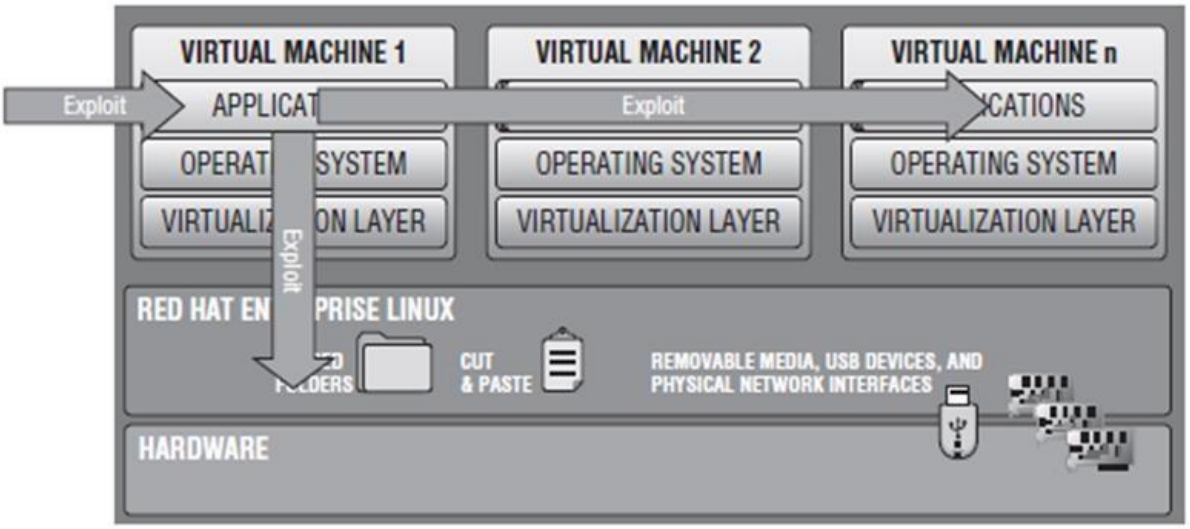
UNIT V CLOUD SECURITY

Virtualization System-Specific Attacks: Guest hopping – VM migration attack – hyperjacking. Data Security and Storage; Identity and Access Management (IAM) - IAM Challenges - IAM Architecture and Practice.

Virtualization System-Specific Attacks

Introduction: Virtual Threats

- Some threats to virtualized systems are general in nature, as they are inherent threats to all computerized systems (such as denial-of-service, or DoS, attacks).
- Many VM vulnerabilities stem from the fact that a vulnerability in one VM system can be exploited to attack other VM systems or the host systems, as multiple virtual machines share the same physical hardware, as shown in Figure



Shared clipboard — Shared clipboard technology allows data to be transferred

between VMs and the host, providing a means of moving data between malicious programs in VMs of different security realms.

Keystroke logging — Some VM technologies enable the logging of keystrokes and screen updates to be passed across virtual terminals in the virtual machine, writing to host fi les and permitting the monitoring of encrypted terminal connections inside the VM

VM monitoring from the host — Because all network packets coming from or going to a VM pass through the host, the host may be able to affect the VM by the following:

- Starting, stopping, pausing, and restart VMs

- Monitoring and configuring resources available to the VMs, including CPU, memory, disk, and network usage of VMs
- Adjusting the number of CPUs, amount of memory, amount and number of virtual disks, and number of virtual network interfaces available to a VM
- Monitoring the applications running inside the VM
- Viewing, copying, and modifying data stored on the VM's virtual disks Virtual machine monitoring from another VM — Usually, VMs should not be able to directly access one another's virtual disks on the host.
- However, if the VM platform uses a virtual hub or switch to connect the VMs to the host, then intruders may be able to use a hacker technique known as "ARP poisoning" to redirect packets going to or from the other VM for sniffing.
- Virtual machine backdoors — A backdoor, covert communications channel between the guest and host could allow intruders to perform potentially dangerous operations.

Introduction : Virtual Threats- VM THREAT LEVELS

When categorizing the threat posed to virtualized environments, often the vulnerability/threat matrix is classified into three levels of compromise:

- **Abnormally terminated** — Availability to the virtual machine is compromised, as the VM is placed into an infinite loop that prevents the VM administrator from accessing the VM's monitor.
- **Partially compromised** — The virtual machine allows a hostile process to interfere with the virtualization manager, contaminating state checkpoints or over-allocating resources.
- **Totally compromised** — The virtual machine is completely overtaken and directed to execute unauthorized commands on its host with elevated privileges.

New Virtualization System-Specific Attacks

Hypervisor Risks

- The *hypervisor* is the part of a virtual machine that allows host resource sharing and enables VM/host isolation.
- Therefore, the ability of the hypervisor to provide the necessary isolation during intentional attack greatly determines how well the virtual machine can survive risk.

- One reason why the hypervisor is susceptible to risk is because it's a software program; risk increases as the volume and complexity of application code increases.
- Ideally, software code operating within a defined VM would not be able to communicate or affect code running either on the physical host itself or within a different VM; but several issues, such as bugs in the software, or limitations to the virtualization implementation, may put this isolation at risk.
- Major vulnerabilities inherent in the hypervisor consist of rogue hypervisor rootkits, external modification to the hypervisor, and VM escape.

Rogue Hypervisors Rootkits or Hyper jacking:

- ❑ In a normal virtualization scenario, the guest operating system (the operating system that is booted inside of a virtualized environment) runs like a traditional OS managing I/O to hardware and network traffic, even though it's controlled by the hypervisor.
- ❑ VM-based rootkits can hide from normal malware detection systems by initiating a "rogue" hypervisor and creating a cover channel to dump unauthorized code into the system.
- ❑ Proof-of-concept (PoC) exploits have demonstrated that a hypervisor rootkit can insert itself into RAM, downgrade the host OS to a VM, and make itself invisible.
- ❑ A properly designed rootkit could then stay "undetectable" to the host OS, resisting attempts by malware detectors to discover and remove it.
- ❑ This creates a serious vulnerability in all virtualized systems.
- ❑ Detectability of malware code lies at the heart of intrusion detection and correction, as security researchers analyze code samples by running the code and viewing the result.
- ❑ In addition, some malware tries to avoid detection by anti-virus processes by attempting to identify whether the system it has infected is traditional or virtual.
- ❑ If found to be a VM, it remains inactivated and hidden until it can penetrate the physical host and execute its payload through a traditional attack vector.

Consists of installing a rogue hypervisor

- Hyperjacking is an attack in which a hacker takes malicious control over the hypervisor that creates the virtual environment within a virtual machine (VM) host.

- The point of the attack is to target the operating system that is below that of the virtual machines so that the attacker's program can run and the applications on the VMs above it will be completely oblivious to its presence.
- Hyperjacking involves installing a malicious, fake hypervisor that can manage the entire server system.
- In hyperjacking, the hypervisor specifically operates in stealth mode and runs beneath the machine, it makes more difficult to detect and more likely gain access to computer servers where it can affect the operation of the entire institution or company.

Consists of installing a rogue hypervisor:

1. Injecting a rogue hypervisor beneath the original hypervisor;

2. Directly obtaining control of the original hypervisor;

3. Running a rogue hypervisor on top of an existing hypervisor.

One method for doing this is overwriting pagefiles on disk that contain paged-out kernel code

- Force kernel to be paged out by allocating large amounts of memory
- Find unused driver in page file and replace its dispatch function with shellcode
- Take action to cause driver to be executed
- Shellcode downloads the rest of the malware
- Host OS is migrated to run in a virtual machine
  –Has been demonstrated for taking control of Host OS
  –Hyperjacking of hypervisors may be possible, but not yet demonstrated
- Hypervisors will come under intense scrutiny because they are such attractive targets Known hyperjacking tools: BluePill, SubVirt, Vitriol

CASE STUDY

Virtualization System Public

Exploits CVE-2015-3456: VENOM

vulnerability

- The Floppy Disk Controller (FDC) in QEMU, as used in Xen 4.5.x and earlier and KVM, allows local guest users to cause a denial of service (out-of-bounds write and guest crash) or possibly execute arbitrary code via the (1) FD_CMD_READ_ID, (2) FD_CMD_DRIVE_SPECIFICATION_COMMAND, or other unspecified commands
- VENOM refers to a security vulnerability that results from a buffer overflow in a kernel-level driver included in many default virtualized environments.

- The VENOM vulnerability has the potential to provide attackers with access to the host operating system and, as a result, other guest operating systems on the same host.
- VENOM, an acronym for Virtualized Environment Neglected Operations Manipulation, arises from QEMU's virtual Floppy Disk Controller (FDC), which carries a vulnerability that could enable an attacker to run code by pairing one of two flawed commands related to the controller with a buffer overflow.
- The VENOM vulnerability affects KVM, Xen and native QEMU virtual machines.
- Virtual machines running on Microsoft Hyper-V or VMware hypervisors are not affected by VENOM.
- The VENOM vulnerability works with the default configuration of the affected virtualization platforms, so even when the FDC drive has not been added to the platform, systems are still vulnerable.

External Modification of the Hypervisor:

- ❑ In additional to the execution of the rootkit payload, a poorly protected or designed hypervisor can also create an attack vector.
- ❑ Therefore, a self-protected virtual machine may allow direct modification of its hypervisor by an external intruder.
- ❑ This can occur in virtualized systems that don't validate the hypervisor as a regular process.

Case Study: Virtualization System Public Exploits

- 36 public exploits against production virtualization systems have been released
- Most of these are attacks against third-party components of these systems
- CVE-2009-2267

–Guest OS user can gain elevated privileges on guest OS by exploiting a bug in handling of page faults

–Affects ESX server 4 and other VMware products

–Exploit binary posted at lists.grok.org.uk

VM migration

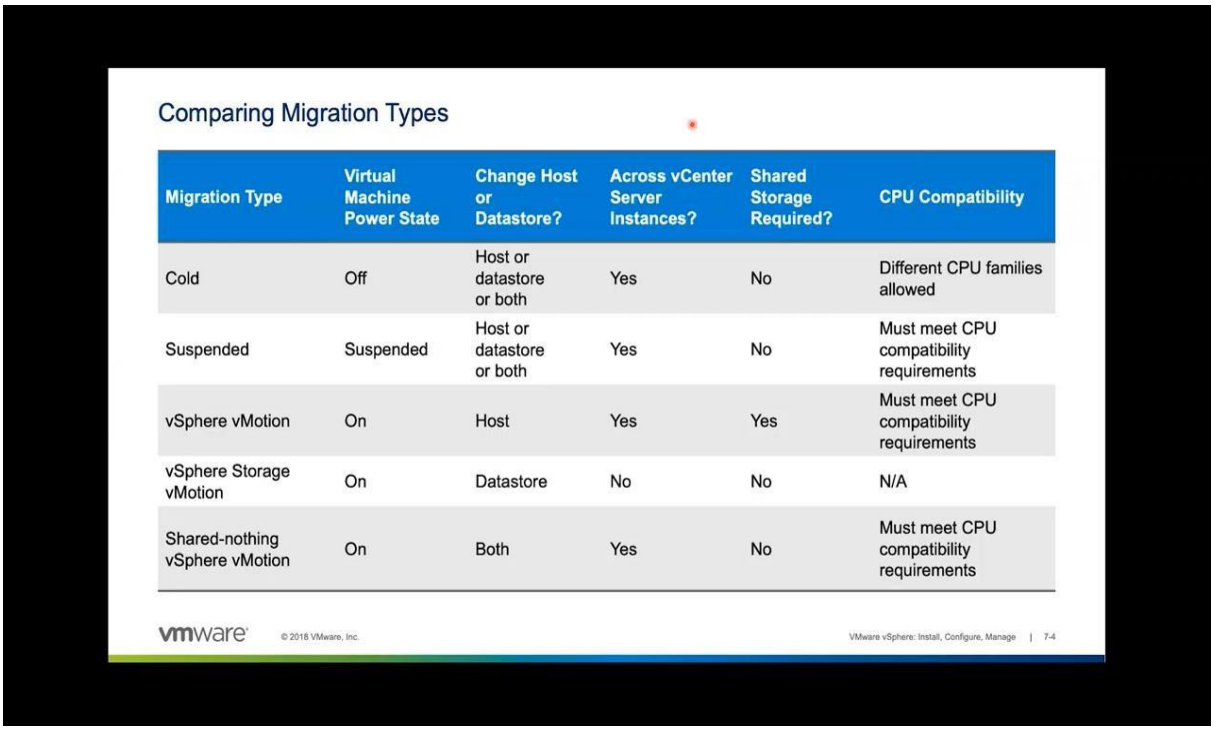
- Migration attack is an attack on the network during VM migration from one place to another. This attack is an exploit on the mobility of virtualization.
- Since VM images are easily moved between physical machines through the network, enterprises constantly move VMs to various places based on their usage.
- For example, VMs from a canceled customer may be moved to a backup data center, and VMs that need maintenance may be moved to a testing data center for changes.
- Thus, when VMs are on the network between secured perimeters, attackers can exploit the network vulnerability to gain unauthorized access to VMs.
- Similarly, the attackers can plant malicious code in the VM images to plant attacks on data centers that VMs travel between.

Migrating Virtual Machines

Migration means moving a virtual machine from one host, datastore, or vCenter Server system to another host, datastore, or vCenter Server system.

Types of migrations:

- Cold: Migrate a powered-off virtual machine to a new host or datastore.
- Suspended: Migrate a suspended virtual machine to a new host or datastore.
- vSphere vMotion: Migrate a powered-on virtual machine to a new host.
- vSphere Storage vMotion: Migrate a powered-on virtual machine's files to a new datastore.
- Shared-nothing vSphere vMotion: Migrate a powered-on virtual machine to a new host and a new datastore simultaneously.



Comparing Migration Types

Migration Type	Virtual Machine Power State	Change Host or Datastore?	Across vCenter Server Instances?	Shared Storage Required?	CPU Compatibility
Cold	Off	Host or datastore or both	Yes	No	Different CPU families allowed
Suspended	Suspended	Host or datastore or both	Yes	No	Must meet CPU compatibility requirements
vSphere vMotion	On	Host	Yes	Yes	Must meet CPU compatibility requirements
vSphere Storage vMotion	On	Datastore	No	No	N/A
Shared-nothing vSphere vMotion	On	Both	Yes	No	Must meet CPU compatibility requirements

VM migration-Types and Techniques

Cold Migration	Before migration, the virtual machine must be powered off, after doing this task. The old one should be deleted from source host. Moreover, the virtual machine need not to be on shared storage.
Warm Migration	Whenever transfer OS and any application, there is no need to suspend the source host. Basically it has high demand in public cloud.
Live Migration	It is the process of moving a running virtual machine without stopping the OS and other applications from source host to destination host.

1) Pre- Copy Migration:

In this migration, the hypervisor copies all memory page from source machine to destination machine while the virtual machine is running. It has two phases: Warm- up Phase and stop and copy phase.

a) Warm Up Phase:

During copying all memory pages from source to destination, some memory pages changed because of source machine CPU is active. All the changed memory pages are known as dirty pages.

All these dirty pages are required to recopy on destination machine; this phase is called as warm up phase.

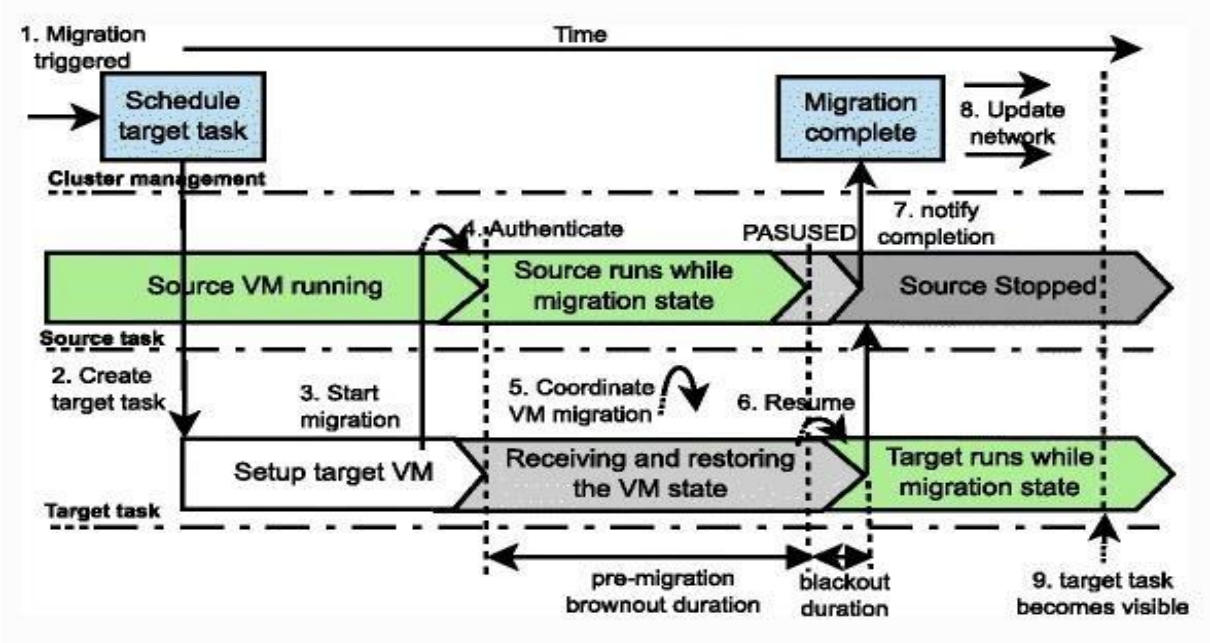
b) Stop & Copy Phase: Warm up phase is repeated until all the dirty pages recopied on destination machine. This time CPU of source machine is deactivated till all memory pages will transfer another machine. Ultimately at this time CPU of both source and destination is suspended, this is known as down time phase. This is the main thing that has to explore in migration for its optimization.

2) Post- Copy Migration*:*

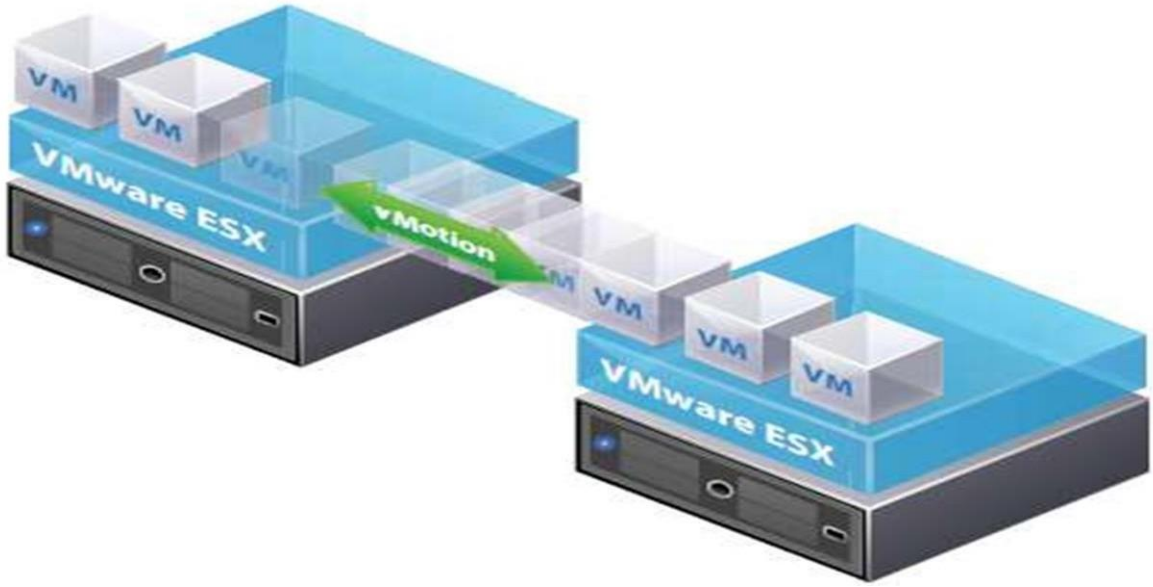
- In this technique, VM at the source is suspended to start post copy VM migration.
- When VM is suspended, execution state of the VM (i.e. CPU state, registers, non-pageable memory) is transferred to the target.
- In parallel the sources actively send the remaining memory pages of the VM to the target.
- This process is known as pre-paging.
- At the target, if the VM tries to access a page that has not been transferred yet, it generates a page fault, also known as network faults. These faults are redirect to the source, which responds with the faulted pages.
- Due to this, the performance of applications is degrading with number of network faults.

To overcome this, pre-paging scheme is used to push pages after the last fault by dynamically using page transmission order.

Live VM migration steps of Google Compute Engine

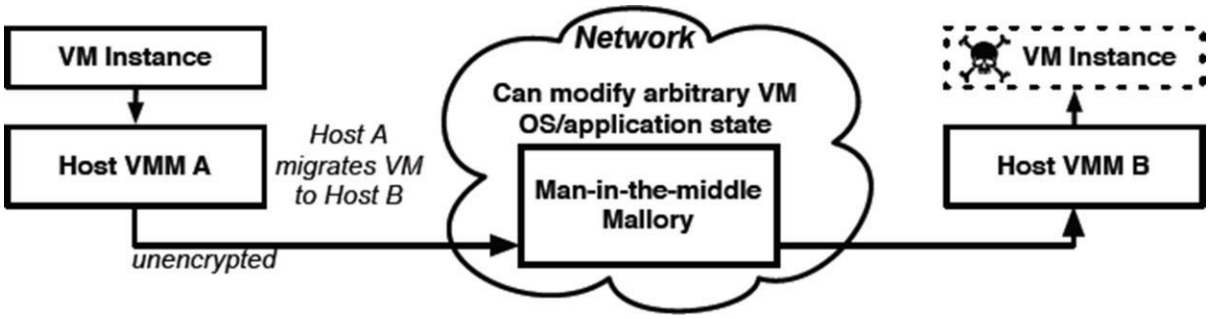


- **VM migration**
  - VM migration is transfer of guest OS from one physical server to another with little or no downtime
  - Implemented by several virtualization products
  - Provides high availability and dynamic load balancing



- **VM migration attack**
  - If migration protocol is unencrypted, susceptible to man-in-the-middle attack

- Allows arbitrary state in VM to be modified
- In default configuration, XenMotion is susceptible (no encryption)
- VMware's VMotion system supports encryption
- Proof-of-concept developed by John Oberheide at the Univ. of Michigan



Analysis of Hyper jacking Attack and Mitigation Techniques

Table 2.3 Analysis of hyper-jacking attack and mitigation technique

Attack mechanism	Mitigation technique
DoS Attack	Disable IP broadcast Disable unused services Deploy firewall rules Deploy IDS policy and rules Apply security patches on host
Live VM migration	Encryption of data by the hypervisor Use IPsec tunnel Source virtual machine monitor level virtual firewall Destination virtual machine monitor level virtual firewall
Hyper-jacking	Separate traffic from usual traffic Restrict the access Regular patches
VM escape	Should be provided access based on role Host should run only the required resource-sharing functionalities/services Guest OS should run less number of application to avoid any pen test
VM sprawl	Restrict the access Should be provided access based on role Should be made periodic verification Properly turn off identified idle VM
Guest OS vulnerabilities	Periodically perform the patching process Adopt firewall applications and traffic Really needed applications should be installed
Hyper-wall	Combination of another model for more security Confidentiality and integrity protection Multi-facilitated functions compared with others

Data Security and Storage

Cloud data security refers to the technologies, policies, services and security controls that protect any type of data in the cloud from loss, leakage or misuse through breaches, exfiltration and unauthorized access. A robust cloud data security strategy should include:

- Ensuring the security and privacy of data across networks as well as within applications, containers, workloads and other cloud environments
- Controlling data access for all users, devices and software
- Providing complete visibility into all data on the network

The cloud data protection and security strategy must also protect data of all types. This includes:

- **Data in use:** Securing data being used by an application or endpoint through user authentication and access control
- **Data in motion:** Ensuring the safe transmission of sensitive, confidential or proprietary data while it moves across the network through encryption and/or other email and messaging security measures
- **Data at rest:** Protecting data that is being stored on any network location, including the cloud, through access restrictions and user authentication

Data Security Mitigation

- Customers of cloud computing services expect that data security will serve as compensating controls for possibly weakened infrastructure security, since part of a customer's infrastructure security moves beyond its control and a provider's infrastructure security may (for many enterprises) or may not (for small to medium-size businesses, or SMBs) be less robust than expectations, you will be disappointed. Although data-in-transit can and should be encrypted, any use of that data in the cloud, beyond simple storage, requires that it be decrypted.
- Therefore, it is almost certain that in the cloud, data will be unencrypted. And if you are using a PaaS-based application or SaaS, customer-unencrypted data will also almost certainly be hosted in a multitenancy environment (in public clouds). Add to that exposure the difficulties in determining the data's lineage, data provenance—where necessary—and even many providers' failure to adequately address such a basic security concern as data remanence, and the risks of data security for customers are significantly increased.

- So, what should you do to mitigate these risks to data security? The only viable option for mitigation is to ensure that any sensitive or regulated data is not placed into a public cloud (or that you encrypt data placed into the cloud for simple storage only). Given the economic considerations of cloud computing today, as well as the present limits of cryptography, CSPs are not offering robust enough controls around data security.
- It may be that those economics change and that providers offer their current services, as well as a "regulatory cloud environment" (i.e., an environment where customers are willing to pay more for enhanced security controls to properly handle sensitive and regulated data). Currently, the only viable option for mitigation is to ensure that any sensitive or regulated data is not put into a public cloud.

Provider Data and Its Security

- In addition to the security of your own customer data, customers should also be concerned about what data the provider collects and how the CSP protects that data. Specifically with regard to your customer data, what metadata does the provider have about your data, how is it secured, and what access do you, the customer, have to that metadata? As your volume of data with a particular provider increases, so does the value of that metadata.
- Additionally, your provider collects and must protect a huge amount of security-related data. For example, at the network level, your provider should be collecting, monitoring, and protecting firewall, intrusion prevention system (IPS), security incident and event management (SIEM), and router flow data. At the host level your provider should be collecting system logfiles, and at the application level SaaS providers should be collecting application log data, including authentication and authorization information.
- What data your CSP collects and how it monitors and protects that data is important to the provider for its own audit purposes (e.g., SAS 70, as discussed in Chapter 8). Additionally, this information is important to both providers and customers in case it is needed for incident response and any digital forensics required for incident analysis.

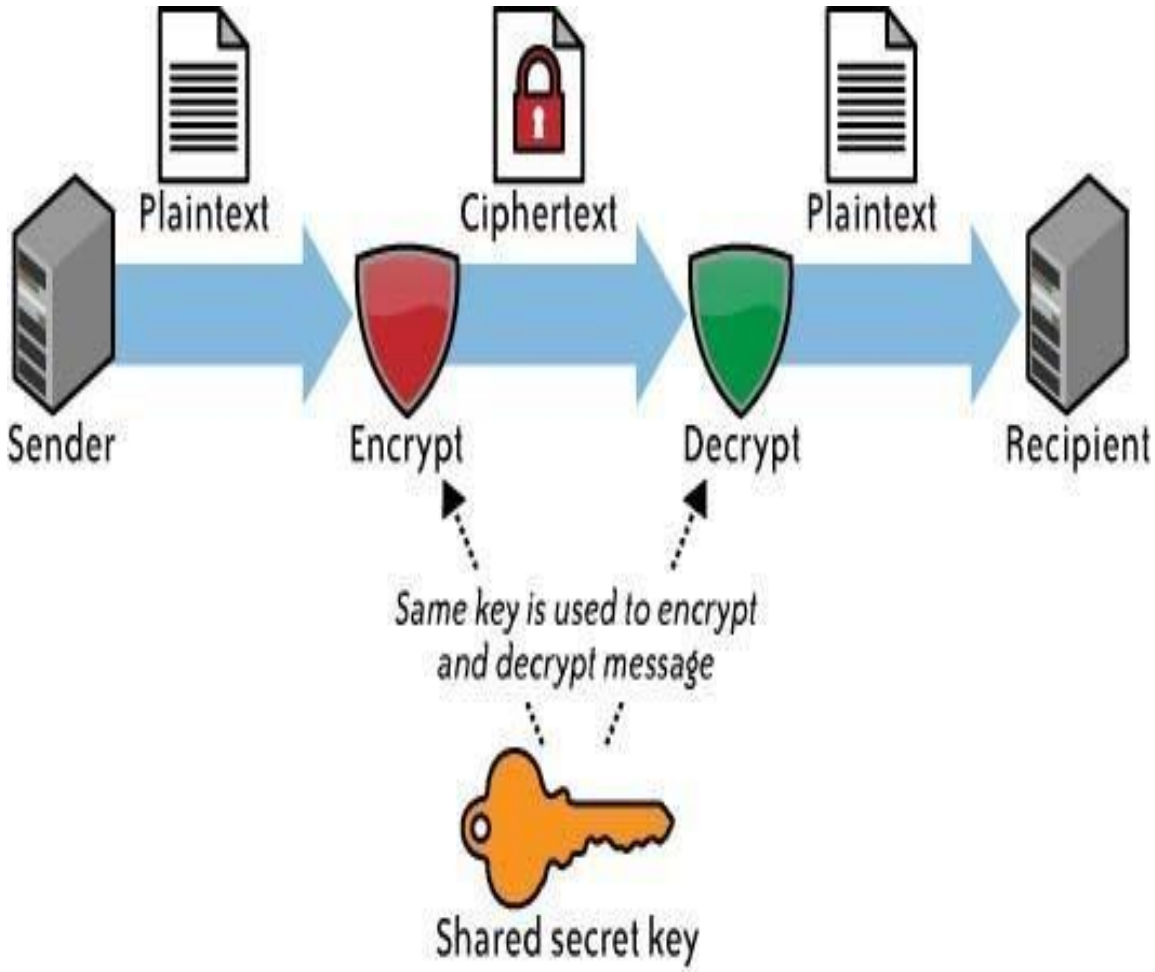
Storage

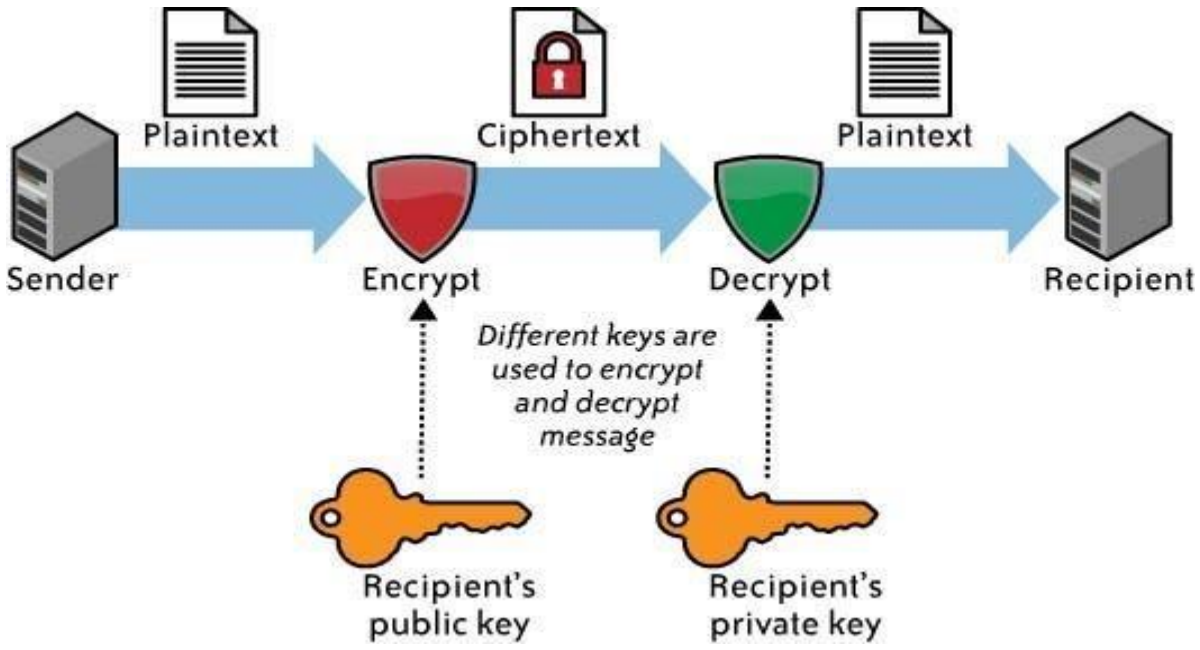
- For data stored in the cloud (i.e., storage-as-a-service), we are referring to IaaS and not data associated with an application running in the cloud on PaaS or SaaS. The same three information security concerns are associated with this data stored in the cloud (e.g., Amazon's S3) as with data stored elsewhere: confidentiality, integrity, and availability.

Confidentiality

- When it comes to the confidentiality of data stored in a public cloud, you have two potential concerns.

- First, what access control exists to protect the data? Access control consists of both authentication and authorization. CSPs generally use weak authentication mechanisms (e.g., username + password), and the authorization ("access") controls available to users tend to be quite coarse and not very granular.
- For large organizations, this coarse authorization presents significant security concerns unto itself. Often, the only authorization levels cloud vendors provide are administrator authorization (i.e., the owner of the account itself) and user authorization (i.e., all other authorized users)—with no levels in between (e.g., business unit administrators, who are authorized to approve access for their own business unit personnel).
- What is definitely relevant to this section, however, is the second potential concern: how is the data that is stored in the cloud actually protected? For all practical purposes, protection of data stored in the cloud involves the use of encryption.





Integrity

- In addition to the confidentiality of your data, you also need to worry about the integrity of your data. Confidentiality does not imply integrity; data can be encrypted for confidentiality purposes, and yet you might not have a way to verify the integrity of that data. Encryption alone is sufficient for confidentiality, but integrity also requires the use of message authentication codes (MACs).
- The simplest way to use MACs on encrypted data is to use a block symmetric algorithm (as opposed to a streaming symmetric algorithm) in cipher block chaining (CBC) mode, and to include a one-way hash function. This is not for the cryptographically uninitiated—and it is one reason why effective key management is difficult. At the very least, cloud customers should be asking providers about these matters.
- Not only is this important for the integrity of a customer's data, but it will also serve to provide insight on how sophisticated a provider's security program is—or is not. Remember, however, that not all providers encrypt customer data, especially for PaaS and SaaS services.

Availability

- Assuming that a customer's data has maintained its confidentiality and integrity, you must alsobe concerned about the availability of your data. There are currently three major threats in this regard—none of which are new to computing, but all of which take on increased importance in cloud computing because of increased risk.
- The first threat to availability is network-based attacks.The second threat to availability is the CSP's own availability. No CSPs offer the

sought-after“five 9s” (i.e., 99.999%) of uptime. A customer would be lucky to get “three 9s” of uptime. AsTable 4-1 shows, there is considerable difference between five 9s and three 9s.

TABLE 4-1. Percentage of uptime

	Total downtime (HH:MM:SS)		
Availability	**Per day**	**Per month**	**Per year**
99.999%	00:00:00.4	00:00:26	00:05:15
99.99%	00:00:08	00:04:22	00:52:35
99.9%	00:01:26	00:43:49	08:45:56
99%	00:14:23	07:18:17	87:39:29

Identity and access management architecture(IAM)

Basic concept and definitions of IAM functions for any service:

Authentication – is a process of verifying the identity of a user or a system.Authentication usually connotes a more roburst form of identification. In some use cases such as service – to- service interaction, authentication involves verifying the network service.

Authorization – is a process of determining the privileges the user or system is entitled to once the identity is established. Authorization usually follows theauthentication step and is used to determine whether the user or service has the necessary privileges to perform certain operations.

Auditing – Auditing entails the process of review and examination ofauthentication, authorization records and activities to determine the adequacy of IAMsystem controls, to verify complaints with established security policies and procedure,to detect breaches in security services and to recommend any changes that areindicated for counter measures.

IAM Architecture and Practice

IAM is not a monolithic solution that can be easily deployed to gain capabilitiesimmediately. It is as much an aspect of architecture as it is acollection of technology components, processes, and standard practices. Standardenterprise IAM architecture encompasses several layers of technology, services, andprocesses. At the core of the deployment architecture is a directory service (such as

LDAP or Active Directory) that acts as a repository for the identity, credential, and user attributes of the organization's user pool. The directory interacts with IAM technology components such as authentication, user management, provisioning, and federation services that support the standard IAM practice and processes within the organization.

The IAM processes to support the business can be broadly categorized as follows:

User management: Activities for the effective governance and management of identity life cycles

Authentication management: Activities for the effective governance and management of the process for determining that an entity is who or what it claims to be.
Authorization management: Activities for the effective governance and management of the process for determining entitlement rights that decide what resources an entity is permitted to access in accordance with the organization's policies.

Access management: Enforcement of policies for access control in response to a request from an entity (user, services) wanting to access an IT resource within the organization.

Data management and provisioning: Propagation of identity and data for authorization to IT resources via automated or manual processes.

Monitoring and auditing: Monitoring, auditing, and reporting compliance by users regarding access to resources within the organization based on the defined policies.

IAM processes support the following operational activities:

Provisioning: Provisioning can be thought of as a combination of the duties of the

human resources and IT departments, where users are given access to data repositories or systems, applications, and databases based on a unique user identity. Deprovisioning works in the opposite manner, resulting in the deletion or deactivation of an identity or of privileges assigned to the user identity.

Credential and attribute management: These processes are designed to manage the life cycle of credentials and user attributes— create, issue, manage, revoke—to inappropriate account use. Credentials are usually bound to an individual and are verified during the authentication process.

The processes include provisioning of attributes, static (e.g., standard text password) and dynamic (e.g., one-time password) credentials that comply with a password standard (e.g., passwords resistant to dictionary attacks), handling password expiration, encryption management of credentials during transit and at rest, and access policies of user attributes (privacy and handling of attributes for various regulatory reasons).Minimize the business risk associated with identityimpersonation.

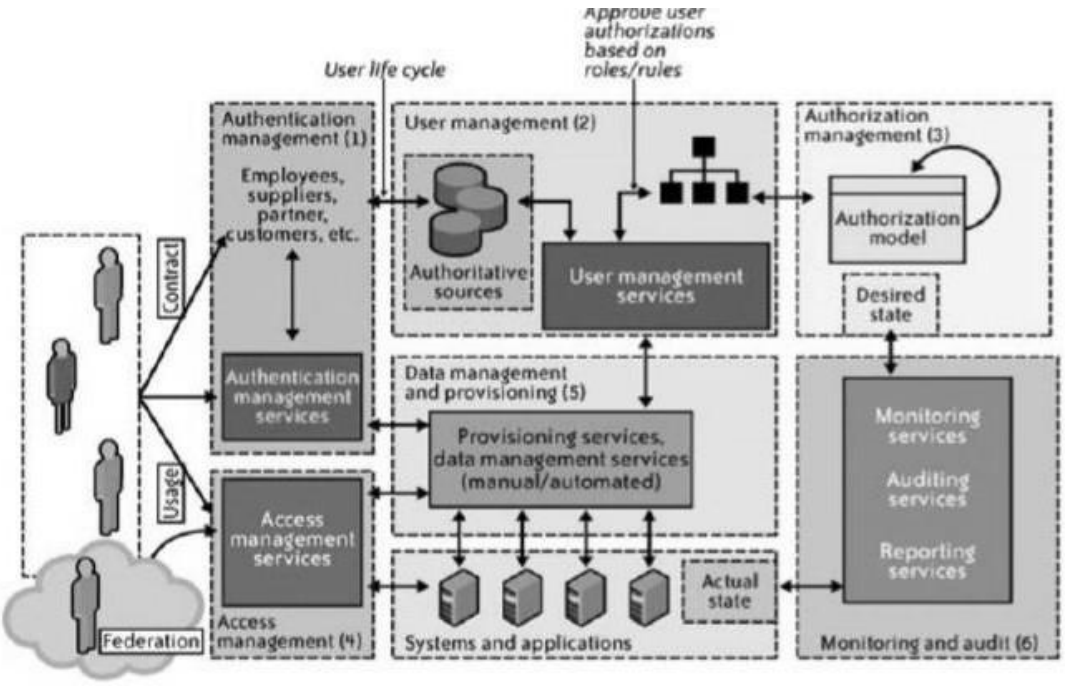


Figure 5.7 Enterprise IAM functional architecture

Entitlement management: Entitlements are also referred to as authorization policies. The processes in this domain address the provisioning and deprovisioning of privileges needed for the user to access resources including systems, applications, and databases. Proper entitlement management ensures that users are assigned only the required privileges.

Compliance management: This process implies that access rights and privileges are monitored and tracked to ensure the security of an enterprise's resources. The process also helps auditors verify compliance to various internal access control policies, and standards that include practices such as segregation of duties, access monitoring, periodic auditing, and reporting. An example is a user certification process that allows application owners to certify that only authorized users have the privileges necessary to access business-sensitive information.

Identity federation management: Federation is the process of managing the trust relationships established beyond the internal network boundaries or administrative domain boundaries among distinct organizations. A federation is an association of organizations that come together to exchange information about their users and resources to enable collaborations and transactions.

Centralization of authentication (authN) and authorization (authZ):

A central authentication and authorization infrastructure alleviates the need for application developers to build custom authentication and authorization features into their applications. Furthermore, it promotes a loose coupling architecture where applications become agnostic to the authentication methods and policies. This approach is also called an —externalization of authN and authZ from applications

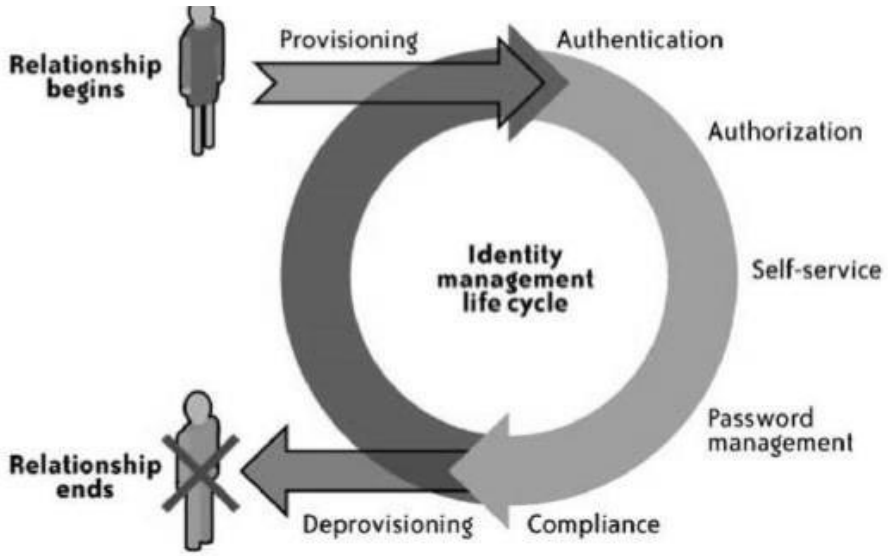


Figure 5.8 Identity Life cycle

IAM Standards and Specifications for Organisations

The following IAM standards and specifications will help organizations implement effective and efficient user access management practices and processes inthe cloud. These sections are ordered by four major challenges in user and access management faced by cloud users:

1. How can I avoid duplication of identity, attributes, and credentials and provide a single sign-on user experience for my users? SAML.

2. How can I automatically provision user accounts with cloud services and automate the process of provisoning and deprovisioning? SPML.

IAM Practices in the Cloud

When compared to the traditional applications deployment model within the enterprise, IAM practices in the cloud are still evolving. In the current state of IAM technology, standards support by CSPs (SaaS, PaaS, and IaaS) is not consistent across providers. Although large providers such as Google, Microsoft, and Salesforce.com seem to demonstrate basic IAM capabilities, our assessment is that they still fall short of enterprise IAM requirements for managing regulatory, privacy, and data protection requirements. The maturity model takes into account the dynamic nature of IAM users, systems, and applications in the cloud and

addresses the four key components of the IAM automation process:

- User Management, New Users
- User Management, User Modifications
- Authentication Management
- Authorization Management

IAM practices and processes are applicable to cloud services; they need to be adjusted to the cloud environment. Broadly speaking, user management functions in the cloud can be categorized as follows:

• Cloud identity administration, Federation or SSO

• Authorization management

• Compliance management

Cloud Identity Administration: Cloud identity administrative functions should focus on life cycle management of user identities in the cloud—provisioning, deprovisioning, identity federation, SSO, password or credentials management, profile management, and administrative management. Organizations that are not capable of supporting federation should explore cloud-based identity management services. This new breed of services usually synchronizes an organization's internal directories with its directory (usually multitenant) and acts as a proxy IdP for the organization.

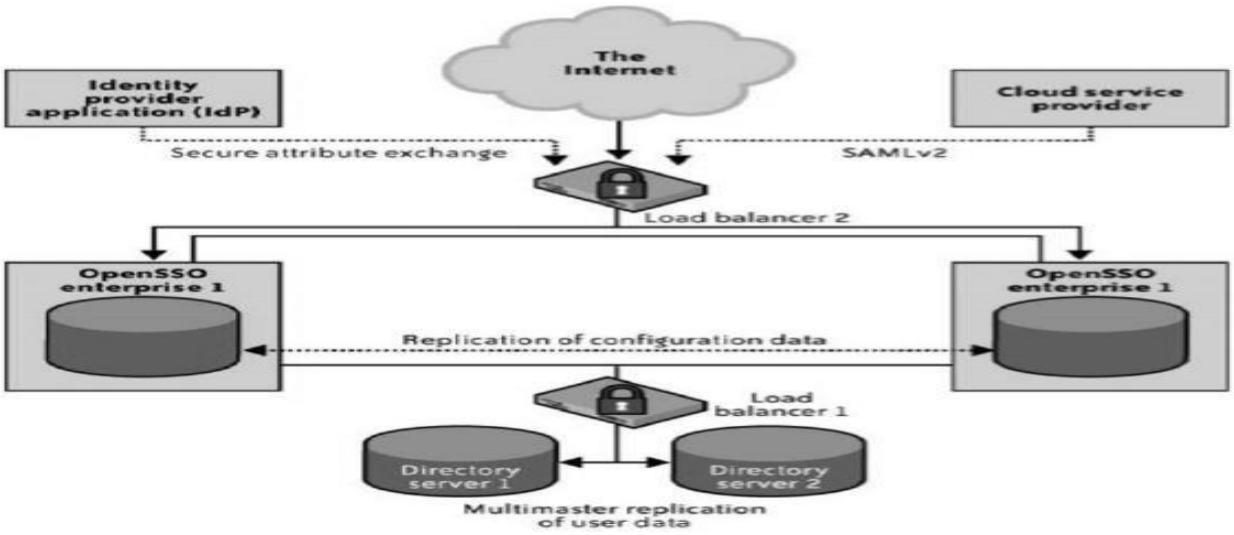
Federated Identity (SSO): Organizations planning to implement identity federation that enables SSO for users can take one of the following two paths (architectures):

• Implement an enterprise IdP within an organization perimeter.

• Integrate with a trusted cloud-based identity management service provider. Both architectures have pros and cons.

Enterprise identity provider: In this architecture, cloud services will delegate authentication to an organization's IdP. In this delegated authentication architecture, the organization federates identities within a trusted circle of CSP domains. A circle of trust can be created with all the domains that are authorized to delegate authentication to the IdP. In this deployment architecture, where the organization will provide and support an IdP, greater control can be exercised over user identities, attributes, credentials, and policies for authenticating and authorizing users to a cloud service.

IdP deployment architecture.



Challenges of Identity and Access Management in the Cloud

Cloud Computing has completely changed the way Identity and Access Management (IAM) is performed in organizations who operate on the cloud. A few years ago, the typical scenario would have been the IT department giving remote access to specific people and only for a few applications. This has changed now, with the employees accessing company resources from their personal devices over unsecure networks.

In order to protect their assets, the security measures should include encryption, logging and monitoring, role-based access control and more. The Cloud SaaS, PaaS and IaaS services offered by Azure and Amazon Web Services, has mandated that the organizations integrate the IAM practices, processes and procedures in a scalable, effective and efficient manner.

Challenges faced by IAM

New cloud-based identity and access management (IAM) services are growing in popularity as more organizations are opting for them to provide a unified and simple identity management. They may add extra security and protection to your company resources. But, it poses key challenges like proper assessment of the existing IT infrastructure, current IAM standards and security before opting for the cloud based IAM services.

The question which most of the organizations now ask, is how to extend their existing IAM systems to manage users and their access to cloud-based applications and services. Also, how to leverage the various cloud services, at a reasonable cost without losing control of the security.

The major challenges faced by the IAM in the cloud:

1. Identity Provisioning / De-provisioning

This concerns with providing a secure and timely management of on-boarding (provisioning) and off-boarding (de-provisioning) of users in the cloud.

When a user has successfully authenticated to the cloud, a portion of the system resources in terms of CPU cycles, memory, storage and network bandwidth is allocated. Depending on the capacity identified for the system, these resources are made available on the system even if no users have been logged on.

Depending on the number of users, the system resources are allocated as and when required, and scaled down regularly, based on projected capacity requirements. Simultaneously, adequate measures need to be in place to ensure that as usage of the cloud drops, system resources are made available for other objectives; else they will remain unused and constitute a dead investment.

2. Maintaining a single ID across multiple platforms and organizations

It is tough for the organizations to keep track of the various logins and ID that the employees maintain throughout their tenure. The centralised federated identity management (FIdM) is the answer for this issue. Here users of cloud services are authenticated using a company chosen identity provider (IdP).

By enabling a single sign on facility, the organization can extend IAM processes and practices to the cloud and implement a standardized federation model to support single sign-on to cloud services.

3. Compliance Visibility: Who has access to what

When it comes to cloud services, it's important to know who has access to applications and data, where they are accessing it, and what they are doing with it. Your IAM should be able to provide a centralised compliance reports across access rights, provisioning/de-provisioning, and end-user and administrator activity. There should be a central visibility and control across all your systems for auditing purposes.

4. Security when using 3rd party or vendor network

A lot of services and applications used in the cloud are from 3rd party or vendor networks. You may have secured your network, but can't guarantee that their security is adequate.

If you are facing any of these challenges, then Sysfore can help you to establish a secure and integrated IAM practices, processes and procedures in a scalable, effective and efficient manner for your organization.