Cloud Computing

CHAPTER 7

HOW ARE BUSINESS APPLICATIONS IN THE CLOUD MANAGED SAFELY

Dr. JAMIL S. ALAGHA

How are Business Applications in the Cloud Managed Safely?

Mission critical data and connecting to systems across distances requires that IT specialists be particularly vigilant regarding who can use, see, or change online resources

Security concerns change for a firm when it moves IT services into the cloud

Common misconception is security becomes solely the concern of the cloud provider and the client is relieved of that responsibility

Organizations need to take proactive role in ensuring their resources are kept safe and secure

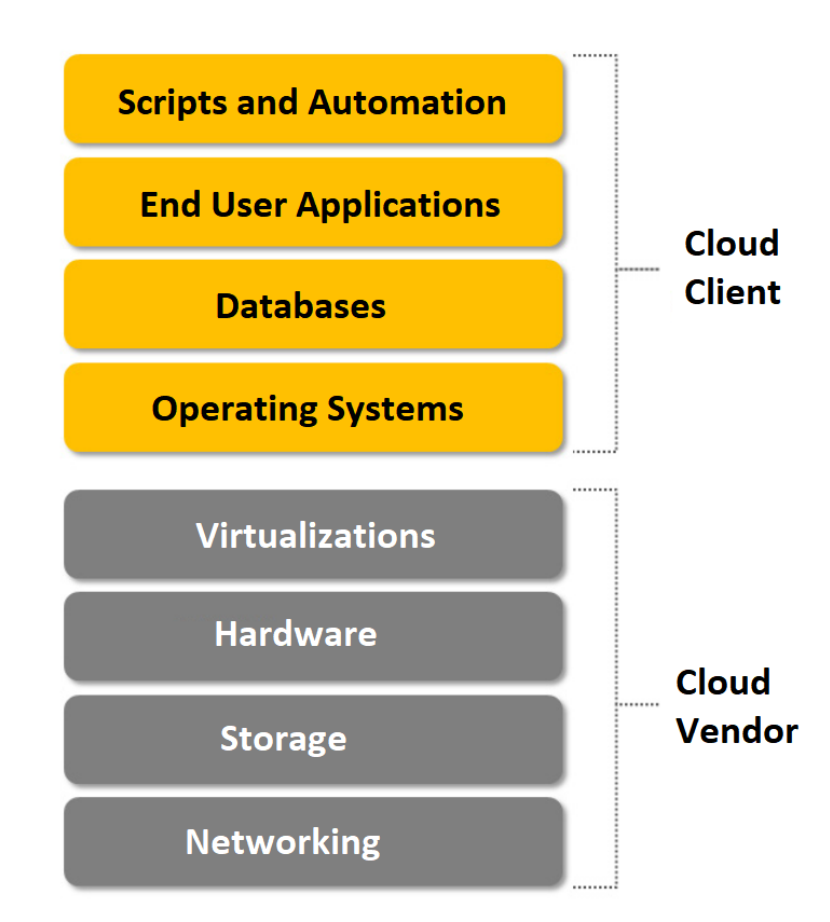
Security is a shared responsibility between cloud vendor and cloud client

Cloud Vulnerabilities

- IT administrators may lose the ability to manage user control and visibility because cloud vendors manage those services
- Managing resources and services more challenging due to virtualization and provisioning with resources that are not be fully removed when not in use
- Unauthorized cloud services, malware infections or data leakage can occur
- Widespread use of APIs to access cloud services opens new points of vulnerability and potential weak spots for malicious attacks and malware
- Use of cloud resources by multiple tenants leaves open the possibility that overlap occurs in a shared public cloud environment
- Data and other resources might remain in unexpected locations because these are spread among multiple storage devices in decentralized ways

Shared Responsibility Model for Cloud Security

- Cloud provider assumes responsibility for security of cloud resources including the infrastructure, storage, databases, networks, containers, VMs, and so forth.
- Cloud client assumes responsibility for use of resources in the cloud including software applications, data, services, operating systems, firewalls, user management, and so forth.
- Many cloud providers offer extra services to help manage aspects of the cloud client's responsibilities.



CLOUD SECURITY IN IAAS ENVIRONMENTS

IaaS Risk Areas

- **Resource misconfiguration -** How and where various cloud systems are deployed, and common mistakes that occur when this is done. Scripts created for automation or orchestration with certain actions that make cloud resource more vulnerable to error, attacks, or other problems. Also include ‘guessable’ or default settings.
- **Vulnerabilities -** incorrectly configured access permissions give unauthorized users access to sensitive, cloud-based information. Some folders might contain additional files with sensitive information useful for additional system malfeasance. Includes scripts containing UserIDs and Password (e.g. leakage).
- **Zombie systems –** Nonproductive resources still running on system

NPBs and IaaS Security Measures

Network packet brokers (NPB) - Devices that offer monitoring capabilities and tools that oversee network traffic at cloud endpoints. NPBs interact with other monitoring and security systems and feed data from the network stack. Provides extra visibility into IaaS security within cloud-based infrastructure. Best practice uses NPBs to direct traffic and data to appropriate performance tools and security applications. NPB can log data to allow further and more in-depth analyses.

Other Security Measures

- Use of Virtual routers
- Virtual web application firewalls that protect servers against malware and viruses.
- Virtual network-based firewalls used to guard cloud endpoints.
- Intrusion Detection and Prevention Systems (hardware and software)
- Segmenting Networks with special consideration given to areas connected to sensitive or highly targeted resources.

Zombie Types in IaaS

***Zombie servers and zombie workloads*.** Servers or workloads are started as tests and then not deprovisioned afterwards. Or, created during development efforts and not properly removed by programmers. Can be security risks because they provide entry points into resources that may not be watched carefully.

***Zombie/orphan storage*.** Remnants from testing or development that have not been deprovisioned. Storage issues also relate to disks not attached to system in a formal way. If critical data were placed onto an unmonitored location, leakage or loss can occur.

Workload problems. Hackers can use cloud resources to set up mail servers, or programs that attempt to launch attacks or determine passwords. Essentially rogue processes that should not be running. Tools can detect and terminate these sorts of activities.

Temporary or dormant resources. Resources taken offline temporarily, and a security update occurs during that time. Item may be out of date and vulnerable to attack. Again, tools can watch for these issues and ensure situation does not occur.

PaaS Security Architecture

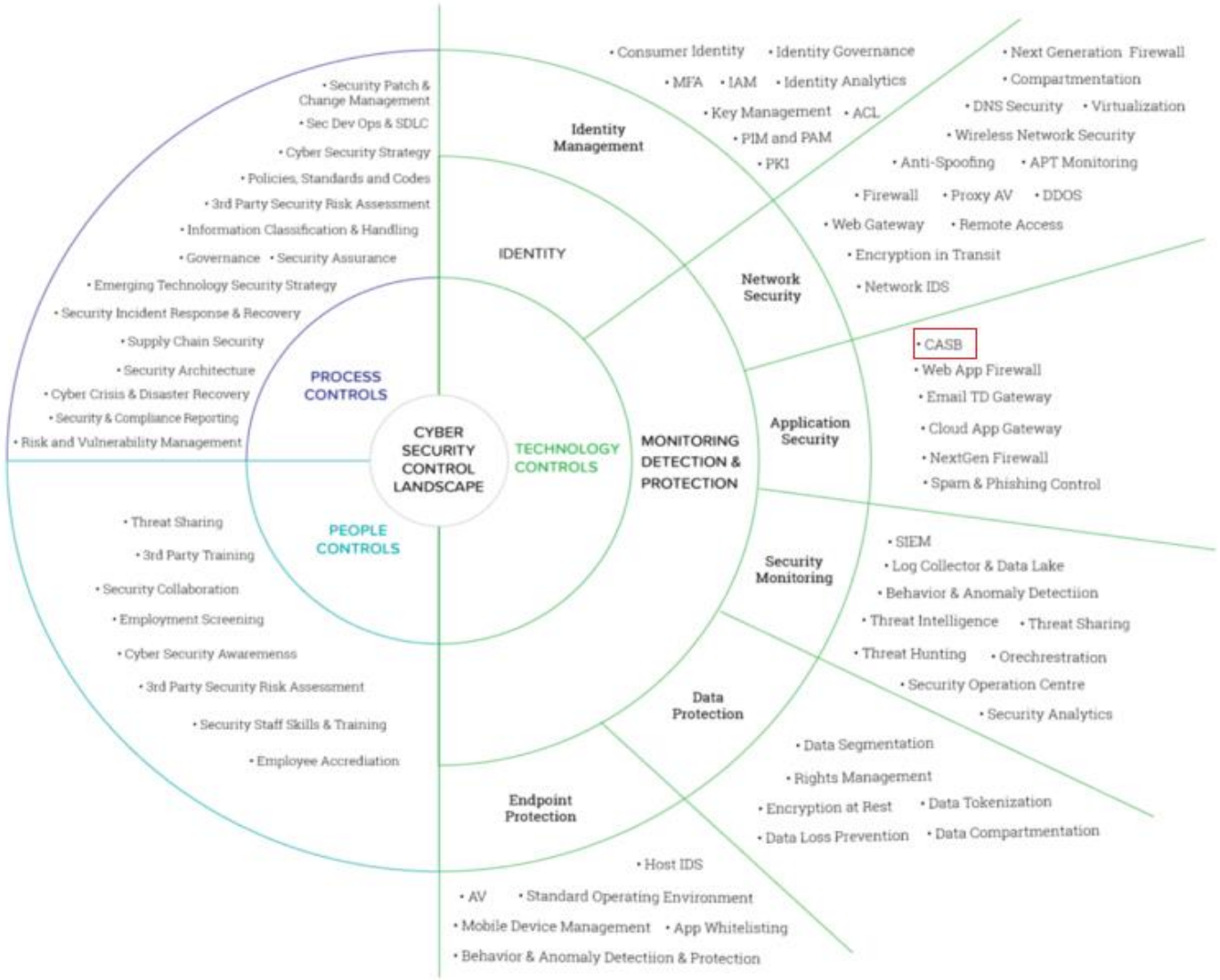
Cloud customer relies on the cloud provider to supply the hardware, some software, and provisioning capabilities for the system

Cloud host takes on more security measures than in IaaS security

In addition to areas in IaaS security, PaaS vendors offer security for logging in, monitoring API gateways, and restricting IP addresses

PaaS providers offer security features that ensure visibility, compliance, data security, and threat protection.

Solutions known as cloud access security broker or CASB



CASB and other cloud security features

4 Main Components of CASB

Visibility: The ability to see resources is a key concept when it comes to cloud computing. An organization loses visibility with PaaS or because the cloud provider manages aspects of resource usage and user access. CASBs help by providing services to enhance visibility which allow administrators to see who is using what.

Compliance: CASBs address laws, regulations, or organizational policies and ensure system rules are updated as laws change. CASB services block access to any untrained users.

Data Security: CASB-enforced rules and protections ensure the correct people access critical data assets.

Threat Protection: Additional malware, firewall, and virus checking measures may be provided within the CASB framework. Particular attention may be given to critical resources and areas of the platform that contain sensitive data or systems.

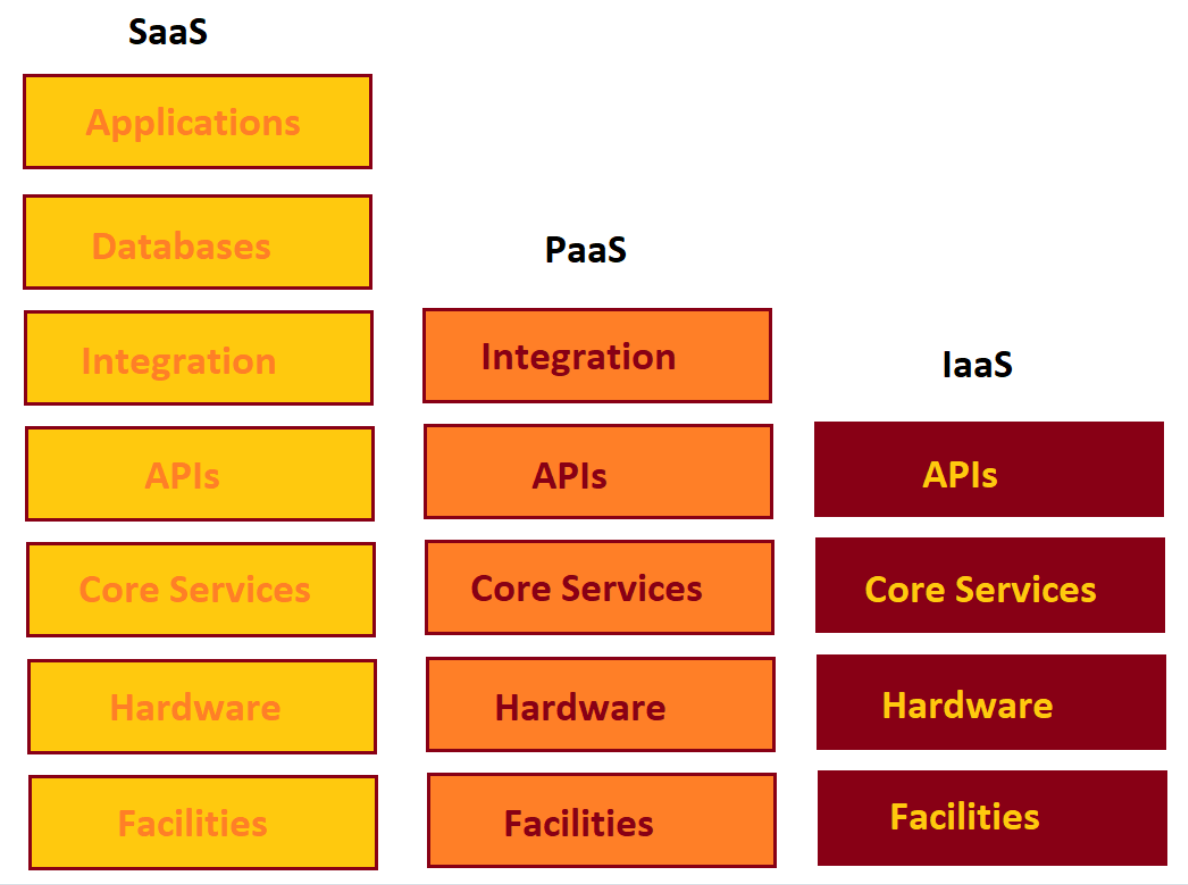
SaaS Security Architecture

SaaS cloud providers take on a high degree of security-related issues for their customers

Services may be used by individuals or small businesses with little or no internal IT functions

Nearly all aspects of security must be managed by the cloud provider

CASBs are used extensively by providers to monitor and discover problems or potential weaknesses related to security in SaaS systems



VENDOR SECURITY RESPONSIBILITIES UNDER DIFFERENT CLOUD COMPUTING MODELS

All Cloud Models Need:

Use a single sign-in approach for accounts with services from multiple vendors to enhance logging, monitoring and visibility.

Use virtual firewalls and ensure these are updated regularly and vigorously.

Use virus checking, malware detection/prevention and data loss prevention tools.

Perform regular audits of security and usage patterns.

Add a security information and event management system (SEIM) and a denial-of-service protection package (DDoS).

Typical Access and Identity Groups in the Cloud (1 of 2)

General employees – People that work for an organization and need general access to a set of common resources required to complete their jobs.

Managers – These individuals will need access to organizational systems that relate to their jobs and need access to data about their directly reporting employees.

Business Administrators – People at higher levels in an organization need access to strategic information, accounting reports, and systems that support their decision-making roles.

Customers / Clients – People that use an organization's e-commerce system may need access to order entry systems and so forth.

Typical Access and Identity Groups in the Cloud (2 of 2)

Business Affiliates – Business partners may need to see inventory levels or access information to support their roles.

Consultants – Temporary and limited accounts may be assigned to people working with an organization.

Business Discipline Groups – People need access to specialized systems that support their specific job roles.

Groups for IT Automation – Accounts will be set up to help with automation and orchestration tasks. These are used by IT administrators to perform needed tasks.

Access Management

Determining who should have access to which resources is challenge

Starts with IT administrators who work in conjunction with other leaders to develop an identity governance strategy

May be in place prior to cloud migration but policies need modifications and updates for cloud environments

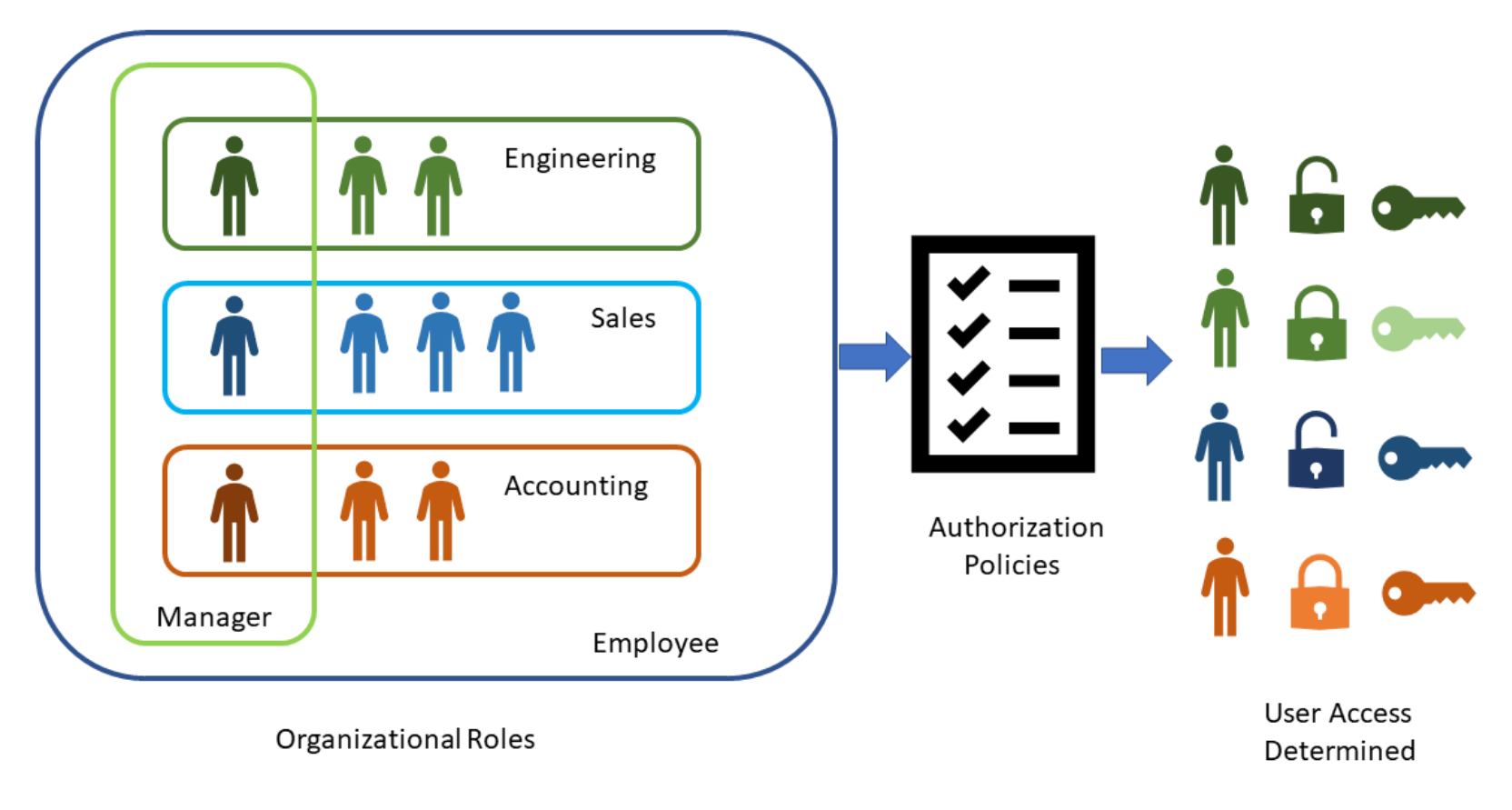
Accounts need to be listed in a central directory service such as Microsoft's Active Directory

Facilitate auditing usage, resource provisioning and deprovisioning, and movement of users between groups as their organizational roles change

Often uses a central dashboard to organize the effort and reduce errors

Uses Identity and Access Management System (IAM)

Policies Determine Access to Cloud Resources



Development Effort integrated with IAM

New cloud applications integrate with the IAM system to check access rights before each resource access.

Prior to serving requested data or services, applications perform a series of checks based on data permissions, application permissions, user group, and specific user privileges.

Data is encrypted according to IAM policies related to the current user, data, and application.

User access rights are continually checked dynamically as resources are used. This differs from merely passing through a doorway that permits access like the stateless approach used by web servers.

IAM Dynamically: Developer's Approach

A stateless approach for IAM is being built into many cloud software applications. The software uses an API that pulls permission data from a database each time a resource is required. The pattern used in these systems is:

1. **Software requests resources**
2. **Identity retrieved**
3. **Identity validated (usually via API from database)**
4. **Resource access permitted with current identity**
5. **Identity validated and limitations applied**
6. **Resource access permitted subject to permission level and limitations**
7. **Resources released**
8. **Software logs completion**

Identity Provisioning

Securely adding and removing cloud users in timely and effective manners

Must consider the user's potential impact on the system

- Do new software licenses need to be added?
- Does the addition of a user impact processing times, storage needs or network bandwidth?
- Do systems need downsizing when a user leaves the organization?

Considerations for Cloud Licensing

- On average, how many users will be on the system?
- What resources are needed by most users?
- Do enough licenses exist to cover users during critical times and average times of usage?
- Are organizational processes in place that enable business users to inform IT administrators that a new user should be added?
- What resource demand thresholds trigger acquisition of more licenses?
- Likewise, are organizational processes in place that enable business users to inform IT administrators that an existing user should be removed?
- What happens to data regarding removed users? Is it retained or archived?
- Are any specific security measures needed regarding user removal?

Licensing Models for Cloud Software

Per Use - monitors either the number of accesses, the amount of time spent in application, or uses other metrics to determine cost.

Per User - assesses total user number to provide a price and may be based on seats, meaning a hard limit on the number of simultaneous users at any given time.

FIM versus SSO

Single Sign On (SSO) and Federated ID Management (FIM) solutions have the same goal---users have one set of credentials to access all organizational computing resources in a secure and trustworthy manner. FIM can be considered a form of SSO but the two have key differences. SSO enables users to have a single set of credentials for use in a single organization. FIM expands the definition and provides users with access across different organizations or cloud systems. Not all SSO solutions use FIM but most FIM solutions rely on SSO technologies across domains. SSO is token-based technology which means each user is assigned a token that provides access to systems within the organization. In infrastructure using a federated approach, users interact with an FIM system that provides permission to enter affiliated systems.

FIM Systems (Also called IDaaS)

- Generally use security assertion markup language (SAML) to ensure a wide range of systems can use federated logins.
- Popular FIM systems include OpenID, OAuth, and Shibboleth.
- FIM processes use a procedure like this:
  - Users authenticate on their home security domain network.
  - After that authentication, users can log into remote, partner networks that use identity federation.
  - An application requests authentication information from the user's home authentication server.
  - The home server authorizes the user to access the remote application.
  - The user is permitted access desired remote resources.

Shibboleth

Shibboleth is a widely used, open-source FIM often deployed in higher education environments. It allows SSO within organizations and permits federated logins across enterprises and domains. It also permits sites to protect online resources and ensure privacy of critical data. Figure 7.5 is open source from the Shibboleth website located at: https://www.shibboleth.net/

FIM Benefits

Simplifies the IT administrator's role when it comes to tracking users

Prevents security issues from occurring when a user leaves an organization (one removal from the home domain ensures the user no longer has access to other resources and domains)

Organization can form an identity federation to ensure outside users have access

No need to remember multiple passwords or user IDs

Updating passwords is easy

IT help desk issues are less likely to occur

End-users are more likely to have a strong password rather than weak variants of the same one

FIM Challenges

Must ensure current systems compatible with federated one

Migration might be required

An organization incurs costs related to training and, if using commercial services, associated subscription costs.

Companies must understand their own security needs plus those of all organizations they are joining

Organization must ensure any third party using their resources meets internal security and usage policies

User visibility becomes more of an issue

Security audits and logs may mean an IT administrator must work with people from outside their firm to uncover usage patterns and needs

Example IAM Products

Microsoft Azure Active Directory: Azure Active Directory (Azure AD) builds on Microsoft's Active Directory (AD) services to provide multi-tenant, cloud-based identity management services.

Google Cloud IAM: Google offers this service to provide cloud identity and access management services and give administrators the ability to determine which users can view, change, or access various cloud-based resources.

Okta: Works across many emerging major platforms in cloud computing and uses an organization's on-premise or cloud identity management system and integrates that with its cloud-based tool called *Universal Directory (UD)*.

Amazon Cognito: Amazon offers federated identity pools that enable users with identities from various providers to access their resources.

What is Active Directory?

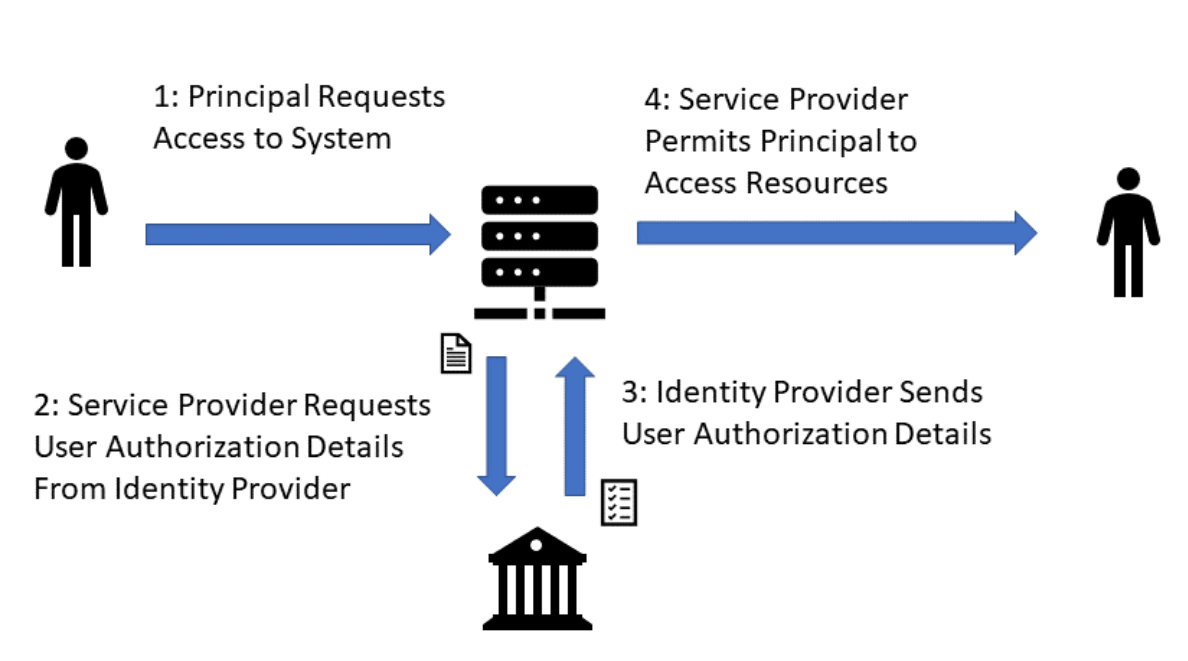
Microsoft's Active Directory (AD) is a Windows OS service used to connect users with network resources. It offers an interface to give IT Administrators access control to network directories, folders, and resources. It controls user access based on security policies set up and organized by an IT administrator.

Identity Management Standards

SAML: Original open authentication standard from about 2001 that stands for Security Assertion Markup Language. Used for authentication and authorization with the concept of a user, called a principal, wishing to access a resource.

OAuth2 (Open Authorization): Open standard used for authentication and authorization with Internet-based systems (although it is not limited to this). Token-based which means after a user enters a correct user ID and password, they are given a token which enables them to access a resource. Token remains valid for a predetermined time and may also be accepted by other resources.

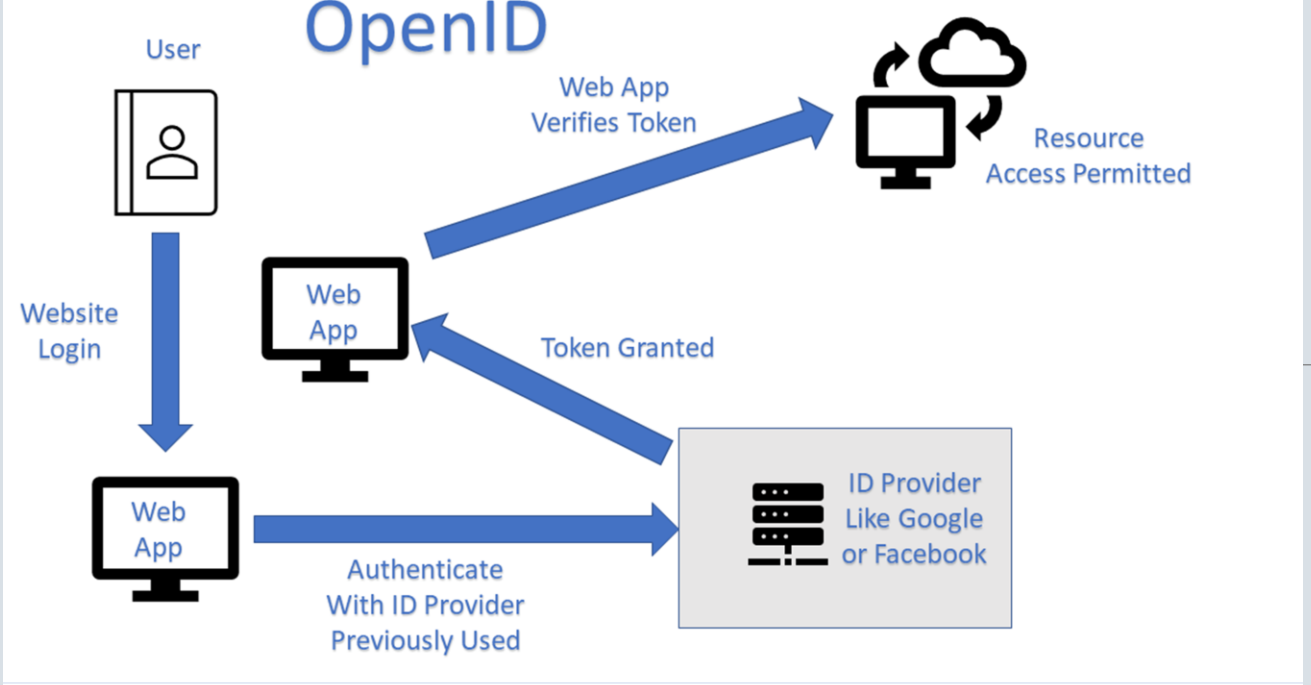
OpenID: Open standard is widely used for authentication by large Internet organizations including Google, Yahoo, PayPal, Amazon.com, Flickr, Blogger and over 1 million web sites requiring a login.

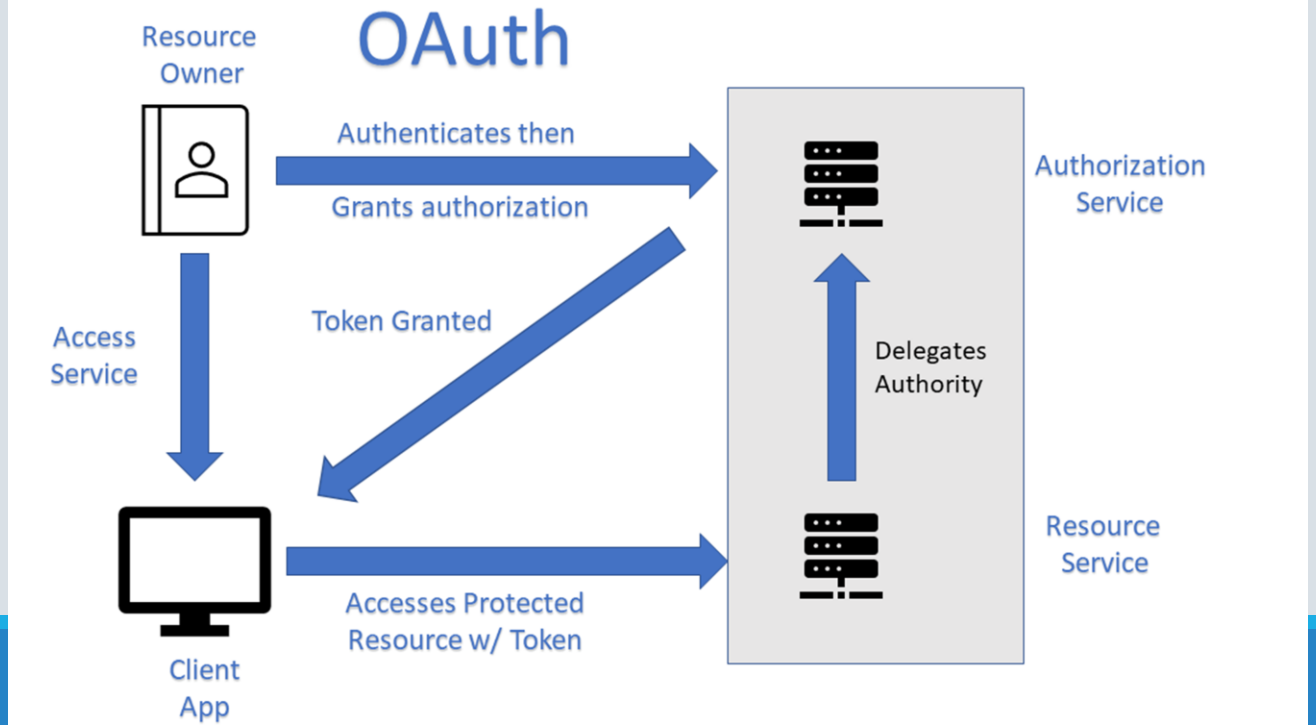


SAML AUTHENTICATION PROCESS

OpenID Approach

1) The user obtains an OpenID account which is owned by the user (e.g. myOpenID.openid.com) from an OpenID identity provider (e.g. Google).
2) The user goes to a different Website, perhaps Blogger and sees the ‘sign in with Google’ option and clicks on that button or link.
3) The Blogger website contacts Google’s OpenID service and receives an association handle.
4) The user is forwarded to the Google login page where he enters his OpenID and password.
5) Google validates the credentials and redirects the user back to Blogger with a validated token.
6) Blogger trusts the Google login and token and permits the user access to the website.





OpenID versus OAuth2

Chapter 7 Summary

Ensuring resource security is key to cloud technology success. Users must be authenticated and authorized to enter and use organizational systems in ways that ensure system protection.

Various tools, procedures and concepts are required to keep cloud computing resources and services safe.

Each cloud model (e.g. SaaS, PaaS, and IaaS) have different challenges regarding security

Cloud clients' and providers' responsibilities start and end differently with each

Identity management and various open standards for authorization and authentication can be leveraged by cloud users to provide seamless and secure use of cloud resources.

Federated identity management (FIM) and how identity management as a service (IDaaS) products are used by cloud providers and third-party vendors to make access more secure for organizations.