Selvam College of Technology
An Autonomous Institution
Accredited by NAAC with "A" Grade, UGC Recognized 2(f) Status,
An ISO 9001:2015 Certified Institution, Approved by AICTE New Delhi, Affiliated to Anna University-Chennai
PONNUSAMY NAGAR, SALEM ROAD(NH-44), NAMAKKAL-637003. TAMILNADU.
Mobile: 9942099122, 9942099109, Web: www.selvamtech.edu.in

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.

GUEST HOPPING:

Guest hopping in the context of virtual machines and cloud computing typically refers to an attack scenario where an unauthorized user gains access to multiple virtual machines within a cloud environment. This type of attack can potentially compromise the security and integrity of the virtual machines and the data they contain.

Here are some considerations related to guest hopping attacks on virtual machines in a cloud computing environment:

Shared Infrastructure: Cloud computing often involves the sharing of physical resources among multiple virtual machines. If an attacker successfully compromises one virtual machine, they may attempt to leverage that access to gain unauthorized access to other virtual machines within the same infrastructure.

Hypervisor Vulnerabilities: The hypervisor is the software layer that manages and orchestrates virtual machines in a cloud environment. Exploiting vulnerabilities in the hypervisor could allow an attacker to break the isolation between virtual machines, enabling guest hopping attacks.

Misconfigurations: Misconfigurations in virtual machine settings or the cloud infrastructure can create security weaknesses that attackers can exploit to move laterally between virtual machines. This includes weak authentication mechanisms, insecure network configurations, or inadequate access controls.

Privilege Escalation: Once inside a virtual machine, an attacker may attempt to escalate their privileges to gain administrative or root access. This can be achieved by exploiting vulnerabilities in the guest operating system or misconfigurations within the virtual machine.

Data Exfiltration and Malware Propagation: Once an attacker gains access to multiple virtual machines, they may exfiltrate sensitive data from those machines or propagate malware to further compromise the cloud infrastructure or launch attacks on other targets.

To mitigate guest hopping attacks in a cloud computing environment, it is crucial to follow security best practices:

Regularly patch and update the hypervisor, virtual machine software, and guest operating systems to address known vulnerabilities.

Implement strong access controls, including robust authentication mechanisms, to prevent unauthorized access to virtual machines.

Use intrusion detection and prevention systems to monitor and detect suspicious activities within the cloud environment.

Regularly audit and review system logs for any signs of unauthorized access or anomalous behavior. Educate users and administrators about secure configuration practices and the importance of adhering to security guidelines.

By implementing these measures, organizations can reduce the risk of guest hopping attacks and enhance the security of their cloud computing environments.

Application-level security issues (or cloud service provider CSP level attacks) refer to intrusion from the malicious attackers due to vulnerabilities of the shared nature of the cloud. Some companies host their applications in shared environments used by multiple users, without considering the possibilities of exposure to security breaches, such as:

In guest-hopping attacks, due to the separation failure between shared infrastructures, an attacker gets access to a virtual machine by penetrating another virtual machine hosted in the same hardware. One possible mitigation of guest-hopping attack is the Forensics and VM debugging tools to observe any attempt to compromise the virtual machine. Another solution is to use the High Assurance Platform (HAP), which provides a high degree of isolation between virtual machines.

1. Side-Channel Attack

An attacker opens a side-channel attack by placing a malicious virtual machine on the same physical machine as the victim machine. Through this, the attacker gains access to all confidential information on the victim machine. The countermeasure to eliminate the risk of side-channel attacks in a virtualized cloud environment is to ensure that no legitimate user VMs reside on the same hardware of other users.

2. Malicious Insider

A malicious insider can be a current or former employee or business associate who maliciously and intentionally abuses system privileges and credentials to access and steal sensitive customer information within the network of an organization. Strict privilege planning and security auditing can minimize this security risk that originates from within an organization.

3. Cookie Poisoning

Cookie poisoning means to gain unauthorized access into an application or a webpage by modifying the contents of the cookie. In a SaaS model, cookies contain user identity credential information that allows the applications to authenticate the user identity. Cookies are forged to impersonate an authorized user. A solution is to clean up the cookie and encrypt the cookie data.

4. Backdoor And Debug Option

The backdoor is a hidden entrance to an application, which was created intentionally or unintentionally by developers while coding. Debug option is also a similar entry point, often used by developers to facilitate troubleshooting in applications. But the problem is that the hackers can use these hidden doors to bypass security policies and enter the website and access the sensitive information. To prevent this kind of attack, developers should disable the debugging option.

5. Cloud Browser Security

A web browser is a universal client application that uses Transport Layer Security (TLS) protocol to facilitate privacy and data security for Internet communications. TLS encrypts the connection between web applications and servers, such as web browsers loading a website. Web browsers only use TLS encryption

and TLS signature, which are not secure enough to defend malicious attacks. One of the solutions is to use TLS and at the same time XML based cryptography in the browser core.

6. Cloud Malware Injection Attack

A malicious virtual machine or service implementation module such as SaaS or IaaS is injected into the cloud system, making it believe the new instance is valid. If succeeded, the user requests are redirected automatically to the new instance where the malicious code is executed. The mitigation is to perform an integrity check of the service instance before using it for incoming requests in the cloud system.

7. ARP Poisoning

Address Resolution Protocol (ARP) poisoning is when an attacker exploits some ARP protocol weakness to map a network IP address to one malicious MAC and then update the ARP cache with this malicious MAC address. It is better to use static ARP entries to minimize this attack. This tactic can work for small networks such as personal clouds, but it is easier to use other strategies such as port security features on large-scale clouds to lock a single port (or network device) to a particular IP address.

VM MIGRATION ATTACK

VM migration is the process of moving a virtual machine from one physical host to another within a cloud infrastructure. It allows for workload balancing, resource optimization, and maintenance activities in a dynamic cloud environment. However, if the migration process is compromised, it can lead to security risks and potential unauthorized access to VMs and their data.

Here are the steps an attacker might take in a VM migration attack:

1. Interception of Migration Traffic: Attackers may attempt to intercept the migration traffic between the source and destination hosts. By positioning themselves as a "man-in-the-middle," they can eavesdrop on sensitive information, such as the VM's contents, network communications, and credentials exchanged during the migration process.

2. Unauthorized VM Migration: An attacker might try to initiate unauthorized VM migrations within the cloud environment. This can involve moving VMs to their control or to compromised hosts under their influence. Once the VM is under their control, the attacker can gain access to sensitive data, manipulate the VM's behavior, or disrupt the cloud infrastructure.

3. Exploiting Migration Channel Vulnerabilities: The migration process relies on communication channels and protocols between the source and destination hosts. Attackers may exploit vulnerabilities or weaknesses in these channels to gain unauthorized access, inject malicious code into the VM, or manipulate the migration process to their advantage.

4. Resource Exhaustion: Attackers can target the resources involved in the migration process, such as network bandwidth or storage, to cause resource exhaustion. By overwhelming these resources, the attacker can disrupt VM migrations, cause denial-of-service conditions, or impact the availability and performance of other cloud services.

5. VM Rollback Attacks: During VM migration, checkpoints or snapshots are often created to ensure data consistency. Attackers might attempt to tamper with these snapshots or manipulate the rollback process. By doing so, they can compromise the integrity of the VM or introduce unauthorized changes to the VM's state or data.

1. Resource Monitoring and Protection: Implement mechanisms to monitor resource utilization during VM migrations. This helps in detecting and mitigating resource exhaustion attacks, ensuring that sufficient resources are available to complete migrations successfully.

2. Regular Updates and Patching: Keep the migration infrastructure, including the hypervisor and migration software, up to date with the latest security patches. Regular updates address known vulnerabilities and minimize the risk of exploitation.

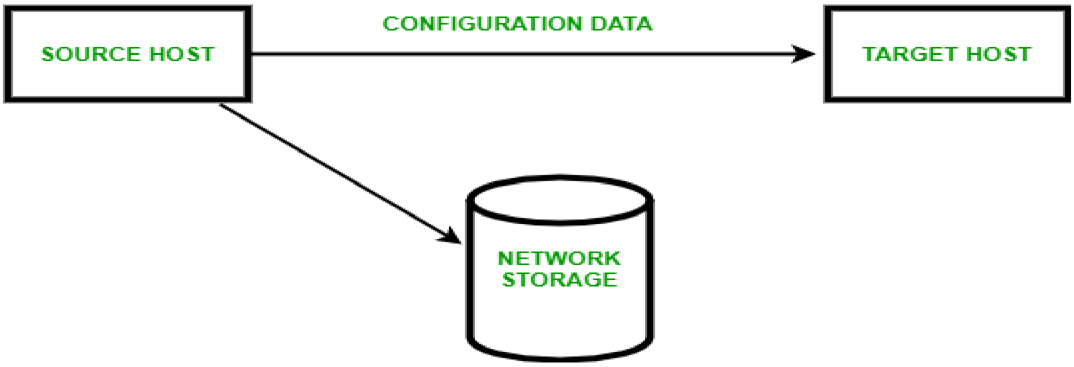
3. Auditing and Logging: Enable comprehensive logging of migration activities, including the source and destination hosts, migration timestamps, and user information. Regularly review the logs to identify any suspicious or unauthorized activities. Logging is crucial for forensic analysis and investigations in case of a security incident.

By implementing these security measures, organizations can strengthen the security and integrity of VM migration processes within their cloud computing

1. Cold Migration :

A powered down Virtual Machine is carried to separate host or data store. Virtual Machine's power state is OFF and there is no need of common shared storage. There is a lack of CPU check and there is long shortage time. Log files and configuration files are migrated from the source host to the destination host.

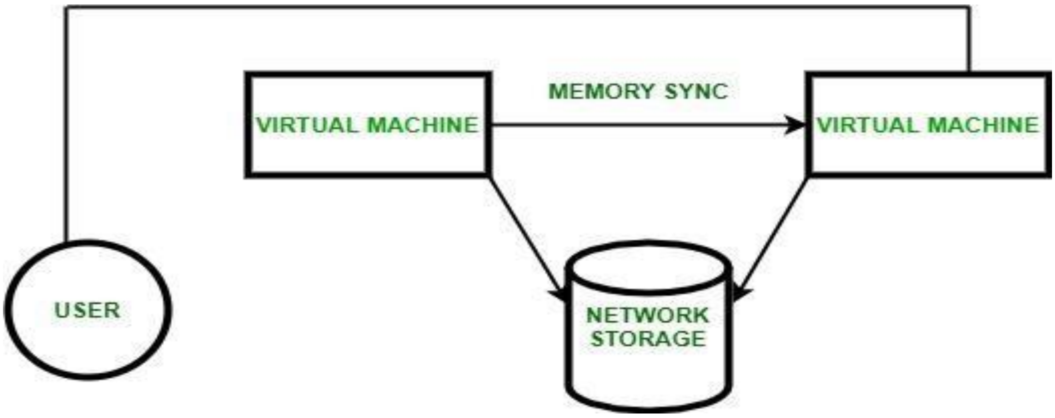
2. The first host's Virtual Machine is shut down and again started on next host. Applications and OS are terminated on Virtual Machines before moving them to physical devices. User is given choice of movement of disks associated from one data store to another one.



Host's Virtual Machine

state is cloned to destination host and then that source host state is discarded. Complete state is shifted to the destination host. Network is moved to destination Virtual Machine.

A common shared storage is needed and CPU checks are put into use. Shortage time is very little.



Without stoppage of OS or applications, they are shifted from Virtual Machines to physical machines. The physical server is freed for maintenance purposes and workloads (which are among physical servers) are dynamically balanced so as to run at optimized levels. Downtime of clients is easily avoidable.

Suspend first host's Virtual Machine and then clone it across registers of CPU and RAM and again resume some time later on second host. This migration runs when source system is operative.

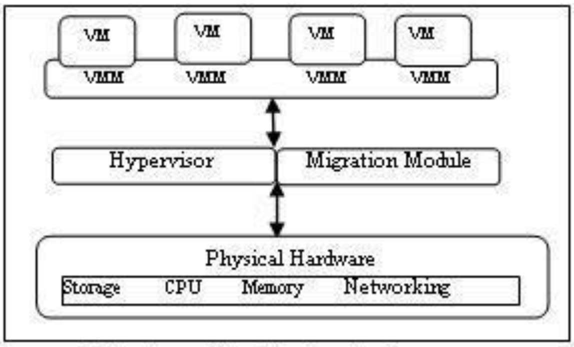
Stage-0:

Is Pre-Migration stage having functional Virtual Machine on primary
host. Stage-1:
Is Reservation stage initializing container on destination
host. Stage-2:
Is Iterative pre-copy stage where shadow paging is enabled and all dirty pages are cloned in succession rounds.
Stage-3:

Is Stop and copy where first host's Virtual Machine is suspended and all remaining Virtual Machine state

are synchronized on second
host. Stage-4:
Is Commitment where there is minimization of Virtual Machine state on first
host. Stage-5:

workload of multiple running virtual machines on a single physical machine. The main difference between virtualization and virtual machine migration is that only migration module is inculcate with hypervisor. The architecture of virtual machine migration virtualized platform is shown in figure:



Migration – Virtualization Architecture

VM migration becomes this process simplified and efficient. It also takes care of load balancing, energy consumption, workload consolidation etc. Henceforth, it becomes more popular and wide adoption in industry. Below table describes the types of VM migrations.

VM Migration Type	Description
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.

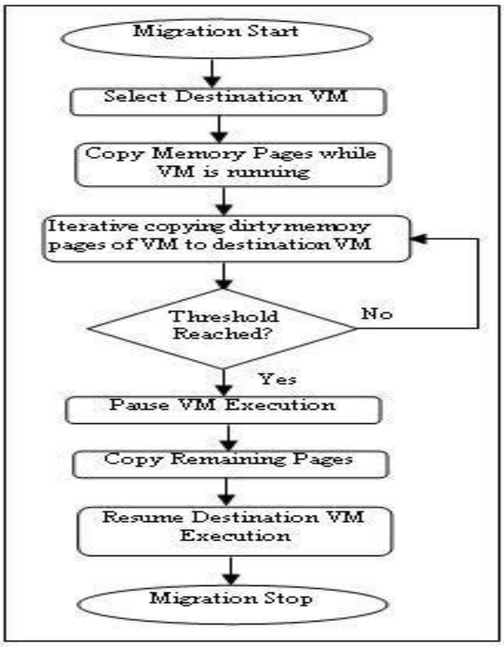
This subsection describes the types of virtual machine migration techniques. It is basically of two types:- copy Migration

Po-Copy Migration

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.

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.

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.


Migration Start
Select Destination VM
Copy Memory Pages while VM is running
Iterative copying dirty memory pages of VM to destination VM
Threshold Reached?
No
Yes
Pause VM Execution
Copy Remaining Pages
Resume Destination VM Execution
Migration Stop

Pre- Copy Migration Technique

1. Hypervisor Hardening: Employ hypervisor hardening techniques to reduce the attack surface and strengthen the security of the hypervisor. This can include measures like disabling unused features, configuring secure network settings, and employing intrusion detection systems for monitoring.

2. Network Segmentation: Implement network segmentation within the virtualized environment to isolate different VMs and limit the lateral movement of an attacker who gains access to the hypervisor. This helps contain the impact of a potential hyperjacking attack.

3. Hypervisor Security Monitoring: Implement robust monitoring and logging mechanisms to detect suspicious activities and potential signs of hyperjacking. Monitor hypervisor logs, network traffic, and other relevant indicators to identify any unauthorized access or abnormal behavior.

4. Access Control and Authentication: Implement strong access control measures for the hypervisor, including multi-factor authentication, role-based access control, and regular review of access privileges. This helps minimize the risk of unauthorized access to the hypervisor.

By implementing these security measures, organizations can reduce the risk of hyperjacking attacks and strengthen the overall security posture of their virtualized environments. Regular security assessments and audits can also help identify and address potential vulnerabilities before they are exploited by attackers.

<u>DATA AND ITS SECURITY</u>

4. **Discuss in detail about provider data and its security.(May-2023)**

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

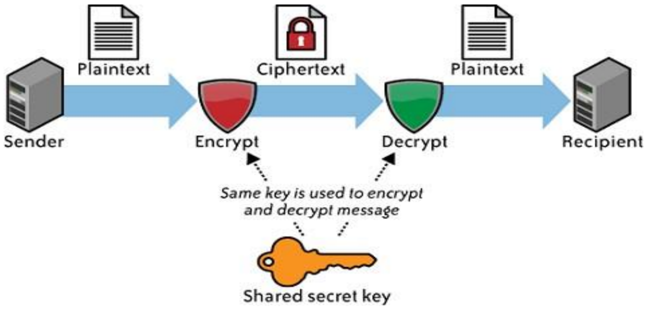
Storage

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.

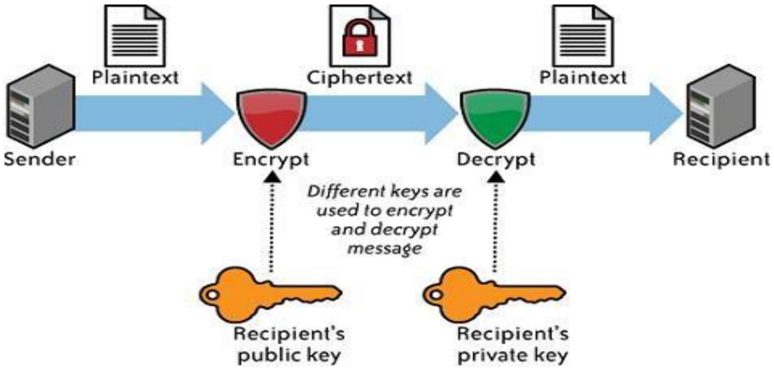
Confidentiality

For large organizations, this coarse authorization presents significant security concerns unto itself. Often, the only authorization levels cloud vendors provide are administrator authorization and user authorization with no levels in between. Again, these access control issues are not unique to CSPs

Symmetric Encryption Diagram



Asymmetric Encryption Diagram



IAM

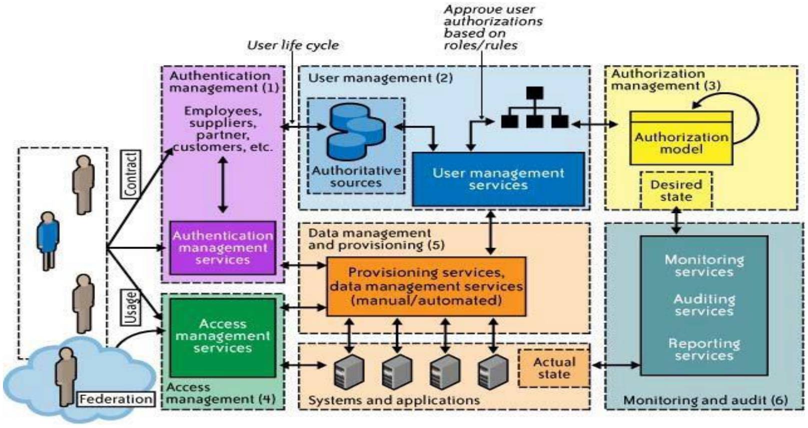
5. Draw the architecture of IAM and explain in detail. IAM- Identity Access Management

The protection of enterprise information assets is critical to improve and sustain the business, which is one of the core security aspects of architecture.

- **Identity Governance:** The ability in making sure the right people are granted the right access rights, making sure the wrong ones are not and managing the lifecycle through organization structure, processes and enabling technology.
- **Directory Services:** The ability in enforcing access rights, within specified policy, when users attempt to access a desired application, system or platform.
- **Access Management:** The ability to provide ways to control storage of identity information about users and access rights.

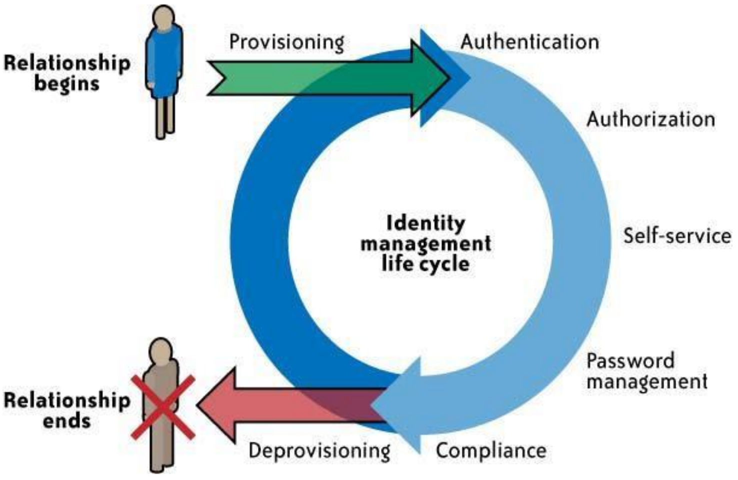
IAM Architecture and Practice

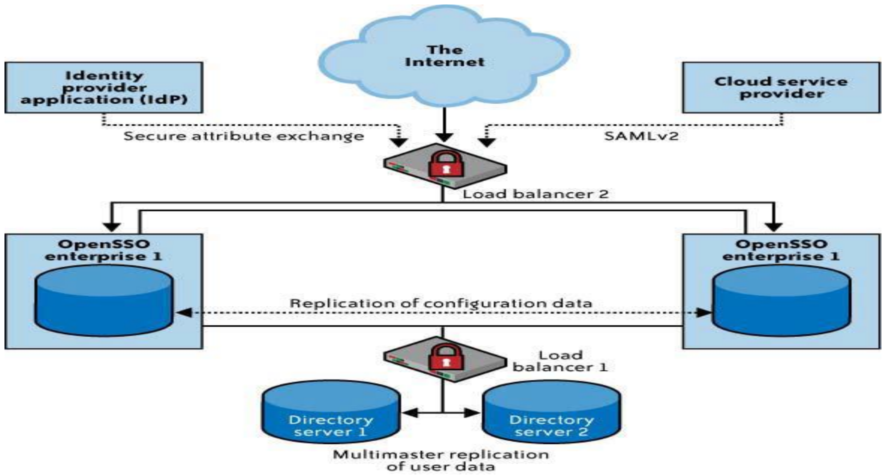
- User management
- Authentication management
- Authorization management
- Access management
- Data management and provisioning
- Monitoring and auditing


User life cycle
Approve user authorizations based on roles/rules
Authentication management (1)
Employees, suppliers, partner, customers, etc.
Authentication management services
User management (2)
Authoritative sources
User management services
Authorization management (3)
Authorization model
Desired state
Contract
Usage
Data management and provisioning (5)
Provisioning services, data management services (manual/automated)
Access management services
Access management (4)
Federation
Actual state
Systems and applications
Monitoring services
Auditing services
Reporting services
Monitoring and audit (6)

Enterprise IAM functional architecture

Identity life cycle

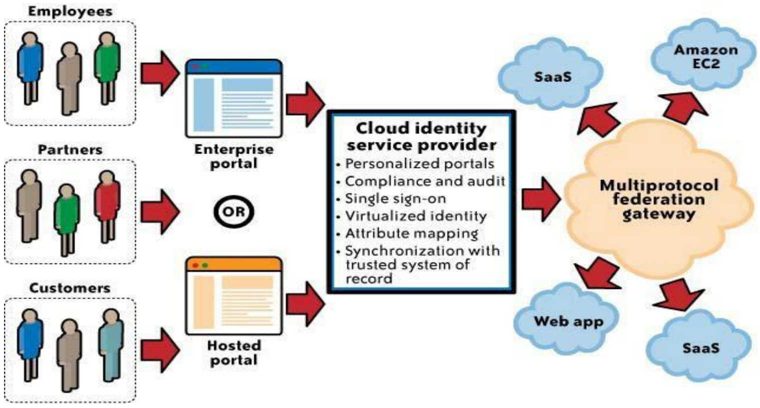




Identity provider deployment architecture

User management functions

- Cloud identity administration
- Federation or SSO
- Authorization management
- Compliance management



IDaaS- IDentity management as a Service

SaaS

- Two major challenges for identity management

– Is the organization ready to provision and manage the user life cycle by extending its established IAM practice to the SaaS service?

– Are the SaaS provider capabilities sufficient to automate user provisioning and life cycle management without implementing a custom solution for the SaaS service?

Customer responsibilities

- User provisioning
- Profile management
- SaaS IAM capability evaluation
- Investigation support
- Compliance management

PaaS

- Customer Responsibility

– PaaS platform service levels

– Third-party web services provider service levels

– Network connectivity parameters for the network (Internet)

- PaaS Health Monitoring

Health Monitoring Services

- Service health dashboard published by the CSP
- CCID (this database is generally community-supported, and may not reflect all CSPs and all incidents that have occurred)
- CSP customer mailing list that notifies customers of occurring and recently occurred outages
- RSS feed for RSS readers with availability and outage information

IaaS availability in cloud

- Availability of a CSP network, host, storage, and support application infrastructure
- Availability of your virtual servers and the attached storage for compute services.
- Availability of virtual storage that your users and virtual server depend on for storage service.
- Availability of your network connectivity to the Internet or virtual network connectivity to IaaS services.
- Availability of network services, including a DNS, routing services, and authentication services required to connect to the IaaS service.

IaaS Health Monitoring

- Service health dashboard published by the CSP.
- CCID (this database is generally community-supported, and may not reflect all CSPs and all incidents that have occurred).
- CSP customer mailing list that notifies customers of occurring and recently occurred outages.
- Internal or third-party-based service monitoring tools (e.g., Nagios) that periodically check the health of your IaaS virtual server.

Key privacy issues in the cloud

- Typical issues with regard to the dependence on the Cloud Computing provider are

– Cloud Computing provider were to go bankrupt and stopped providing services, the customer could experience problems in accessing data and therefore potentially in business continuity

– Some widely used Cloud Computing services (e.g. GoogleDocs) do not include any contract between the customer and Cloud Computing provider.

The IAM architecture is made up of several processes and activities (see Fig. 4.9.2). The processes supported by IAM are given as follows.

a) **User management -** It provides processes for managing the identity of different entities.

b) **Authentication management -** It provides activities for management of the process for determining that an entity is who or what it claims to be.

c) **Access management -** It provides policies for access control in response to request for resource by entity.

d) **Data management -** It provides activities for propagation of data for authorization to resources using automated processes.

e) **Authorization management -** It provides activities for determining the rights associated with entities and decide what resources an entity is permitted to access in accordance with the organization's policies.

f) **Monitoring and auditing -** Based on the defined policies, it provides monitoring, auditing, and reporting compliance by users regarding access to resources.

The activities supported by IAM are given as follows.

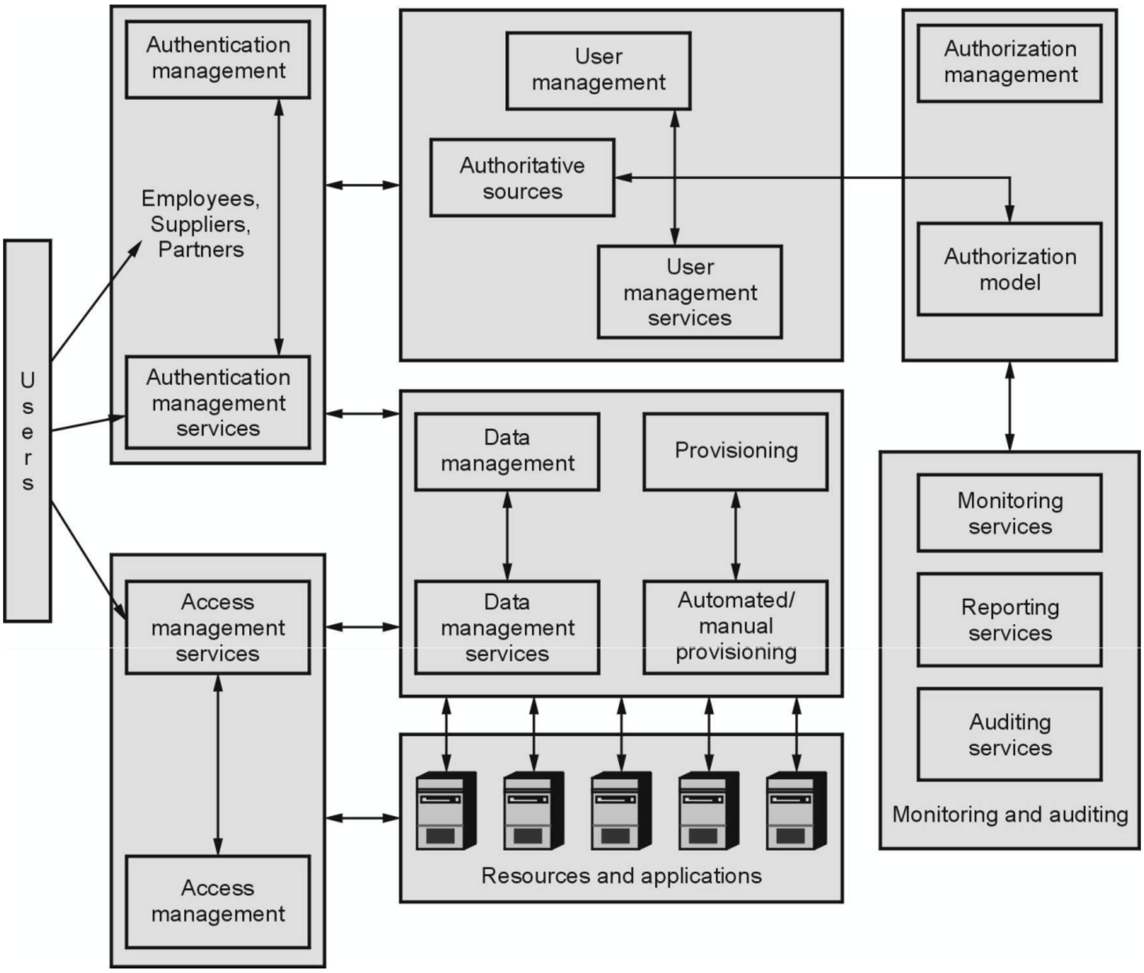
a) **Provisioning -** The provisioning has essential processes that provide users with necessary access to data and resources. It supports management of all user account operations like add, modify, suspend, and delete users with password management. By provisioning the users are given access to data, systems, applications, and databases based on a unique user identity. The deprovisioning does the reverse of provisioning which deactivate of delete the users identity with privileges.

b) **Credential and attribute management -** The Credential and attribute management prevents identity impersonation and inappropriate account use. It deals with management of credentials and user attributes such as create, issue, manage and revoke users to minimize the business risk associated with it. The individuals' credentials are verified during the authentication process. The Credential and attribute management processes include provisioning of static or dynamic attributes that comply with a password standard, encryption management of credentials and handling access policies for user attributes.

c) **Compliance management -** The Compliance management is the process used for monitoring the access rights and privileges and tracked to ensure the security of an enterprise's resources. It also helpful to auditors to verify the compliance to various access control policies, and standards. It includes practices like access monitoring, periodic auditing, and reporting.

Identity federation management - Identity federation management is the process of managing the trust relationships beyond the network boundaries where organizations come together to exchange the information about their users and entities.

e) **Entitlement management -** In IAM, entitlements are nothing but authorization policies. The Entitlement management provides processes for provisioning and deprovisioning of privileges needed for the users to access the resources
including systems, applications, and databases.



IAM

Security Standards

Security standards are needed to define the processes, measures and practices required to implement the security program in a web or network environment. These standards also apply to cloud-related IT exercises and include specific actions to ensure that a secure environment is provided for cloud services along with privacy for confidential information. Security standards are based on a set of key principles designed to protect a trusted environment of this kind. The following sections explain the different security standards used in protecting cloud environment.

Security Assertion Markup Language (SAML)

Security Assertion Markup Language (SAML) is a security standard developed by OASIS Security Services Technical Committee that enables Single Sign-On technology (SSO) by offering a way of authenticating a user once and then communicating authentication to multiple applications. It is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.

The XML schema is mainly used to specify SAML assertions and protocols. For authentication and message integrity, both SAML 1.1 and SAML 2.0 use digital signatures based on the XML Signature Standard. XML encryption is supported in SAML 2.0 but not by SAML 1.0 as it doesn’t support encryption capabilities. SAML defines assertions, protocol, bindings and profiles based on XML.

Open Authentication (OAuth)

OAuth is a standard protocol which allows secure API authorization for various types of web applications in a simple, standard method. OAuth is an open standard for delegating access and uses it as a way of allowing internet users to access their data on websites and applications without passwords. all their identities. This mechanism is used by companies such as Amazon, Google, Facebook, Microsoft and Twitter to permit the users to share information about their accounts with third party applications or websites. It specifies a process for resource owners to authorize third-party access to their server resources without

sharing their credentials. Over secure Hypertext Transfer Protocol (HTTPs), OAuth essentially allows access tokens to be issued to third-party clients by an authorization server, with the approval of the resource owner. The third party then uses the access token to access the
protected resources hosted by the resource server.

Secure Sockets Layer and Transport Layer Security

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are cryptographically secure protocols to provide security and data integrity for TCP/IP based communications. The network connections segments in the transport layer are encrypted by the TLS and SSL.

In web browsers, e-mail, instant messaging and voice over IP, many implementations of these protocols are widely used. TLS is the latest updated IETF standard protocol for RFC 5246.

The TLS protocol allows client/server applications to communicate across a network in a way that avoids eavesdropping, exploitation, tampering and message forgery. TLS uses cryptography to ensure endpoint authentication and data confidentiality.

A more secure bilateral connection mode is also supported by TLS ensuring that both ends of the connection communicate with the individual they believe is connected. This is called mutual authentication.

The TLS client side must also keep a certificate for mutual authentication. Three basic phases involve TLS are Algorithm support for pair negotiation involves cipher suites that are negotiated between the client and the server to determine the ciphers being used; Authentication and key exchange involves decisions on authentication algorithms and key exchange to be used