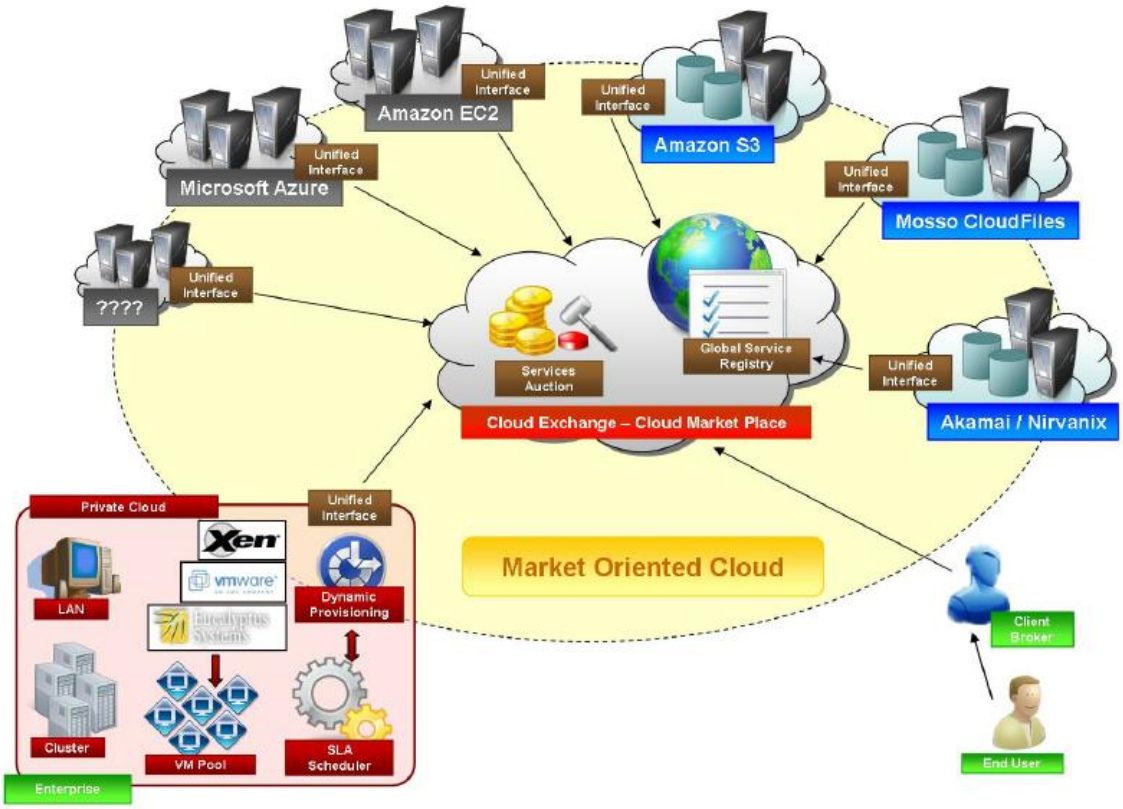
GLOBAL EXCHANGE OF CLOUD RESOURCES

Limitations of present service providers

- Inflexible pricing
- Consumers are restricted to offering from a single provider at a time
- Unable to swap one provider for another
- No standard interface

Global Cloud Exchange

- Market directory
- Banking system
- Brokers
- Price setting mechanism
- Admission control mechanism
- Resource management system
- Consumers utility function
- Resource management proxy



Challenges

- Unwillingness to shift from traditional controlled environment
- Regulatory pressure
- How to obtain restitution in case of SLA violation

Security in cloud computing

Here are some of the most common cloud computing security risks

Distributed-Denial-of-Service Attacks

When cloud computing first became popular, Distributed Denial-of-Service (DDoS) attacks against cloud platforms were largely unthinkable; the sheer amount of resources cloud computing services had made DDoS attacks extremely difficult to initiate. But with as many Internet of Things devices, smartphones, and other computing systems as there are available now, DDoS attacks have greatly increased in viability. If enough traffic is initiated to a cloud computing system, it can either go down entirely or experience difficulties.

Shared Cloud Computing Services

Not all cloud hosting solutions and cloud computing services are made equal. Many cloud solutions do not provide the necessary security *between clients*, leading to shared resources, applications, and systems. In this situation, threats can originate from *other clients* with the cloud computing service, and threats targeting one client could also have an impact on other clients.

Employee Negligence

Employee negligence and employee mistakes remain one of the biggest security issues for *all* systems, but the threat is particularly dangerous with cloud solutions. Modern employees may log into cloud solutions from their mobile phones, home tablets, and home desktop PCs, potentially leaving the system vulnerable to many outside threats.

Data Loss and Inadequate Data Backups

Inadequate data backups and improper data syncing is what has made many businesses vulnerable to *ransomware*, a specific type of cloud security threat. Ransomware "locks" away a company's data in encrypted files, only allowing them to access the data once a ransom has been paid. With appropriate data backup solutions, companies need no longer fall prey to these threats.

Phishing and Social Engineering Attacks

Due to the openness of a cloud computing system, phishing and social engineering attacks have become particularly common. Once login information or other confidential information is acquired, a malicious user can potentially break into a system with ease -- as the system itself is available from anywhere. Employees must be knowledgeable about phishing and social engineering enough to avoid these types of attackS.

System Vulnerabilities

Cloud computing systems can still contain system vulnerabilities, especially in networks that have complex infrastructures and multiple third-party platforms. Once a vulnerability becomes known with a popular third-party system, this vulnerability can be easily used against organizations. Proper patching and upgrade protocols -- in addition to network monitoring solutions -- are critical for fighting this threat.

Data Breach

Data Breaches result from an attack or employee negligence and error. This is a primary cause for concern in cloud platforms. Vulnerabilities in the application or ineffective security practices can also cause data breaches. Employees may log into cloud systems from their phones or personal laptops thus exposing the system to targeted attacks.

Account Hijacking

With the increase in adoption of cloud services, organizations have reported an increased occurrence of account hijacking. Such attacks involve using employee's login information to access sensitive information. Attackers can also modify, insert false information and manipulate the data present in the cloud. They also use scripting bugs or reused passwords to steal credentials without being detected.

Account hijacking could have a detrimental effect at the enterprise level, undermining the firm's integrity and reputation. This could also have legal implications in industries such as healthcare where patients' personal medical records are compromised. A robust IAM (Identity Access Management) system can prevent unauthorized access and damage to the organization's data assets.

Insecure APIs and Interfaces

Customers can tailor their cloud computing experience according to their needs by using Application Programming Interface or APIs.

These are used to extract, manage and interact with information on the cloud. However, the unique characteristics of API leave the door wide open for threats. Hence the security of APIs affects the security and availability of cloud services and platforms.

APIs facilitate communication between applications, herein lies the vulnerability. Firms need to focus on designing APIs with adequate authentication, other access control methods, and encryption technology.

The most recent example of an insecure API was at Salesforce, where an API bug in its Marketing Cloud service exposed customer data. This caused data to be written from one customer account to another.

Insider Threat

An Insider threat is the misuse of information through hostile intent, malware, and even accidents. Insider threats originate from employees or system administrators, who can access confidential information they can also access even more critical systems and eventually data.

When the relationship between the employer and system administrator turn sour, they may resort to leaking privileged information.
There can be several instances of insider threat such as a Salesperson who jumps ship or a rogue admin. In scenarios where the cloud service provider is responsible for security, the risk from insider threat is often greater.
Insider threats can be circumvented through business partnerships, controlled access and prioritizing initiatives.

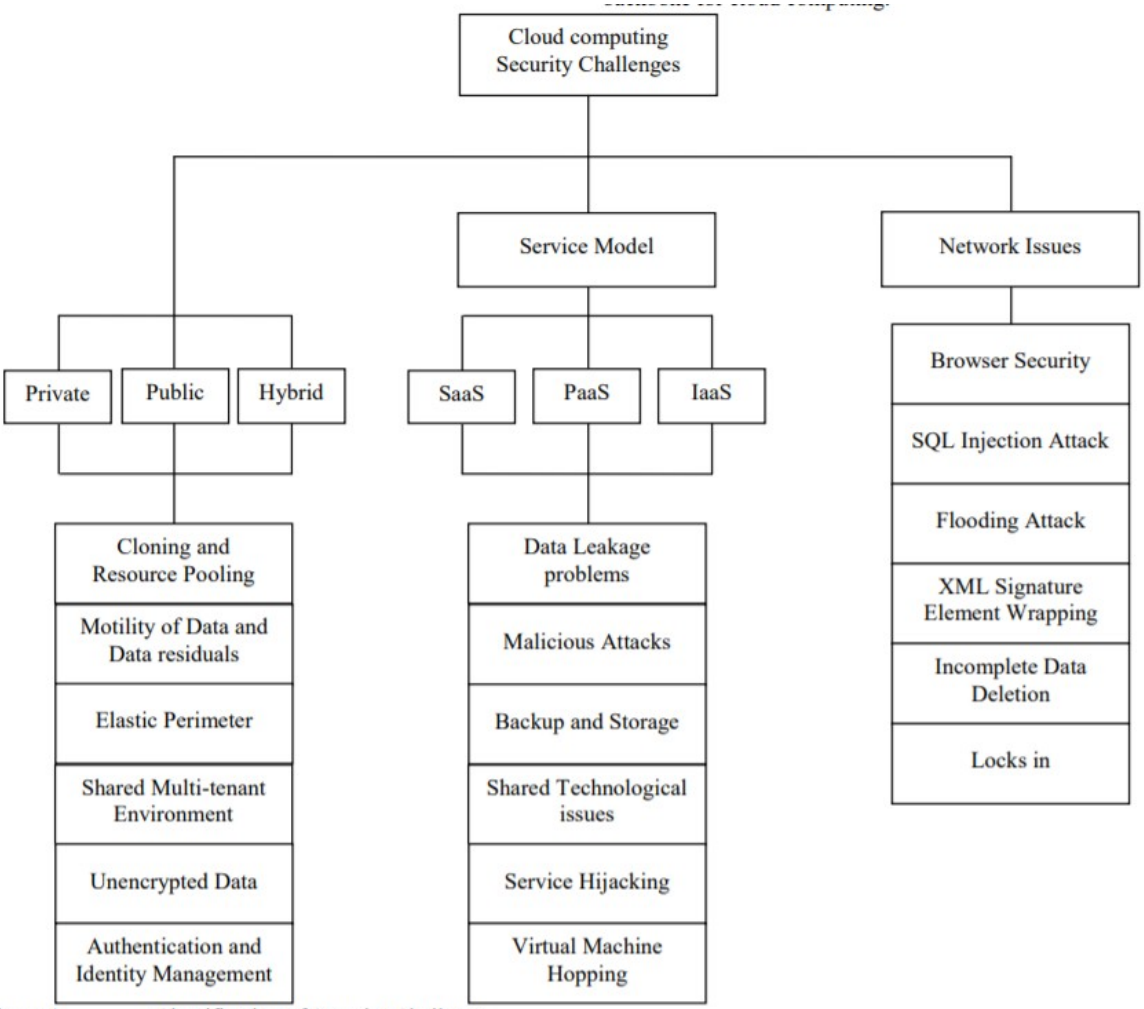


Figure 1: Classification of Security Challenge

Various security challenges related to these deployment models are discussed below:

• Cloning and Resource Pooling: Cloning deals with replicating or duplicating the data. According to cloning 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.
• 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.
• 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.
• Shared Multi-tenant Environment: 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.
• 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.
• 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.

Various security challenges with the service models are discussed below:

• 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.
• 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.
• 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.
• 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.
• 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.
• 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, Thomas Ristenpart et al. [15] have shown that 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. Additionally, multi-tenancy makes the impact of a VM hopping attack larger than in a conventional IT environment. Because quite a few VMs can run at the same time and on the same host there is a possibility of all of them becoming a victim VMs. VM hopping is thus a critical vulnerability for IaaS and PaaS infrastructures.

• 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. Several types of attacks might take advantage of weaknesses in VM mobility which includes man in-the-middle attacks. The severity of the attacks ranges from leaking perceptive information, to completely compromising the guest OS.

• 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

The network issues

The network structure of this cloud faces various attacks and security issues like cloud malware injection attack, browser security issues, flooding attacks, locks-in, incomplete data deletion, data protection and XML signature element wrapping, which are explained further below.

• 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.

• 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.

• 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.

• 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

• 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.

• 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.

CLOUD 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 helps answer leadership questions such as:

- Are our security investments yielding the desired returns?
- Do we know our security risks and their business impact?
- Are we progressively reducing security risks to acceptable levels?
- Have we established a security-conscious culture within the enterprise?

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.

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:

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

Lack of embedded management operational controls
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.

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.

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.

Virtual machine security

Security Risks in Virtualization

Cons

a. Scaling: it is easy to replicate a VM or creating a copy is very easy..
b. A single fatal event or a single system attacked with worm or malicious code can be replicated which can cause destruction to the virtual environment.
c. Transience: in a virtual environment large number of mobile machines comes and goes very frequently. Network with traditional machines were much more stable as it was easy to analyze the configuration of the existing network.
d. Diversity: in a virtual environment it is difficult to enforce homogeneity in the network. Some of the VM will be running with new updated patches, but some will be still running with the older version of OS. If one has to migrate their machine from one version to another, being a very diverse environment it would be difficult to migrate all the system from older version to newer version.
e. Mobility: it is easy to copy VMs and it can give rise to security threats.

Steps to ensure virtual machine security in cloud computing

Security is a problem. Network security is an even bigger problem because of the complex factors that define risks and the profound negative effects that can occur if you fail.

Virtual network security is the worst problem of all because it combines issues generated by traditional hosting and application security with those from network security, and then adds the challenges of virtual resources and services. In short, cloud-virtual service security issues occur because security tools designed to protect hosted software features are different than those safeguarding physical devices.

Following are some step that can ensure security virtual cloud management:-

1. Protect hosted elements by segregating them

Step one in securing virtual machine security in cloud computing is to *isolate the new hosted elements*. For example, let's say three features hosted inside an edge device could be deployed in the cloud either as part of the service data plane, with addresses visible to network users, or as part of a private sub network that's invisible. If you deploy in the cloud, then any of the features can be attacked, and

it's also possible your hosting and management processes will become visible and vulnerable. If you isolate your hosting and feature connections inside a private sub network, they're protected from outside access.

In container hosting today, both in the data center and in the cloud, application components deploy inside a private sub network. As a result, only the addresses representing APIs that users are supposed to access are exposed. That same principle needs to be applied to virtual functions; expose the interfaces that users actually connect to and hide the rest with protected addresses.

2. Ensure all components are tested and reviewed

Step two in cloud-virtual security is to *certify virtual features and functions for security compliance before you allow them to be deployed*. Outside attacks are a real risk in virtual networking, but an insider attack is a disaster. If a feature with a back-door security fault is introduced into a service, it becomes part of the service infrastructure and is far more likely to possess open attack vectors to other infrastructure elements.

Private subnetworks can help in addressing virtual machine security in cloud computing. If new components can only access other components in the same service instance, the risk is reduced that malware can be introduced in a new software-hosted feature. Yes, a back-door attack could put the service itself at risk, but it's less likely the malware will spread to other services and customers.

This approach, however, doesn't relieve operators of the burden of security testing. It's important to insist on a strong lifecycle management compliance process flow for all hosted features and functions -- one that operators can audit and validate. If the companies supplying your hosted features or functions properly test their new code, it's less likely it will contain accidental vulnerabilities or deliberately introduced back-door faults

3. Separate management APIs to protect the network

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

By containing access, you limit your security risk. Additionally, operators should require that access to infrastructure management and orchestration APIs by any source is chronicled, and that any access or change is reviewed to prevent a management access leak from occurring.

4. Keep connections secure and separate

The fourth and final point in cloud-virtual network security is to *ensure that virtual network connections don't cross over between tenants or services*. Virtual networking is a wonderful way of creating agile connections to redeployed or scaled features, but each time a virtual network change is made, it's possible it can establish an inadvertent connection between two different services, tenants or feature/function deployments. This can produce a data plane leak, a connection between the actual user networks or a management or control leak that could allow one user to influence the service of another

IAM(Identity and access management)

Identity and access management (IAM) in enterprise IT is about defining and managing the roles and access privileges of individual network users and the circumstances in which users are granted (or denied) those privileges. Those users might be customers (customer identity management) or employees (employee identity management. The core objective of IAM systems is one digital identity per individual. Once that digital identity has been established, it must be maintained, modified and monitored throughout each user's "access lifecycle."
Thus, the overarching goal of identity management is to "grant access to the right enterprise assets to the right users in the right context, from a user's system onboarding to permission authorizations to the offboarding of that user as needed in a timely fashion,"
IAM systems provide administrators with the tools and technologies to change a user's role, track user activities, create reports on those activities, and enforce policies on an ongoing basis. These systems are designed to provide a means of administering user access across an entire enterprise and to ensure compliance with corporate policies and government regulations.

BENEFITS OF IAM

1. Improving User Experiences

While this may seem the most obvious benefit, it deserves to be said: SSO eliminates the need for users to remember and input multiple passwords to access different areas of your system. Gone are the days of trying to keep dozens of password variations straight; with SSO, users can enjoy automatic logins every time they move to a different connected system.

All vendors offer a variety of user authentication schemes ranging from more strict multi-factor authentication to federated solutions that leverage existing user security profiles.

2. Enhancing Security Profiles

Just because SSO *can* grant users automatic access to all applications does not mean it *has* to. More advanced IAM systems, most commonly using Security Assertion Markup Language (SAML) 2.0 can use SSO with additional levels of security. IAM systems can authenticate and authorize users based on the access level indicated in their directory profiles. IAM system can also automaetically control user access using other factors. to specific functions of your system. For example, Okta allows you to create identity management policies restricting access to applications based on time of day, or adding additional authentication factors such as physical location. PingFederate can extend a user security profile integrating with existing identity stores, directories or other social identity providers. Additional rules can automate access decisions by identity attribute, group membership or authentication method.

3. Simplifies Auditing and Reporting

Consolidating user identities and passwords with SSO makes it easier for IT departments to audit where and how these user credentials are used. In the event that user credentials are compromised, IAM systems make it easier for IT departments to identify which user was compromised and which data was accessed during the breach. PingFederate allows you to monitor sign on performance metrics, traffic, and compliance centrally. Detailed audit trails allow systems to record user provisioning and de-provisioning as employees are on-boarded or teminated. OneLogin allows you to run detailed analytical reports on users, apps, logins other events.

4. Allows Easy Access No Matter Where You Are

IAM/SSO allows users to access to all interconnected systems, regardless of where the user is physically located. This can be especially useful for large companies doing business globally, providing ease of access to employees, parnters and clients alike. OneLogin offers apps that allow users to access any enterprise web-based application anywhere on any device. OneLogin Mobile identity management provides users one-click access to all enterprise apps on smartphones and tablets.

Some vendors offer suites of identity management solutions that require additional setup and configuration. Okta claims to provide the only truly comprehensive mobile solution to securely and efficiently enable new mobile initiatives, with enterprise mobility management completely integrated with its identity management solutions.

5. Increases Productivity and Reduces IT Costs

- The original benefit of SSO for IT departments was to eliminate the cost of internal help desks helping users locked out of their application accounts.
- IAM is purporting to do much more. By leveraging already existing identity stores such as Active Director or LDAP, IAM allows you to extend what you have into the future.
- Cloud-based and mobile-based IAM tools not only allow users to authenticate from anywhere anytime, they also provide the extensive audit trails, analytics, access rules and policies to truly automate identity access and management across the enterprise.

DISADVANTAGES OF IAM

Major cloud providers specifically design and optimize their IAM products for their own platforms. This might be fine for organizations that run all of their operations on that platform, but many IT teams also manage on-premises applications, multiple cloud services, hybrid environments, distributed data stores and customized legacy systems. In these situations, IT must either balance multiple IAM products or find a single product that supports multiple environments, such as tools from Ping Identity or RSA.

Primary concern with SSO systems is that it creates a single point of failure. One of the main disadvantages to SSO is decreased security, especially if it isn't implemented properly. For starters, there's a single sign-on, but there's no single logout. The logout process will vary across applications. Just because a user logs out of one application doesn't mean that the rest also shut down. In fact, user sessions stay active long after a user logs out of a single application. Because SSO only requires one set of credentials to access all of a user's resources, a hacker could quite easily utilize all of them. This is especially dangerous if that user has access to privileged information or mission-critical data.

CLOUD SECURITY STANDARDS

.1 Information Technology Infrastructure Library (ITIL)

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

Realization of security requirements: "Security requirements are usually defined in the SLA as well as in other external requirements, which are specified in underpinning contracts, legislation, and internally or externally imposed policies".

Realization of a basic level of security: "This is necessary to guarantee the security and continuity of the organization and to reach simplified service-level management for information security management".

Information security practices are divided into four different levels. :

1. **Policies:** The major objective an organization is trying to achieve.
2. **Processes:** What steps to follow to achieve those objectives?
3. **Procedures:** Distribution of activities amongst people and setting up deadlines.
4. **Work instructions:** Specifying guidelines to perform certain activities.

The major challenge for organizations that fail to adopt ITIL efficiently is that they might have to re-define or re-implement the entire set of ITIL processes that they have. Thus, for implementing ITIL a detailed analysis of existing processes along with gaps in relation to the ITIL framework and level of process integration would be needed.

.2 Open Virtualization Format (OVF)

Open Virtualization Format (OVF) is a standard pertaining to portability concern described in section 3.3. OVF provides the ability for an efficient, flexible and secure distribution of enterprise software over the cloud. OVF thus provides customers: vendor and platform

independence as it facilitates mobility of virtual machines [OVF2]. Across the cloud OVF plays a major role in providing cross-platform portability. It also helps provide simplified deployment over multiple platforms. OVF 2.0 was released in January 2013 [OVF2].

An OVF format virtual machine can be deployed easily by customers. They can do so on the platform of their choice. It helps enhance customer experience as it provides customers with portability, platform independence, verification, signing, versioning, and licensing terms [OVF2].

The key features and benefits of the format are:

- Portable VM packaging
- Optimization for secure distribution
- Simplified Installation and Deployment
- Supports both VM and multi-VM configurations
- Vendor and platform independent
- Extensible
- Localizable

.3 ITU-T X.1601

The ITU standard presents a sketch of issues pertaining to cloud computing and proposes a framework for cloud security. It talks in detail about various security challenges and ways to reduce these security risks in cloud computing. It also discusses a framework that provides an insight into what security capabilities are required for making the cloud secure and facing security challenges. ITU-T X.1601 starts by listing down major security threats that the cloud can encounter. As we have already discussed major security threats for cloud computing in section 2, in this section we will discuss the cloud security challenges and the security capabilities that this standard deals with and those help in mitigating the relevant threats.

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

1. **Cloud Service Provider (CSP):** An individual or an organization responsible for making cloud services available.
2. **Cloud Service Customer (CSC):** An individual or an organization that uses cloud services.
3. **Cloud Service Partner (CSN):** A partner that helps support the CSPs or the CSCs.

.4 PCI DSS

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

Though the responsibility for managing security is shared between client and provider the client still has an important role to play. The client holds the responsibility of ensuring their cardholder

data is secure under PCI DSS requirements. The division of responsibilities between the client and the CSP for managing PCI DSS controls is influenced by multiple factors, which are :

- The client uses the cloud service for what purpose.
- What scope of PCI DSS requirements is the client outsourcing to the CSP.
- The CSP validates which service and system components within its own operations.
- The service option that the client has selected to engage the CSP (IaaS, PaaS or SaaS).
- The scope of any additional services the CSP is providing to pro-actively manage the client's compliance (for example, additional managed security services).

The client must have a clear understanding of the scope of responsibility that the CSP is accepting for each PCI DSS requirement.

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

This standard is yet to be launched in the market. It aims to provide further guidance in the information security domain of cloud computing. It is aimed at supplementing the guidance in ISO/IEC 27002 and various other ISO27k standards including ISO/IEC 27018 on the privacy aspects of cloud computing, ISO/IEC 27031 on business continuity, and ISO/IEC 27036-4 on relationship management, as well as all the other ISO27k standards [ISO27017].

The scope and purpose is listed below:

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

Unit 4

Virtual machine security

Security Risks in Virtualization

Cons

a. Scaling: it is easy to replicate a VM or creating a copy is very easy..
b. A single fatal event or a single system attacked with worm or malicious code can be replicated which can cause destruction to the virtual environment.
c. Transience: in a virtual environment large number of mobile machines comes and goes very frequently. Network with traditional machines were much more stable as it was easy to analyze the configuration of the existing network.
d. Diversity: in a virtual environment it is difficult to enforce homogeneity in the network. Some of the VM will be running with new updated patches, but some will be still running with the older version of OS. If one has to migrate their machine from one version to another, being a very diverse environment it would be difficult to migrate all the system from older version to newer version.
e. Mobility: it is easy to copy VMs and it can give rise to security threats.

Steps to ensure virtual machine security in cloud computing

Security is a problem. Network security is an even bigger problem because of the complex factors that define risks and the profound negative effects that can occur if you fail.

Virtual network security is the worst problem of all because it combines issues generated by traditional hosting and application security with those from network security, and then adds the challenges of virtual resources and services. In short, cloud-virtual service security issues occur because security tools designed to protect hosted software features are different than those safeguarding physical devices.

Following are some step that can ensure security virtual cloud management:-

1. Protect hosted elements by segregating them

Step one in securing virtual machine security in cloud computing is to *isolate the new hosted elements*. For example, let's say three features hosted inside an edge device could be deployed in the cloud either as part of the service data plane, with addresses visible to network users, or as part of a private sub network that's invisible. If you deploy in the cloud, then any of the features can be attacked, and it's also possible your hosting and management processes will become visible and vulnerable. If you isolate your hosting and feature connections inside a private sub network, they're protected from outside access.

In container hosting today, both in the data center and in the cloud, application components deploy inside a private sub network. As a result, only the addresses representing APIs that users are supposed to access are exposed. That same principle needs to be applied to virtual functions; expose the interfaces that users actually connect to and hide the rest with protected addresses.

2. Ensure all components are tested and reviewed

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

attack is a disaster. If a feature with a back-door security fault is introduced into a service, it becomes part of the service infrastructure and is far more likely to possess open attack vectors to other infrastructure elements.

Private subnetworks can help in addressing virtual machine security in cloud computing. If new components can only access other components in the same service instance, the risk is reduced that malware can be introduced in a new software-hosted feature. Yes, a back-door attack could put the service itself at risk, but it's less likely the malware will spread to other services and customers.

This approach, however, doesn't relieve operators of the burden of security testing. It's important to insist on a strong lifecycle management compliance process flow for all hosted features and functions -- one that operators can audit and validate. If the companies supplying your hosted features or functions properly test their new code, it's less likely it will contain accidental vulnerabilities or deliberately introduced back-door faults

3. Separate management APIs to protect the network

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

By containing access, you limit your security risk. Additionally, operators should require that access to infrastructure management and orchestration APIs by any source is chronicled, and that any access or change is reviewed to prevent a management access leak from occurring.

4. Keep connections secure and separate

The fourth and final point in cloud-virtual network security is to *ensure that virtual network connections don't cross over between tenants or services*. Virtual networking is a wonderful way of creating agile connections to redeployed or scaled features, but each time a virtual network change is made, it's possible it can establish an inadvertent connection between two different services, tenants or feature/function deployments. This can produce a data plane leak, a connection between the actual user networks or a management or control leak that could allow one user to influence the service of another

IAM(Identity and access management)

Identity and access management (IAM) in enterprise IT is about defining and managing the roles and access privileges of individual network users and the circumstances in which users are granted (or denied) those privileges. Those users might be customers (customer identity management) or employees (employee identity management. The core objective of IAM systems is one digital identity per individual. Once that digital identity has been established, it must be maintained, modified and monitored throughout each user's "access lifecycle."
Thus, the overarching goal of identity management is to "grant access to the right enterprise assets to the right users in the right context, from a user's system onboarding to permission authorizations to the offboarding of that user as needed in a timely fashion,"
IAM systems provide administrators with the tools and technologies to change a user's role, track user activities, create reports on those activities, and enforce policies on an ongoing basis. These systems are designed to provide a means of administering user access across an entire enterprise and to ensure compliance with corporate policies and government regulations.

BENEFITS OF IAM

1. Improving User Experiences

While this may seem the most obvious benefit, it deserves to be said: SSO eliminates the need for users to remember and input multiple passwords to access different areas of your system. Gone are the days of trying to keep dozens of password variations straight; with SSO, users can enjoy automatic logins every time they move to a different connected system.

All vendors offer a variety of user authentication schemes ranging from more strict multi-factor authentication to federated solutions that leverage existing user security profiles.

2. Enhancing Security Profiles

Just because SSO *can* grant users automatic access to all applications does not mean it *has* to. More advanced IAM systems, most commonly using Security Assertion Markup Language (SAML) 2.0 can use SSO with additional levels of security. IAM systems can authenticate and authorize users based on the access level indicated in their directory profiles. IAM system can also automaetically control user access using other factors. to specific functions of your system. For example, Okta allows you to create identity management policies restricting access to applications based on time of day, or adding additional authentication factors such as physical location. PingFederate can extend a user security profile integrating with existing identity stores, directories or other social identity providers. Additional rules can automate access decisions by identity attribute, group membership or authentication method.

3. Simplifies Auditing and Reporting

Consolidating user identities and passwords with SSO makes it easier for IT departments to audit where and how these user credentials are used. In the event that user credentials are compromised, IAM systems make it easier for IT departments to identify which user was compromised and which data was accessed during the breach. PingFederate allows you to monitor sign on performance metrics, traffic, and compliance centrally. Detailed audit trails allow systems to record user provisioning and de-provisioning as employees are on-boarded or teminated. OneLogin allows you to run detailed analytical reports on users, apps, logins other events.

4. Allows Easy Access No Matter Where You Are

IAM/SSO allows users to access to all interconnected systems, regardless of where the user is physically located. This can be especially useful for large companies doing business globally, providing ease of access to employees, parnters and clients alike. OneLogin offers apps that allow users to access any enterprise web-based application anywhere on any device. OneLogin Mobile identity management provides users one-click access to all enterprise apps on smartphones and tablets.

Some vendors offer suites of identity management solutions that require additional setup and configuration. Okta claims to provide the only truly comprehensive mobile solution to securely and efficiently enable new mobile initiatives, with enterprise mobility management completely integrated with its identity management solutions.

5. Increases Productivity and Reduces IT Costs

- The original benefit of SSO for IT departments was to eliminate the cost of internal help desks helping users locked out of their application accounts.
- IAM is purporting to do much more. By leveraging already existing identity stores such as Active Director or LDAP, IAM allows you to extend what you have into the future.
- Cloud-based and mobile-based IAM tools not only allow users to authenticate from anywhere anytime, they also provide the extensive audit trails, analytics, access rules and policies to truly automate identity access and management across the enterprise.

DISADVANTAGES OF IAM

Major cloud providers specifically design and optimize their IAM products for their own platforms. This might be fine for organizations that run all of their operations on that platform, but many IT teams also manage on-premises applications, multiple cloud services, hybrid environments, distributed data stores and customized legacy systems. In these situations, IT must either balance multiple IAM products or find a single product that supports multiple environments, such as tools from Ping Identity or RSA.

Primary concern with SSO systems is that it creates a single point of failure. One of the main disadvantages to SSO is decreased security, especially if it isn't implemented properly. For starters, there's a single sign-on, but there's no single logout. The logout process will vary across applications. Just because a user logs out of one application doesn't mean that the rest also shut down. In fact, user sessions stay active long after a user logs out of a single application. Because SSO only requires one set of credentials to access all of a user's resources, a hacker could quite easily utilize all of them. This is especially dangerous if that user has access to privileged information or mission-critical data.

CLOUD SECURITY STANDARDS

.1 Information Technology Infrastructure Library (ITIL)

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

Realization of security requirements: "Security requirements are usually defined in the SLA as well as in other external requirements, which are specified in underpinning contracts, legislation, and internally or externally imposed policies".

Realization of a basic level of security: "This is necessary to guarantee the security and continuity of the organization and to reach simplified service-level management for information security management".

Information security practices are divided into four different levels. :

1. **Policies:** The major objective an organization is trying to achieve.
2. **Processes:** What steps to follow to achieve those objectives?
3. **Procedures:** Distribution of activities amongst people and setting up deadlines.
4. **Work instructions:** Specifying guidelines to perform certain activities.

The major challenge for organizations that fail to adopt ITIL efficiently is that they might have to re-define or re-implement the entire set of ITIL processes that they have. Thus, for implementing ITIL a detailed analysis of existing processes along with gaps in relation to the ITIL framework and level of process integration would be needed.

.2 Open Virtualization Format (OVF)

Open Virtualization Format (OVF) is a standard pertaining to portability concern described in section 3.3. OVF provides the ability for an efficient, flexible and secure distribution of enterprise software over the cloud. OVF thus provides customers: vendor and platform independence as it facilitates mobility of virtual machines [OVF2]. Across the cloud OVF plays a major role in providing cross-platform portability. It also helps provide simplified deployment over multiple platforms. OVF 2.0 was released in January 2013 [OVF2].

An OVF format virtual machine can be deployed easily by customers. They can do so on the platform of their choice. It helps enhance customer experience as it provides customers with portability, platform independence, verification, signing, versioning, and licensing terms [OVF2].

The key features and benefits of the format are:

- Portable VM packaging
- Optimization for secure distribution
- Simplified Installation and Deployment
- Supports both VM and multi-VM configurations
- Vendor and platform independent
- Extensible
- Localizable

.3 ITU-T X.1601

The ITU standard presents a sketch of issues pertaining to cloud computing and proposes a framework for cloud security. It talks in detail about various security challenges and ways to reduce these security risks in cloud computing. It also discusses a framework that provides an insight into what security capabilities are required for making the cloud secure and facing security challenges. ITU-T X.1601 starts by listing down major security threats that the cloud can encounter. As we have already discussed major security threats for cloud computing in section 2, in this section we will discuss the cloud security challenges and the security capabilities that this standard deals with and those help in mitigating the relevant threats.

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

1. **Cloud Service Provider (CSP):** An individual or an organization responsible for making cloud services available.
2. **Cloud Service Customer (CSC):** An individual or an organization that uses cloud services.
3. **Cloud Service Partner (CSN):** A partner that helps support the CSPs or the CSCs.

.4 PCI DSS

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

Though the responsibility for managing security is shared between client and provider the client still has an important role to play. The client holds the responsibility of ensuring their cardholder data is secure under PCI DSS requirements. The division of responsibilities between the client and the CSP for managing PCI DSS controls is influenced by multiple factors, which are :

- The client uses the cloud service for what purpose.
- What scope of PCI DSS requirements is the client outsourcing to the CSP.
- The CSP validates which service and system components within its own operations.
- The service option that the client has selected to engage the CSP (IaaS, PaaS or SaaS).
- The scope of any additional services the CSP is providing to pro-actively manage the client's compliance (for example, additional managed security services).

The client must have a clear understanding of the scope of responsibility that the CSP is accepting for each PCI DSS requirement.

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

This standard is yet to be launched in the market. It aims to provide further guidance in the information security domain of cloud computing. It is aimed at supplementing the guidance in ISO/IEC 27002 and various other ISO27k standards including ISO/IEC 27018 on the privacy aspects of cloud computing, ISO/IEC 27031 on business continuity, and ISO/IEC 27036-4 on relationship management, as well as all the other ISO27k standards [ISO27017].

The scope and purpose is listed below:

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