U19ITE07	VIRTUALIZATION AND CLOUD COMPUTING	L	T	P	C
		3	0	2	4

Pre-Requisites : U19CSE03, U19ITE04

Objectives:

- To impart the fundamentals and essentials of Cloud Computing.
- To study about virtualization and cloud resource management.
- To provide a sound foundation of the Cloud Computing Services and tools
- To be aware of different cloud platforms.
- To study the core issues of cloud security and to understand various cloud applications.

Course Outcomes:

At the end of this course students will demonstrate the ability to

CO 1 : Articulate the main concepts, key technologies, strengths and limitations of cloud computing.

CO 2 : Explain the concept of cloud resource virtualization.

CO 3 : Apply the fundamental concepts in datacenters to understand the tradeoffs in power, efficiency and cost.

CO 4 : Choose the appropriate technologies, algorithms and approaches for implementation and use of cloud

CO 5 : Create and deploy cloud applications.

Unit I INTRODUCTION 9

Introduction - Overview of Computing Paradigms - The Cloud Computing reference model - Benefits and Characteristics of Cloud- Challenges - Cloud Computing Architecture - Cloud computing stack Service Models: Infrastructure as a Service, Platform as a Service, Software as a Service- Deployment Models: Public cloud, Private cloud, Hybrid cloud – Challenges

Unit II CLOUD RESOURCE VIRTUALIZATION 9

Introduction to virtualization - Characteristics of virtualized environments- Taxonomy of virtualization techniques- Virtualization and cloud computing- Pros and cons of virtualization - Examples - Virtual Machine Provisioning and Manageability - VM Migration-Management of VM: Anatomy of cloud infrastructures - Scheduling techniques.

Unit III CLOUD PLATFORM ARCHITECTURES OVER VIRTUALIZED DATA CENTERS 9

Data-Center design and Interconnection networks - Architectural Design of Compute and Storage Clouds - Public Cloud Platforms, GAE, AWS, Azure - Inter-cloud Resource Management - Cloud Security and Trust Management.

Unit IV CLOUD PROGRAMMING AND SOFTWARE ENVIRONMENTS 9

Features of Cloud and Grid Platforms - Parallel and Distributed Programming Paradigms - Programming Support of Google App Engine - Programming on Amazon AWS and Microsoft Azure - Emerging Cloud Software Environments.Case Studies: Open stack, Heroku, and Docker Containers –Amazon EC2, Google Compute Engine.

Unit V CLOUD SECURITY & APPLICATIONS 9

Cloud Security Risks, Trust, Operating System Security, VM Security, Security of Virtualization, Security Risks Posted by Shared Images, Security Risks Posted by Management OS, Data privacy and security issues, Identity and Access Management , Access Control , Authentication in cloud computing - Applications: Scientific Applications - Business and Consumer Applications

Total Periods: 45

Unit V

CLOUD SECURITY & APPLICATIONS

Cloud Security Risks:

All companies face security risks, threats, and challenges every day. Many think these terms all mean the same thing, but they're more nuanced. Understanding the subtle differences between them will help you better protect your cloud assets.

What is the difference between risks, threats, and challenges?

- A **risk** is a potential for loss of data or a weak spot.
- A **threat** is a type of attack or adversary.
- A **challenge** is an organization's hurdles in implementing practical cloud security.

Let's consider an example: An API endpoint hosted in the cloud and exposed to the public Internet is a **risk**, the attacker who tries to access sensitive data using that API is the **threat** (along with any specific techniques they could try), and your organization's **challenge** is effectively protecting public APIs while keeping them available for legitimate users or customers who need them.

A complete cloud security strategy addresses all three aspects, so no cracks exist within the foundation. You can think of each as a different lens or angle with which to view cloud security. A solid strategy must mitigate risk (security controls), defend against threats (secure coding and deployment), and overcome challenges (implement cultural and technical solutions) for your business to use the cloud to grow securely.

4 Cloud Security Risks

You cannot completely eliminate risk; you can only manage it. Knowing common risks ahead of time will prepare you to deal with them within your environment. **What are four cloud security risks?**

. Unmanaged Attack Surface
. Human Error

- Misconfiguration
- Data Breach

1. Unmanaged Attack Surface

An attack surface is your environment's total exposure. The adoption of microservices can lead to an explosion of publicly available workload. Every workload adds to the attack surface. Without close management, you could expose your infrastructure in ways you don't know until an attack occurs.

No one wants that late-night call.

Attack surface can also include subtle information leaks that lead to an attack. For example, CrowdStrike's team of threat hunters found an attacker using sampled DNS request data gathered over public WiFi to work out the names of S3 buckets. CrowStrike stopped the attack before the attackers did any damage, but it's a great illustration of risk's ubiquitous nature. Even strong controls on the S3 buckets weren't enough to completely hide their existence. As long as you use the public Internet or cloud, you're automatically exposing an attack surface to the world.

Your business may need it to operate, but keep an eye on it.

2. Human Error

According to Gartner, through 2025, 99% of all cloud security failures will be due to some level of human error. Human error is a constant risk when building business applications. However, hosting resources on the public cloud magnifies the risk.

The cloud's ease of use means that users could be using APIs you're not aware of without proper controls and opening up holes in your perimeter. Manage human error by building strong controls to help people make the right decisions.

One final rule — don't blame people for errors. Blame the process. Build processes and guardrails to help people do the right thing. Pointing fingers doesn't help your business become more secure.

3. Misconfiguration

Cloud settings keep growing as providers add more services over time. Many companies are using more than one provider.

Providers have different default configurations, with each service having its distinct implementations and nuances. Until organizations become proficient at securing their various cloud services, adversaries will continue to exploit misconfigurations.

4. Data breaches

A data breach occurs when sensitive information leaves your possession without your knowledge or permission. Data is worth more to attackers than anything else, making it the goal of most attacks. Cloud misconfiguration and lack of runtime protection can leave it wide open for thieves to steal.

The impact of data breaches depends on the type of data stolen. Thieves sell personally identifiable information (PII) and personal health information (PHI) on the dark web to those who want to steal identities or use the information in phishing emails.

Other sensitive information, such as internal documents or emails, could be used to damage a company's reputation or sabotage its stock price. No matter the reason for stealing the data, breaches continue to be an imposing threat to companies using the cloud.

How to manage cloud security risks

Follow these tips to manage risk in the cloud:

- Perform regular risk assessments to find new risks.

- Prioritize and implement security controls to mitigate the risks you've identified (CrowdStrike can help).
- Document and revisit any risks you choose to accept.

Cloud security threats

A threat is an attack against your cloud assets that tries to exploit a risk. **What are four common threats faced by cloud security?**

. Zero-Day Exploits
. Advanced Persistent Threats
. Insider Threats
. Cyberattacks

1. Zero-day exploits

Cloud is "someone else's computer." But as long as you're using computers and software, even those run in another organization's data center, you'll encounter the threat of zero-day exploits.

Zero-day exploits target vulnerabilities in popular software and operating systems that the vendor hasn't patched. They're dangerous because even if your cloud configuration is top-notch, an attacker can exploit zero-day vulnerabilities to gain a foothold within the environment.

2. Advanced persistent threats

An advanced persistent threat (APT) is a sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network to steal sensitive data over a prolonged time.

APTs aren't a quick "drive-by" attack. The attacker stays within the environment, moving from workload to workload, searching for sensitive information to steal and sell to the highest bidder. These attacks are dangerous because they may start using a zero-day exploit and then go undetected for months.

3. Insider threats

An insider threat is a cybersecurity threat that comes from within the organization — usually by a current or former employee or other person who has direct access to the company network, sensitive data and intellectual property (IP), as well as knowledge of business processes, company policies or other information that would help carry out such an attack.

4. Cyberattacks

A cyber attack is an attempt by cybercriminals, hackers or other digital adversaries to access a computer network or system, usually for the purpose of altering, stealing, destroying or exposing information.

Common cyberattacks performed on companies include malware, phishing, DoS and DDoS, SQL Injections, and IoT based attacks.

How to handle cloud security threats

There are so many specific attacks; it's a challenge to protect against them all. But here are three guidelines to use when protecting your cloud assets from these threats and others.

- Follow secure coding standards when building microservices
- Double and triple check your cloud configuration to plug any holes
- With a secure foundation, go on the offensive with threat hunting. (CrowdStrike can help)

Operating System Security:

Security refers to providing a protection system to computer system resources such as CPU, memory, disk, software programs and most importantly data/information stored in the computer system. If a computer program is run by an unauthorized user, then he/she may cause severe damage to computer or data stored in it. So a computer system must be protected against unauthorized access, malicious access to system memory, viruses, worms etc. We're going to discuss following topics in this chapter.

- Authentication
- One Time passwords
- Program Threats
- System Threats
- Computer Security Classifications

Authentication

Authentication refers to identifying each user of the system and associating the executing programs with those users. It is the responsibility of the Operating System to create a protection system which ensures that a user who is running a particular program is authentic. Operating Systems generally identifies/authenticates users using following three ways −

- **Username / Password** − User need to enter a registered username and password with Operating system to login into the system.
- **User card/key** − User need to punch card in card slot, or enter key generated by key generator in option provided by operating system to login into the system.
- **User attribute - fingerprint/ eye retina pattern/ signature** − User need to pass his/her attribute via designated input device used by operating system to login into the system.

One Time passwords

One-time passwords provide additional security along with normal authentication. In One-Time Password system, a unique password is required every time user tries to login into the system. Once a one-time password is used, then it cannot be used again. One-time password are implemented in various ways.

- **Random numbers** − Users are provided cards having numbers printed along with corresponding alphabets. System asks for numbers corresponding to few alphabets randomly chosen.

- **Secret key** − User are provided a hardware device which can create a secret id mapped with user id. System asks for such secret id which is to be generated every time prior to login.

- **Network password** − Some commercial applications send one-time passwords to user on registered mobile/ email which is required to be entered prior to login.

Program Threats

Operating system's processes and kernel do the designated task as instructed. If a user program made these process do malicious tasks, then it is known as **Program Threats**. One of the common example of program threat is a program installed in a computer which can store and send user credentials via network to some hacker. Following is the list of some well-known program threats.

- **Trojan Horse** − Such program traps user login credentials and stores them to send to malicious user who can later on login to computer and can access system resources.

- **Trap Door** − If a program which is designed to work as required, have a security hole in its code and perform illegal action without knowledge of user then it is called to have a trap door.

Logic Bomb − Logic bomb is a situation when a program misbehaves only when certain conditions met otherwise it works as a genuine program. It is harder to detect.

-
-

Virus − Virus as name suggest can replicate themselves on computer system. They are highly dangerous and can modify/delete user files, crash systems. A virus is generatlly a small code embedded in a program. As user accesses the program, the virus starts getting embedded in other files/ programs and can make system unusable for user

-

System Threats

System threats refers to misuse of system services and network connections to put user in trouble. System threats can be used to launch program threats on a complete network called as program attack. System threats creates such an environment that operating system resources/ user files are misused. Following is the list of some well-known system threats.

-

Worm − Worm is a process which can choked down a system performance by using system resources to extreme levels. A Worm process generates its multiple copies where each copy uses system resources, prevents all other processes to get required resources. Worms processes can even shut down an entire network.

-
-

Port Scanning − Port scanning is a mechanism or means by which a hacker can detects system vulnerabilities to make an attack on the system.

-
-

Denial of Service − Denial of service attacks normally prevents user to make legitimate use of the system. For example, a user may not be able to use internet if denial of service attacks browser's content settings.

Computer Security Classifications

As per the U.S. Department of Defense Trusted Computer System's Evaluation Criteria there are four security classifications in computer systems: A, B, C, and D. This is widely used specifications to determine and model the security of systems and of security solutions. Following is the brief description of each classification.

S. N.	Classification Type & Description
1	**Type A** Highest Level. Uses formal design specifications and verification techniques. Grants a high degree of assurance of process security.
2	**Type B** Provides mandatory protection system. Have all the properties of a class C2 system. Attaches a sensitivity label to each object. It is of three types. **B1** − Maintains the security label of each object in the system. Label is used for making decisions to access control. **B2** − Extends the sensitivity labels to each system resource, such as storage objects, supports covert channels and auditing of events. **B3** − Allows creating lists or user groups for access-control to grant access or revoke access to a given named object.
3	**Type C**

Provides protection and user accountability using audit capabilities. It is of two types.

C1 − Incorporates controls so that users can protect their private information and keep other users from accidentally reading / deleting their data. UNIX versions are mostly Cl class.

C2 − Adds an individual-level access control to the capabilities of a Cl level system.

Type D

Lowest level. Minimum protection. MS-DOS, Window 3.1 fall in this category.

VM Security:

The term "Virtualized Security," sometimes known as "security virtualization," describes security solutions that are software-based and created to operate in a virtualized IT environment. This is distinct from conventional hardware-based network security, which is static and is supported by equipment like conventional switches, routers, and firewalls.

Virtualized security is flexible and adaptive, in contrast to hardware-based security. It can be deployed anywhere on the network and is frequently cloud-based so it is not bound to a specific device.

In Cloud Computing, where operators construct workloads and applications on-demand, virtualized security enables security services and functions to move around with those on-demand-created workloads. This is crucial for virtual machine security. It's crucial to protect virtualized security in cloud computing technologies such as isolating multitenant setups in public cloud settings. Because data and workloads move around a complex ecosystem including several providers, virtualized security's flexibility is useful for securing hybrid and multi-cloud settings.

Types of Hypervisors

Type-1 Hypervisors

Its functions are on unmanaged systems. Type 1 hypervisors include Lynx Secure, RTS Hypervisor, Oracle VM, Sun xVM Server, and Virtual Logic VLX. Since they are placed on bare systems, type 1 hypervisor do not have any host operating systems.

Type-2 Hypervisor

It is a software interface that simulates the hardware that a system typically communicates with. Examples of Type 2 hypervisors include containers, KVM, Microsoft Hyper V, VMWare Fusion, Virtual Server 2005 R2, Windows Virtual PC, and VMware workstation 6.0.

Type I Virtualization

In this design, the Virtual Machine Monitor (VMM) sits directly above the hardware and eavesdrops on all interactions between the VMs and the hardware. On top of the VMM is a management VM that handles other guest VM management and handles the majority of a hardware connections. The Xen system is a common illustration of this kind of virtualization design.

Type II virtualization

In these architectures, like VMware Player, allow for the operation of the VMM as an application within the host operating system (OS). I/O drivers and guest VM management are the responsibilities of the host OS.

Service Provider Security

The system's virtualization hardware shouldn't be physically accessible to anyone not authorized. Each VM can be given an access control that can only be established through the Hypervisor in order to safeguard it against unwanted access by Cloud administrators. The three fundamental tenets of access control, identity, authentication, and authorization, will prevent unauthorized data and system components from being accessed by administrators.

Hypervisor Security

The Hypervisor's code integrity is protected via a technology called Hyper safe. Securing the write-protected memory pages, expands the hypervisor implementation and prohibits coding changes. By restricting access to its code, it defends the Hypervisor from control-flow hijacking threats. The only way to carry out a VM Escape assault is through a local physical setting. Therefore, insider assaults must be

prevented in the physical Cloud environment. Additionally, the host OS and the interaction between the guest machines need to be configured properly.

Virtual Machine Security

The administrator must set up a program or application that prevents virtual machines from consuming additional resources without permission. Additionally, a lightweight process that gathers logs from the VMs and monitors them in real-time to repair any VM tampering must operate on a Virtual Machine. Best security procedures must be used to harden the guest OS and any running applications. These procedures include setting up firewalls, host intrusion prevention systems (HIPS), anti-virus and anti-spyware programmers, online application protection, and log monitoring in guest operating systems.

Guest Image Security

A policy to control the creation, use, storage, and deletion of images must be in place for organizations that use virtualization. To find viruses, worms, spyware, and rootkits that hide from security software running in a guest OS, image files must be analyzed.

Benefits of Virtualized Security

Virtualized security is now practically required to meet the intricate security requirements of a virtualized network, and it is also more adaptable and effective than traditional physical security.

Cost-Effectiveness: Cloud computing's virtual machine security enables businesses to keep their networks secure without having to significantly raise their expenditures on pricey proprietary hardware. Usage-based pricing for cloud-based virtualized security services can result in significant savings for businesses that manage their resources effectively.

Flexibility: It is essential in a virtualized environment that security operations can follow workloads wherever they go. A company is able to profit fully from virtualization while simultaneously maintaining data security thanks to the protection it offers across various data centers, in multi-cloud, and hybrid-cloud environments.

Operational Efficiency: Virtualized security can be deployed more quickly and easily than hardware-based security because it doesn't require IT, teams, to set up and configure several hardware appliances. Instead, they may quickly scale security systems by setting them up using centralized software. Security-related duties can be automated when security technology is used, which frees up more time for IT employees.

Regulatory Compliance: Virtual machine security in cloud computing is a requirement for enterprises that need to maintain regulatory compliance because traditional hardware-based security is static and unable to keep up with the demands of a virtualized network.

Virtualization Machine Security Challenges

As we previously covered, buffer overflows are a common component of classical network attacks. Trojan horses, worms, spyware, rootkits, and DoS attacks are examples of malware.

In a cloud context, more recent assaults might be caused via VM rootkits, hypervisor malware, or guest hopping and hijacking. Man-in-the-middle attacks against VM migrations are another form of attack. Typically, passwords or sensitive information are stolen during passive attacks. Active attacks could alter the kernel's data structures, seriously harming cloud servers.

HIDS or NIDS are both types of IDSs. To supervise and check the execution of code, use programmed shepherding. The RIO dynamic optimization infrastructure, the v Safe and v Shield tools from VMware, security compliance for hypervisors, and Intel vPro technology are some further protective solutions.

Four Steps to ensure VM Security in Cloud Computing

Protect Hosted Elements by Segregation

To secure virtual machines in cloud computing, the first step is to segregate the newly hosted components. Let's take an example where three features that are now running on an edge device may be placed in the cloud either as part of a private subnetwork that is invisible or as part of the service data plane, with addresses that are accessible to network users.

All Components are Tested and Reviewed

Before allowing virtual features and functions to be implemented, you must confirm that they comply with security standards as step two of cloud-virtual security. Virtual networking is subject to outside attacks, which can be dangerous, but insider attacks can be disastrous. When a feature with a backdoor security flaw is added to a service, it becomes a part of the infrastructure of the service and is far more likely to have unprotected attack paths to other infrastructure pieces.

Separate Management APIs to Protect the Network

The third step is to isolate service from infrastructure management and orchestration. Because they are created to regulate features, functions, and service behaviors,

management APIs will always pose a significant risk. All such APIs should be protected, but the ones that keep an eye on infrastructure components that service users should never access must also be protected.

Keep Connections Secure and Separate

The fourth and last aspect of cloud virtual network security is to make sure that connections between tenants or services do not cross over into virtual networks. Virtual Networking is a fantastic approach to building quick connections to scaled or redeployed features, but each time a modification is made to the virtual network, it's possible that an accidental connection will be made between two distinct services, tenants, or feature/function deployments. A data plane leak, a link between the actual user networks, or a management or control leak could result from this, allowing one user to affect the service provided to another.

Security of Virtualization:

Virtualized security, or security virtualization, refers to security solutions that are software-based and designed to work within a virtualized IT environment. This differs from traditional, hardware-based network security, which is static and runs on devices such as traditional firewalls, routers, and switches.

In contrast to hardware-based security, virtualized security is flexible and dynamic. Instead of being tied to a device, it can be deployed anywhere in the network and is often cloud-based. This is key for virtualized networks, in which operators spin up workloads and applications dynamically; virtualized security allows security services and functions to move around with those dynamically created workloads.

Cloud security considerations (such as isolating multitenant environments in public cloud environments) are also important to virtualized security. The flexibility of virtualized security is helpful for securing hybrid and multi-cloud environments, where data and workloads migrate around a complicated ecosystem involving multiple vendors.

What are the benefits of virtualized security?

Virtualized security is now effectively necessary to keep up with the complex security demands of a virtualized network, plus it's more flexible and efficient than traditional physical security. Here are some of its specific benefits:

Cost-effectiveness: Virtualized security allows an enterprise to maintain a secure network without a large increase in spending on expensive proprietary hardware. Pricing for cloud-based virtualized security services is often determined by usage, which can mean additional savings for organizations that use resources efficiently.

Flexibility: Virtualized security functions can follow workloads anywhere, which is crucial in a virtualized environment. It provides protection across multiple data centers and in multi-cloud and hybrid cloud environments, allowing an organization to take advantage of the full benefits of virtualization while also keeping data secure.

Operational efficiency:Quicker and easier to deploy than hardware-based security, virtualized security doesn't require IT teams to set up and configure multiple hardware appliances. Instead, they can set up security systems through centralized software, enabling rapid scaling. Using software to run security technology also allows security tasks to be automated, freeing up additional time for IT teams.

Regulatory compliance:Traditional hardware-based security is static and unable to keep up with the demands of a virtualized network, making virtualized security a necessity for organizations that need to maintain regulatory compliance.

How does virtualized security work?

Virtualized security can take the functions of traditional security hardware appliances (such as firewalls and antivirus protection) and deploy them via software. In addition, virtualized security can also perform additional security functions. These functions are only possible due to the advantages of virtualization, and are designed to address the specific security needs of a virtualized environment.

For example, an enterprise can insert security controls (such as encryption) between the application layer and the underlying infrastructure, or use strategies such as micro-segmentation to reduce the potential attack surface.

Virtualized security can be implemented as an application directly on a bare metal hypervisor (a position it can leverage to provide effective application monitoring) or as a hosted service on a virtual machine. In either case, it can be quickly deployed where it is most effective, unlike physical security, which is tied to a specific device.

What are the risks of virtualized security?

The increased complexity of virtualized security can be a challenge for IT, which in turn leads to increased risk. It's harder to keep track of workloads and applications in

a virtualized environment as they migrate across servers, which makes it more difficult to monitor security policies and configurations. And the ease of spinning up virtual machines can also contribute to security holes.

It’s important to note, however, that many of these risks are already present in a virtualized environment, whether security services are virtualized or not. Following enterprise security best practices (such as spinning down virtual machines when they are no longer needed and using automation to keep security policies up to date) can help mitigate such risks.

How is physical security different from virtualized security?

Traditional physical security is hardware-based, and as a result, it’s inflexible and static. The traditional approach depends on devices deployed at strategic points across a network and is often focused on protecting the network perimeter (as with a traditional firewall). However, the perimeter of a virtualized, cloud-based network is necessarily porous and workloads and applications are dynamically created, increasing the potential attack surface.

Traditional security also relies heavily upon port and protocol filtering, an approach that’s ineffective in a virtualized environment where addresses and ports are assigned dynamically. In such an environment, traditional hardware-based security is not enough; a cloud-based network requires virtualized security that can move around the network along with workloads and applications.

What are the different types of virtualized security?

There are many features and types of virtualized security, encompassing network security, application security, and cloud security. Some virtualized security technologies are essentially updated, virtualized versions of traditional security technology (such as next-generation firewalls). Others are innovative new technologies that are built into the very fabric of the virtualized network.

Some common types of virtualized security features include:

Segmentation, or making specific resources available only to specific applications and users. This typically takes the form of controlling traffic between different network segments or tiers.

Micro-segmentation, or applying specific security policies at the workload level to create granular secure zones and limit an attacker's ability to move through the network. Micro-segmentation divides a data center into segments and allows IT teams to define security controls for each segment individually, bolstering the data center's resistance to attack.

Isolation, or separating independent workloads and applications on the same network. This is particularly important in a multitenant public cloud environment, and can also be used to isolate virtual networks from the underlying physical infrastructure, protecting the infrastructure from attack.

Security Risks Posted by Shared Images:

Security risks posed by shared images Image sharing is critical for the IaaS cloud delivery model. For example, a user of AWS has the option to choose between 1.Amazon Machine Images (AMIs) accessible through the Quick Start. 2.Community AMI menus of the EC2 service. Many of the images analyzed by a recent report allowed a user to undelete files, recover credentials, private keys, or other types of sensitive information with little effort and using standard tools. A software vulnerability audit revealed that 98% of the Windows AMIs and 58% of Linux AMIs audited had critical vulnerabilities. Security risks: Backdoors and leftover credentials. Unsolicited connections. Malware. Example:- Its discovered that all images shared via a Google Hangout Chat are not private to the parties on the hangout/chat! It turns out, anyone can view any images you share via Hangout without any sweat. This is the proof; From your Gmail, Pop our Hangout and Start a Hangout Chat with a friend. Share an image

with them either as an Upload Image from Computer (works as well for image stored in Drive, photos to and send to the other party The person can preview the image through the Hangout or can click on the image to view the full image in a new tab/windows image. The link Opens in New tab/Window. Copy the Image URL and Open a New Browser/Incognito/Private session and paste. You are able to view the Image. Which means, the private image you shared in via Google Hangout is actually available publicly and anyone with sufficient acknowledge of URLs can view your

images. TOPIC-2:- Security risks posed by a management OS A virtual machine monitor, or hypervisor, is considerably smaller than an operating system, e.g., the XenVMM has ~ 60,000 lines of code. The Trusted Computer Base (TCB) of a cloud computing environment includes not only the hypervisor but also the management OS. The management OS supports administrative tools, live migration, device drivers, and device emulators. EXAMPLE:- Just as technology and software change and advance in no time at all, so too do cyber threats. Viruses, malware and attacks get more and more sophisticated. Plus, cybercriminals know (and can exploit) the weaknesses in outdated software.

So, if your outdated software includes the use, storage or application of data, that data becomes at risk. Your systems will be more vulnerable to ransomware attacks, malware and data breaches. Out of date software, then, can give attackers a back door into the rest of your systems. Topic-3:- Terra -a trusted virtual machine monitor Novel ideas for a trusted virtual machine monitor (TVMM): It should support not only traditional operating systems, by exporting the hardware abstraction for open-box platforms, but also the abstractions for closed-box platforms (do not allow the contents of the system to be either manipulated or inspected by the platform owner).

An application should be allowed to build its software stack based on its needs. Applications requiring a very high level of security should run under a very thin OS supporting only the functionality required by the application and the ability to boot. At the other end of the spectrum are applications demanding low assurance, but a rich set of OS features; such applications need a commodity operating system. Provide trusted paths from a user to an application. Such a path allows a human user to determine with certainty the identity of the VM it is interacting with and allows the VM to verify the identity of the human user. Deny the platform administrator the root access. Support attestation, the ability of an application running in a closed-box to gain trust from a remote party, by cryptographically identifying itself.

Security Risks Posted by Management OS:

The security of an organization is the greatest concern of the people working at the organization. Safety and security are the pillars of cyber technology. It is hard to imagine the cyber world without thinking about security. The architecture of security is thus a very important aspect of the organization. The OSI (Open Systems Interconnection) Security Architecture defines a systematic approach to providing security at each layer. It defines security services and security mechanisms that can be used at each of the seven layers of the OSI model to provide security for data transmitted over a network. These security services and mechanisms help to ensure the confidentiality, integrity, and availability of the data. OSI architecture is internationally acceptable as it lays the flow of providing safety in an organization.

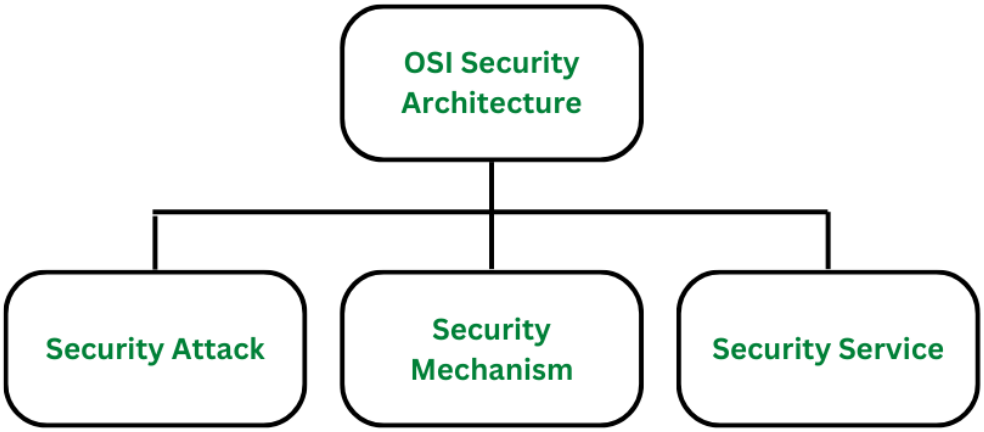
OSI Security Architecture focuses on these concepts:

Security Attack:

Security mechanism: A security mechanism is a means of protecting a system, network, or device against unauthorized access, tampering, or other security threats.

Security Service:

Classification of OSI Security Architecture



Classification of OSI Security Architecture

OSI Security Architecture is categorized into three broad categories namely Security Attacks, Security mechanisms, and Security Services. We will discuss each in detail:

1. Security Attacks:

A security attack is an attempt by a person or entity to gain unauthorized access to disrupt or compromise the security of a system, network, or device. These are defined as the actions that put at risk an organization’s safety. They are further classified into 2 sub-categories:

A. Passive Attack:

Attacks in which a third-party intruder tries to access the message/ content/ data being shared by the sender and receiver by keeping a close watch on the transmission or eave-dropping the transmission is called Passive Attacks. These types of attacks involve the attacker observing or monitoring system, network, or device activity without actively disrupting or altering it. Passive attacks are typically focused on gathering information or intelligence, rather than causing damage or disruption.

Here, both the sender and receiver have no clue that their message/ data is accessible to some third-party intruder. The message/ data transmitted remains in its usual form without any deviation from its usual behavior. This makes passive attacks very risky as there is no information provided about the attack happening in the communication process. One way to prevent passive attacks is to encrypt the message/data that needs to be transmitted, this will prevent third-party intruders to use the information though it would be accessible to them.

Passive attacks are further divided into two parts based on their behavior:

Eavesdropping: This involves the attacker intercepting and listening to communications between two or more parties without their knowledge or consent. Eavesdropping can be performed using a variety of techniques, such as packet sniffing, or man-in-the-middle attacks.

Traffic analysis: This involves the attacker analyzing network traffic patterns and metadata to gather information about the system, network, or device. Here the intruder can’t read the message but only understand the pattern and length of encryption. Traffic analysis can be performed using a variety of techniques, such as network flow analysis, or protocol analysis.

B. Active Attacks:

Active attacks refer to types of attacks that involve the attacker actively disrupting or altering system, network, or device activity. Active attacks are typically focused on causing damage or disruption, rather than gathering information or intelligence. Here, both the sender and receiver have no clue that their message/ data is modified by some third-party intruder. The message/ data transmitted doesn’t remain in its usual form and shows deviation from its usual behavior. This makes active attacks dangerous as there is no information provided of the attack happening in the

communication process and the receiver is not aware that the data/ message received is not from the sender.

Active attacks are further divided into four parts based on their behavior:

Masquerade is a type of attack in which the attacker pretends to be an authentic sender in order to gain unauthorized access to a system. This type of attack can involve the attacker using stolen or forged credentials, or manipulating authentication or authorization controls in some other way.

Replay is a type of active attack in which the attacker intercepts a transmitted message through a passive channel and then maliciously or fraudulently replays or delays it at a later time.

Modification of Message involves the attacker modifying the transmitted message and making the final message received by the receiver look like it’s not safe or non-meaningful. This type of attack can be used to manipulate the content of the message or to disrupt the communication process.

Denial of service (DoS) attacks involve the attacker sending a large volume of traffic to a system, network, or device in an attempt to overwhelm it and make it unavailable to legitimate users.

2. Security Mechanism

The mechanism that is built to identify any breach of security or attack on the organization, is called a security mechanism. Security Mechanisms are also responsible for protecting a system, network, or device against unauthorized access, tampering, or other security threats. Security mechanisms can be implemented at various levels within a system or network and can be used to provide different types of security, such as confidentiality, integrity, or availability.

Some examples of security mechanisms include:

Encipherment (Encryption) involves the use of algorithms to transform data into a form that can only be read by someone with the appropriate decryption key. Encryption can be used to protect data it is transmitted over a network, or to protect data when it is stored on a device.

Digital signature is a security mechanism that involves the use of cryptographic techniques to create a unique, verifiable identifier for a digital document or message, which can be used to ensure the authenticity and integrity of the document or message.

Traffic padding is a technique used to add extra data to a network traffic stream in an attempt to obscure the true content of the traffic and make it more difficult to analyze.

Routing control allows the selection of specific physically secure routes for specific data transmission and enables routing changes, particularly when a gap in security is suspected.

3. Security Services:

Security services refer to the different services available for maintaining the security and safety of an organization. They help in preventing any potential risks to security. Security services are divided into 5 types:

Authentication is the process of verifying the identity of a user or device in order to grant or deny access to a system or device.

Access control involves the use of policies and procedures to determine who is allowed to access specific resources within a system.

Data Confidentiality is responsible for the protection of information from being accessed or disclosed to unauthorized parties.

Data integrity is a security mechanism that involves the use of techniques to ensure that data has not been tampered with or altered in any way during transmission or storage.

Non- repudiation involves the use of techniques to create a verifiable record of the origin and transmission of a message, which can be used to prevent the sender from denying that they sent the message.

Benefits of OSI Architecture:

Below listed are the benefits of OSI Architecture in an organization:

1. Providing Security:

OSI Architecture in an organization provides the needed security and safety, preventing potential threats and risks.

Managers can easily take care of the security and there is hassle-free security maintenance done through OSI Architecture.

2. Organising Task:

The OSI architecture makes it easy for managers to build a security model for the organization based on strong security principles.

Managers get the opportunity to organize tasks in an organization effectively.

3. Meets International Standards:

Security services are defined and recognized internationally meeting international standards.

The standard definition of requirements defined using OSI Architecture is globally accepted.

Data privacy and security issues

Security Issues in Cloud Computing :

There is no doubt that Cloud Computing provides various Advantages but there are also some security issues in cloud computing. Below are some following Security Issues in Cloud Computing as follows.

Data Loss –

Data Loss is one of the issues faced in Cloud Computing. This is also known as Data Leakage. As we know that our sensitive data is in the hands of Somebody else, and we don't have full control over our database. So, if the security of cloud service is to break by hackers then it may be possible that hackers will get access to our sensitive data or personal files.

Interference of Hackers and Insecure API's –

As we know, if we are talking about the cloud and its services it means we are talking about the Internet. Also, we know that the easiest way to communicate with Cloud is using API. So it is important to protect the Interface's and API's which are used by an external user. But also in cloud computing, few services are available in the public domain which are the vulnerable part of Cloud Computing because it may be possible that these services are accessed by some third parties. So, it may be possible that with the help of these services hackers can easily hack or harm our data.

User Account Hijacking –

Account Hijacking is the most serious security issue in Cloud Computing. If somehow the Account of User or an Organization is hijacked by a hacker then the hacker has full authority to perform Unauthorized Activities.

Changing Service Provider –

Vendor lock-In is also an important Security issue in Cloud Computing. Many organizations will face different problems while shifting from one vendor to another.

For example, An Organization wants to shift from AWS Cloud to Google Cloud Services then they face various problems like shifting of all data, also both cloud services have different techniques and functions, so they also face problems regarding that. Also, it may be possible that the charges of AWS are different from Google Cloud, etc.

Lack of Skill –

While working, shifting to another service provider, need an extra feature, how to use a feature, etc. are the main problems caused in IT Company who doesn't have skilled Employees. So it requires a skilled person to work with Cloud Computing.

Denial of Service (DoS) attack –

This type of attack occurs when the system receives too much traffic. Mostly DoS attacks occur in large organizations such as the banking sector, government sector, etc. When a DoS attack occurs, data is lost. So, in order to recover data, it requires a great amount of money as well as time to handle it.

Security Issues in Cloud Computing :

There is no doubt that Cloud Computing provides various Advantages but there are also some security issues in cloud computing. Below are some following Security Issues in Cloud Computing as follows.

Data Loss –

Data Loss is one of the issues faced in Cloud Computing. This is also known as Data Leakage. As we know that our sensitive data is in the hands of Somebody else, and we don't have full control over our database. So, if the security of cloud service is to break by hackers then it may be possible that hackers will get access to our sensitive data or personal files.

Interference of Hackers and Insecure API's –

As we know, if we are talking about the cloud and its services it means we are talking about the Internet. Also, we know that the easiest way to communicate with Cloud is using API. So it is important to protect the Interface's and API's which are used by an external user. But also in cloud computing, few services are available in the public domain which are the vulnerable part of Cloud Computing because it may be possible that these services are accessed by some third parties. So, it may be possible that with

the help of these services hackers can easily hack or harm our data.

User Account Hijacking –

Account Hijacking is the most serious security issue in Cloud Computing. If somehow the Account of User or an Organization is hijacked by a hacker then the hacker has full authority to perform Unauthorized Activities.

Changing Service Provider –

Vendor lock-In is also an important Security issue in Cloud Computing. Many organizations will face different problems while shifting from one vendor to another. For example, An Organization wants to shift from AWS Cloud to Google Cloud Services then they face various problems like shifting of all data, also both cloud services have different techniques and functions, so they also face problems regarding that. Also, it may be possible that the charges of AWS are different from Google Cloud, etc.

Lack of Skill –

While working, shifting to another service provider, need an extra feature, how to use a feature, etc. are the main problems caused in IT Company who doesn't have skilled Employees. So it requires a skilled person to work with Cloud Computing.

Denial of Service (DoS) attack –

This type of attack occurs when the system receives too much traffic. Mostly DoS attacks occur in large organizations such as the banking sector, government sector, etc. When a DoS attack occurs, data is lost. So, in order to recover data, it requires a great amount of money as well as time to handle it.

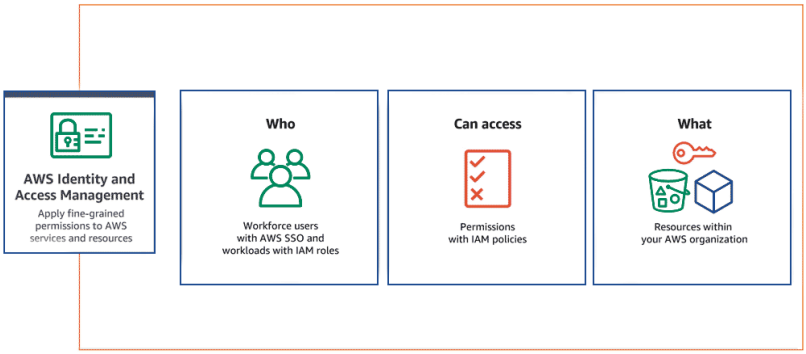
Identity and Access Management

In a recent study by Verizon, 63% of the confirmed data breaches are due to either weak, stolen, or default passwords used. There is a saying in the cybersecurity world that goes like this "No matter how good your chain is it's only as strong as your weakest link." and exactly hackers use the weakest links in the organization to infiltrate. They usually use phishing attacks to infiltrate an organization and if they get at least one person to fall for it, it's a serious turn of events from thereon. They use the

stolen credentials to plant back doors, install malware or exfiltrate confidential data, all of which will cause serious losses for an organization.

How Identity and Access Management Works?

AWS(Amazon Web Services) will allows you to maintain the fine-grained permissions to the AWS account and the services provided Amazon cloud. You can manage the permissions to the individual users or you can manage the permissions to certain users as group and roles will helps you to manage the permissions to the resources.



What Is Identity and Access Management(IAM)?

Identity and Access Management (IAM) is a combination of policies and technologies that allows organizations to identify users and provide the right form of access as and when required. There has been a burst in the market with new applications, and the requirement for an organization to use these applications has increased drastically. The services and resources you want to access can be specified in IAM. IAM doesn't provide any replica or backup. IAM can be used for many purposes such as, if one want's to control access of individual and group access for your AWS resources. With IAM policies, managing permissions to your workforce and systems to ensure least-privilege permissions becomes easier. The AWS IAM is a global service.

Components of Identity and Access Management (IAM)

Users

Roles

Groups

Policies

With these new applications being created over the cloud, mobile and on-premise can hold sensitive and regulated information. It's no longer acceptable and feasible to

just create an Identity server and provide access based on the requests. In current times an organization should be able to track the flow of information and provide least privileged access as and when required, obviously with a large workforce and new applications being added every day it becomes quite difficult to do the same. So organizations specifically concentrate on managing identity and its access with the help of a few IAM tools. It's quite obvious that it is very difficult for a single tool to manage everything but there are multiple IAM tools in the market that help the organizations with any of the few services given below.

IAM Identities Classified As

IAM Users

IAM Groups

IAM Roles

Root user

The root user will automatically be created and granted unrestricted rights. We can create an admin user with fewer powers to control the entire Amazon account.

IAM Users

We can utilize IAM users to access the AWS Console and their administrative permissions differ from those of the Root user and if we can keep track of their login information.

Example

With the aid of IAM users, we can accomplish our goal of giving a specific person access to every service available in the Amazon dashboard with only a limited set of permissions, such as read-only access. Let's say user-1 is a user that I want to have read-only access to the EC2 instance and no additional permissions, such as create, delete, or update. By creating an IAM user and attaching user-1 to that IAM user, we may allow the user access to the EC2 instance with the required permissions.

IAM Groups

A group is a collection of users, and a single person can be a member of several groups. With the aid of groups, we can manage permissions for many users quickly and efficiently.

Example

Consider two users named user-1 and user-2. If we want to grant user-1 specific permissions, such as the ability to delete, create, and update the auto-calling group only, and if we want to grant user-2 all the necessary permissions to maintain the

auto-scaling group as well as the ability to maintain EC2,S3 we can create groups and add this user to them. If a new user is added, we can add that user to the required group with the necessary permissions.

IAM Roles

While policies cannot be directly given to any of the services accessible through the Amazon dashboard, IAM roles are similar to IAM users in that they may be assumed by anybody who requires them. By using roles, we can provide AWS Services access rights to other AWS Services.

Example

Consider Amazon EKS. In order to maintain an autoscaling group, AWS eks needs access to EC2 instances. Since we can't attach policies directly to the eks in this situation, we must build a role and then attach the necessary policies to that specific role and attach that particular role to EKS.

IAM Policies

IAM Policies can manage access for AWS by attaching them to the IAM Identities or resources IAM policies defines permissions of AWS identities and AWS resources when a user or any resource makes a request to AWS will validate these policies and confirms whether the request to be allowed or to be denied. AWS policies are stored in the form of Jason format the number of policies to be attached to particular IAM identities depends upon no.of permissions required for one IAM identity. IAM identity can have multiple policies attached to them.

Access management for AWS resourcesIdentity management

Access management

Federation

RBAC/EM

Multi-Factor authentication

Access governance

Customer IAM

API Security

IDaaS – Identity as a service

Granular permissions

Privileged Identity management – PIM (PAM or PIM is the same)

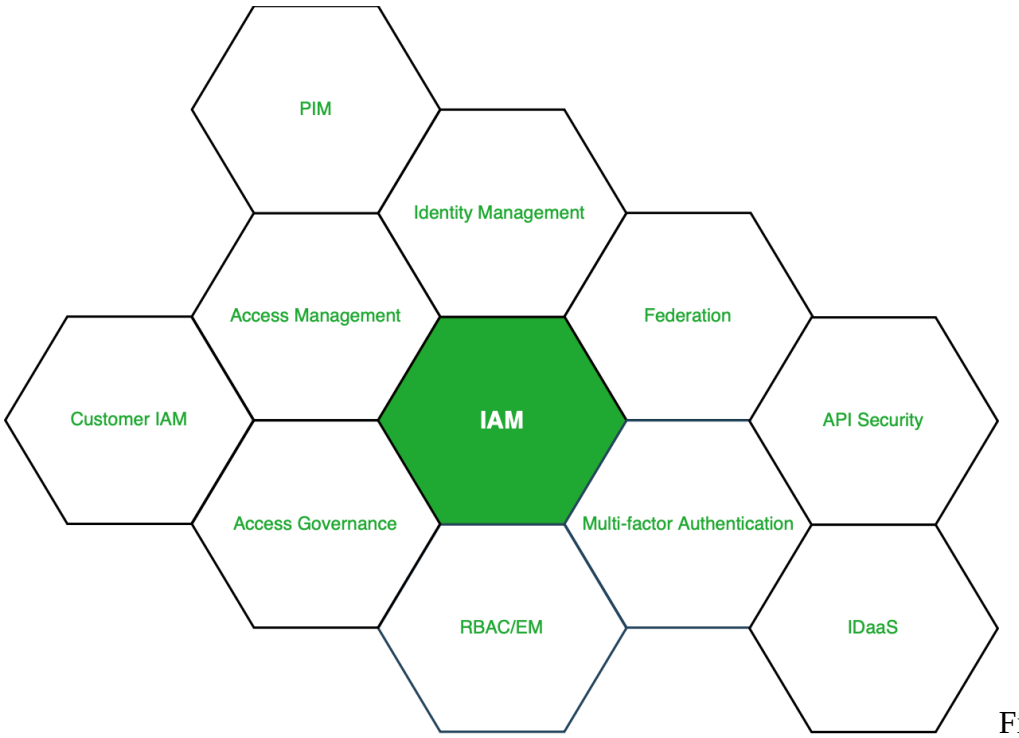


Figure – Services under IAM

More About the Services: Looking into the services on brief, Identity management is purely responsible for managing the identity lifecycle. Access management is responsible for the access to the resources, access governance is responsible for access request grant and audits. PIM or PAM is responsible for managing all the privileged access to the resources. The remaining services either help these services or help in increasing the productivity of these services.

Market for IAM: Current situation of the market, there are three market leaders (Okta, SailPoint and Cyberark) who master one of the three domains (Identity Management, Identity Governance and Privilege access management), according to Gartner and Forrester reports. These companies have developed solutions and are still developing new solutions that allow an organization to manage identity and its access securely without any hindrances in the workflow. There are other IAM tools, Beyond Trust, Ping, One login, Centrify, Azure Active Directory, Oracle Identity Cloud Services and many more.

Use cases Identity and Access Management(IAM)

Resource Access Control: Identity and access management (IAM) will allows you to manage the permissions to the resources in the AWS cloud like users who can access particular serivce to which extent and also instead of mantaing the permissions individually you can manage the permissions to group of users at a time.

Managing permissions: For example you want to assign an permission to the user that he/her can only perform restart the instance task on AWS EC2 instance then you can do using AWS IAM.

Implemneting role-based access control(RBAC): Identity and Access Management(IAM) will helps you to manage the permissions based on roles Roles will helps to assign the the permissions to the resourcesw in the AWS like which resources can access the another resource according to the requirement.

Enabling single sign-on (SSO): Identity and Access Management will helps you to maintain the same password and user name which will reduce the effort of remembering the different password.

IAM Features

Shared Access to your Account: A team working on a project can easily share resources with the help of the shared access feature.

Free of cost: IAM feature of the AWS account is free to use & charges are added only when you access other Amazon web services using IAM users.

Have Centralized control over your AWS account: Any new creation of users, groups, or any form of cancellation that takes place in the AWS account is controlled by you, and you have control over what & how data can be accessed by the user.

Grant permission to the user: As the root account holds administrative rights, the user will be granted permission to access certain services by IAM.

Multifactor Authentication: Additional layer of security is implemented on your account by a third party, a six-digit number that you have to put along with your password when you log into your accounts.

Accessing IAM

AWS Console: Access the AWS IAM through the GUI. It is an web application provided by the AWS(Amazon Web Application) it is an console where users can access the aws console

AWS Command Line Tools: Instead of accessing the console you can access y the command line interface (CLI) to access the AWS web application. You can autiomate the process by using the Scripts.

IAM Query API: Programmatic access to IAM and AWS by allowing you to send HTTPS requests directly to the service.

FAQ’s On Identity and Access Maagement

1. What Are The 4 Components Of Identity Access Management?

The 4 four major components of dentity Access Management are

Identity

Authentication

Authorization

Auditing

2. What Is The Role Of Identity Access Management?

Identity and access management (IAM) is a security discipline that enables organizations to manage digital identities and control user access to critical information and systems.

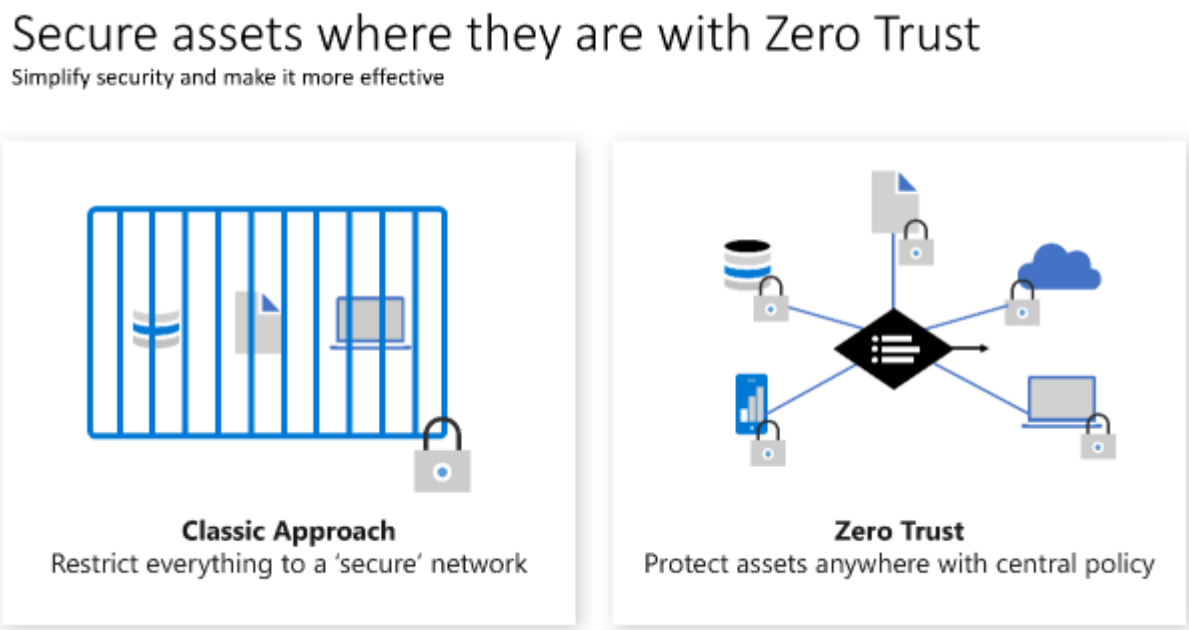
Access Control

Access control is the part of security that people experience first and most often. They see it when they sign in to their computers and mobile phones, when they share a file or try to access an application, and when they use an ID card key to enter a building or room. While access control isn't everything in security, it's critically important, and it requires proper attention so that both the user experience and the security assurances are right.

Watch the following video to learn how you can develop an access control strategy that meets your specific needs.

From security perimeter to zero trust

The traditional approach of access control for IT has been based on restricting access to a corporate network and then supplementing it with more controls as appropriate. This model restricts all resources to a corporate owned network connection and has become too restrictive to meet the needs of a dynamic enterprise.



Organizations must embrace a zero trust approach to access control as they embrace remote work and use cloud technology to digitally transform their business model, customer engagement model, employee engagement, and empowerment model.

Zero trust principles help establish and continuously improve security assurances, while maintaining flexibility to keep pace with this new world. Most zero trust journeys start with access control and focus on identity as a preferred and primary control while they continue to embrace network security technology as a key element. Network technology and the security perimeter tactic are still present in a modern access control model, but they aren't the dominant and preferred approach in a complete access control strategy.

Modern access control

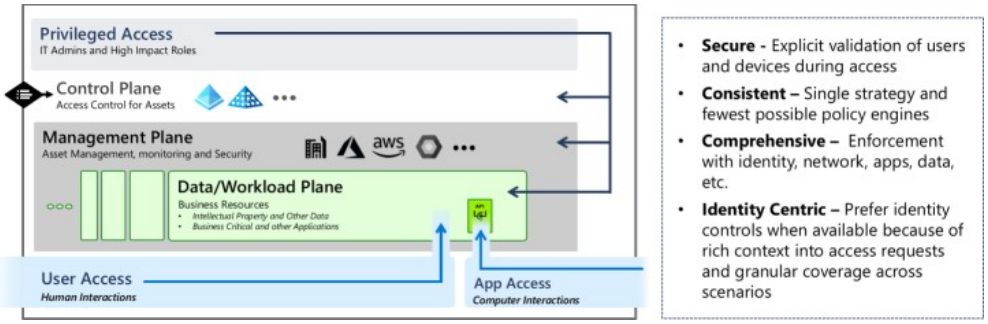
Organizations should develop an access control strategy that:

Is comprehensive and consistent.

Rigorously applies security principles throughout the technology stack.

Is flexible enough to meet the needs of the organization.

This diagram illustrates all of the different elements that an organization must consider for an access control strategy for multiple workloads, multiple clouds, various business sensitivity levels, and access by both people and devices.



A good access control strategy goes beyond a single tactic or technology. It requires a pragmatic approach that embraces the right technology and tactics for each scenario.

Modern access control must meet the productivity needs of the organization, and also be:

Secure: Explicitly validate the trust of users and devices during access requests, using all available data and telemetry. This configuration makes it more difficult for attackers to impersonate legitimate users without being detected. Also, the access control strategy should focus on eliminating unauthorized escalation of privilege, for example, granting a privilege that can be used to get higher privileges. For more information on protecting privileged access, see Securing privileged access.

Consistent: Ensure that security assurances are applied consistently and seamlessly across the environment. This standard improves the user experience and removes opportunities for attackers to sneak in through weaknesses in a disjointed or highly complex access control implementation. You should have a single access control strategy that uses the fewest number of policy engines to avoid configuration inconsistencies and configuration drift.

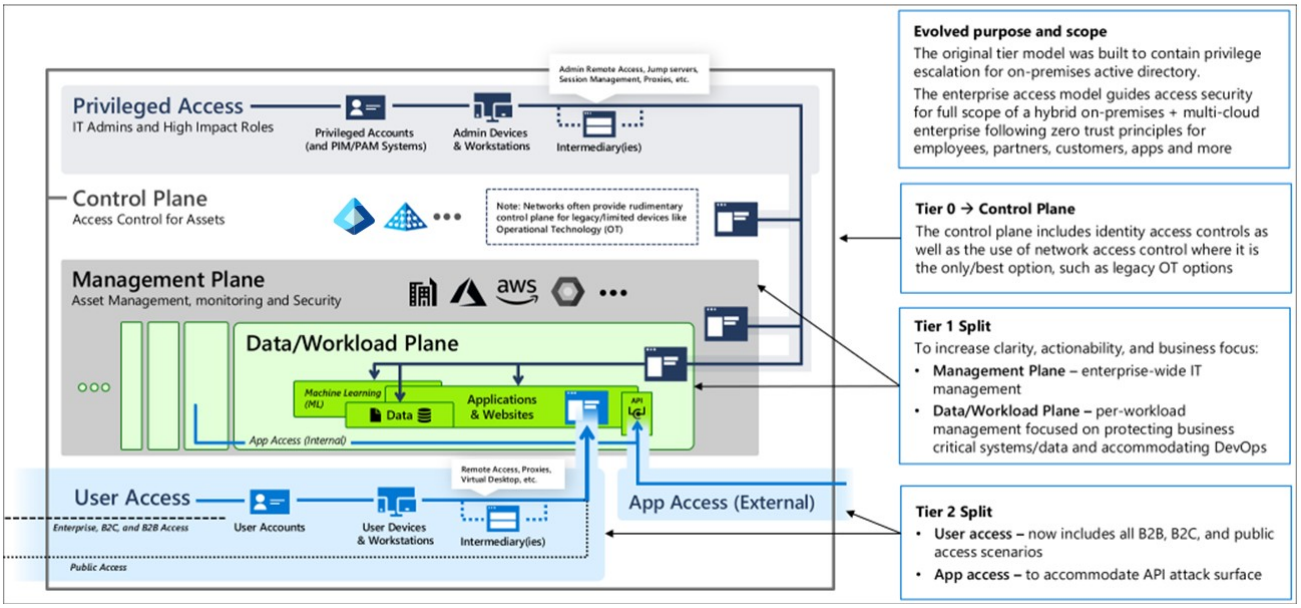
Comprehensive: Enforcement of access policy should be done as closely to the resources and access pathways as possible. This configuration improves security coverage, and helps security fit smoothly into scenarios and expectations of users. Take advantage of security controls for data, applications, identity, networks, and databases to drive policy enforcement closer to the business assets of value.

Identity-centric: Prioritize the use of identity and related controls when available. Identity controls provide rich context into access requests, and application context that isn't available from raw network traffic. Networking controls are still important, and sometimes the only available option (such as in operational technology environments), but identity should always be the first choice if available. A failure dialog during application access from the identity layer will be more precise and

informative than a network traffic block, making it more likely the user can correct the issue without a costly help desk call.

Enterprise access model

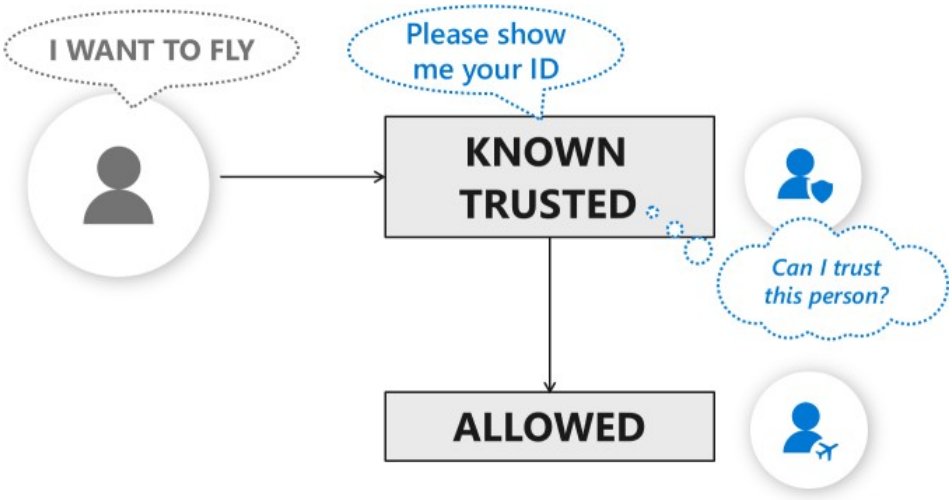
The enterprise access model is a comprehensive access model based on zero trust. This model addresses all types of access by internal and external users, services, applications, and privileged accounts with administrative access to systems.



The enterprise access model is described in detail in Enterprise access model

Known, trusted, allowed

One helpful perspective on the zero trust transformation of access control is that it shifts from a static two-step process of authentication and authorization, to a dynamic three-step process called known, trusted, allowed:



Known: Authentication that ensures you are who you say you are. This process is analogous to the physical process of checking a government-issued photo identification document.

Trusted: Validation that the user or device is trustworthy enough to access the resource. This process is analogous to security at an airport that screens all passengers for security risks before allowing them to enter the airport.

Allowed: Granting of specific rights and privileges for the application, service, or data. This process is analogous to an airline that manages where passengers are going, what cabin they sit in (first class, business class, or coach), and whether they have to pay for luggage.

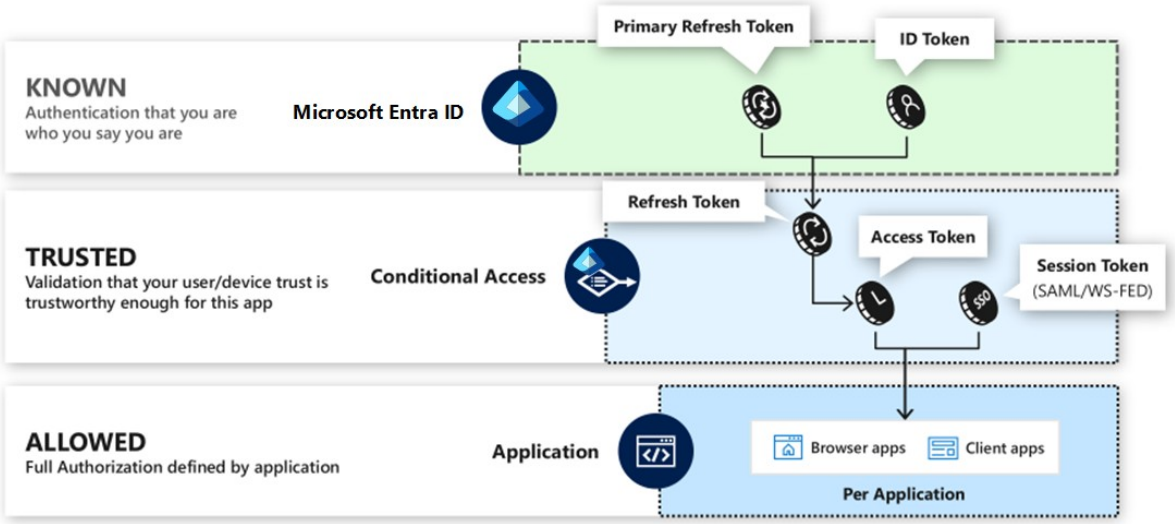
Key access control technologies

The key technical capabilities that enable modern access control are:

Policy engine: The component where organizations configure the technical security policy to meet the organization's productivity and security objectives.

Policy enforcement points: Points that enforce, across the organization's resources, the central policy decisions by the policy engine. The resources include data, applications, identity, network, and databases.

This diagram depicts how Microsoft Entra ID provides a policy engine and a policy enforcement point, so that security protocols can implement a known, trusted, allowed approach.



The Microsoft Entra policy engine can be extended to other policy enforcement points, including:

Modern applications: Applications that use modern authentication protocols.

Legacy applications: Via Microsoft Entra application proxy.

VPN and remote access solutions: Such as Cisco AnyConnect, Palo Alto Networks, F5, Fortinet, Citrix, and Zscaler.

Documents, email, and other files: Via Microsoft Purview Information Protection.

SaaS applications: For more information, see Tutorials for integrating SaaS applications with Microsoft Entra ID.

Data-driven access decisions

To fulfill the zero trust principle of explicit validation, it's critical to make an informed decision. The zero trust policy engine should have access to diverse data on the users and devices in order to make sound security decisions. This diversity helps to identify these aspects with greater confidence:

Whether the actual user is in control of the account.

Whether the device has been compromised by an attacker.

Whether the user has the appropriate roles and permissions.

Microsoft built a threat intelligence system that integrates security context from many and diverse signal sources. For more information, see Summary of Microsoft threat intelligence.

Segmentation: Separate to protect

Organizations often choose to create boundaries to divide the internal environment into separate segments, as part of their access control approach. This configuration is intended to contain the damage of a successful attack to the attacked segment. Segmentation is traditionally done with firewalls or other network filtering technology, though the concept can also be applied to identity and other technologies.

For information on applying segmentation to Azure environments, see Azure components and reference model

Isolation: Avoid firewall and forget

Isolation is an extreme form of segmentation that is sometimes required for protecting critically important assets. Isolation is most often used for assets that are both business-critical, and difficult to bring up to current policy and standards.

Classes of assets that might require isolation include operational technology (OT) systems like:

Supervisory control and data acquisition (SCADA)

Industrial control system (ICS)

Isolation must be designed as a complete people/process/technology system and be integrated with business processes to be successful and sustainable. This approach typically fails over time if it's implemented as a purely technology approach without processes and training to validate and sustain the defenses. It's easy to fall into a firewall and forget trap by defining the problem as static and technical.

In most cases, processes are needed to implement isolation, processes that various teams like security, IT, operational technology (OT), and sometimes business operations must follow. Successful isolation usually consists of:

People: Train all employees, vendors, and stakeholders on isolation strategy and their part in it. Include why it's important, for example, threats, risks and potential business impact, what they're expected to do, and how to do it.

Process: Establish clear policy and standards and document processes for business and technical stakeholders for all scenarios such as vendor access, change management process, threat response procedures, including exception management. Monitor to ensure the configuration doesn't drift and that other processes are followed correctly and rigorously.

Technology: Implement technical controls to block unauthorized communications, detect anomalies and potential threats, and harden bridging and transit devices that interact with the isolated environment, for example, operator consoles for operational technology (OT) systems.

Authentication in cloud computing

Cloud Storage uses OAuth 2.0 for API authentication and authorization. Authentication is the process of determining the identity of a client. The details of

authentication vary depending on how you are accessing Cloud Storage, but fall into two general types:

A server-centric flow allows an application to directly hold the credentials of a service account to complete authentication. Use this flow if your application works with its own data rather than user data. Google Cloud projects have default service accounts you can use, or you can create new ones.

A user-centric flow allows an application to obtain credentials from an end user. The user signs in to complete authentication. Use this flow if your application needs to access user data. See the User account credentials section later in this page for scenarios where a user-centric flow is appropriate.

Keep in mind that you can use both types of authentication together in an application. For more background information about authentication, see the Google Cloud Auth Guide.

Scopes

Authorization is the process of determining what permissions an authenticated identity has on a set of specified resources. OAuth 2.0 uses scopes to determine if an authenticated identity is authorized. Applications use a credential (obtained from a user-centric or server-centric authentication flow) together with one or more scopes to request an access token from a Google authorization server to access protected resources. For example, application A with an access token with read-only scope can only read, while application B with an access token with read-write scope can read and modify data. Neither application can read or modify access control lists on objects and buckets; only an application with full-control scope can do so.

Type	Description	Scope URL
read-only	Only allows access to read data, including listing buckets.	https://www.googleapis.com/a
read-write	Allows access to read and change data, but not metadata like IAM policies.	https://www.googleapis.com/a
full-control	Allows full control over data, including the	https://www.googleapis.com/a

	ability to modify IAM policies.	
cloud-platform.read-only	View your data across Google Cloud services. For Cloud Storage, this is the same as devstorage.read-only.	https://www.googleapis.com/a only
cloud-platform	View and manage data across all Google Cloud services. For Cloud Storage, this is the same as devstorage.full-control.	https://www.googleapis.com/a

Command line interface authentication

If you work with Cloud Storage using gcloud storage or gsutil commands from the command line, you should typically authenticate with your user account credentials. To do so, run the command gcloud auth login and follow the instructions, which includes logging into your user account.

For additional gcloud storage authentication options, see Authenticate for using the gcloud CLI.

For additional gsutil authentication options, see Credential types supporting various use cases.

Client library authentication

Client libraries can use Application Default Credentials to easily authenticate with Google APIs and send requests to those APIs. With Application Default Credentials, you can test your application locally and deploy it without changing the underlying code. For more information, see Authenticate for using client libraries.

Google Cloud

If you're running your application on services that support attached service accounts, such as App Engine, Cloud Functions, Cloud Run, or Compute Engine, the environment already provides a service account's authentication information, so no further setup is required. For Compute Engine, the service account scope depends on

how you created the instance. See Access scopes in the Compute Engine documentation. For App Engine, the cloud-platform scope is used.

Other environments

To initialize your local development or production environment, create a Google Cloud service account, download its key, and set the GOOGLE_APPLICATION_CREDENTIALS environment variable to use the key. For step-by-step information, see Setting up authentication with Cloud Storage client libraries.

API authentication

To make requests using OAuth 2.0 to either the Cloud Storage XML API or JSON API, include your application's access token in the Authorization header in every request that requires authentication. You can generate an access token from the OAuth 2.0 Playground:

In the OAuth 2.0 Playground, click Cloud Storage API v1, and then select an access level for your application (full_control, read_only, or read_write).

Click Authorize APIs.

Sign in to your Google account when prompted. In the dialogue that appears, click Allow.

In Step 2 of the playground, click Exchange authorization code for tokens for the authorization code that appears.

Copy your access token and include it in the Authorization header of your request:

Authorization: Bearer OAUTH2_TOKEN

The following is an example of a request that lists objects in a bucket.

JSON APIXML API

Use the list method of the Objects resource.

GET /storage/v1/b/example-bucket/o HTTP/1.1

Host: www.googleapis.com

Authorization: Bearer ya29.AHES6ZRVmB7fkLtd1XTmq6mo0S1wqZZi3-Lh_s-6Uw7p8vtgSwg

To authorize requests from the command line or for testing, you can use the curl command with the following syntax:

curl -H "Authorization: Bearer OAUTH2_TOKEN" "https://storage.googleapis.com/storage/v1/b/BUCKET_NAME/o"

For local testing, you can use the gcloud auth application-default print-access-token command to generate a token.

Due to the complexity of managing and refreshing access tokens and the security risk when dealing directly with cryptographic applications, we strongly encourage you to use a verified client library.

If you're looking for HMAC keys to use with the XML API for interoperable access with Amazon S3, see Managing HMAC keys for service accounts.

User account credentials

Use user account credentials for authentication when your application requires access to data on a user's behalf; otherwise, use service account credentials. Here are examples of scenarios where user account credentials can be used:

Web server applications

Installed and desktop applications

Mobile applications

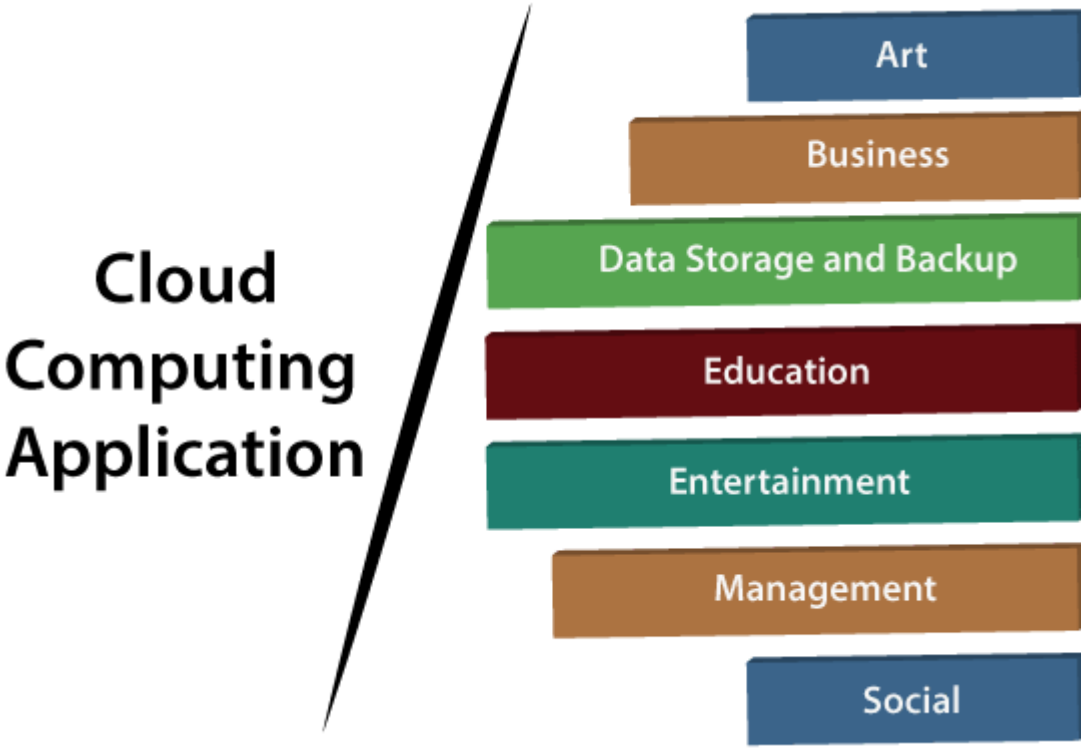
Client-side JavaScript

Applications on limited-input devices

Applications: Scientific Applications - Business and Consumer Applications

Cloud service providers provide various applications in the field of art, business, data storage and backup services, education, entertainment, management, social networking, etc.

The most widely used cloud computing applications are given below -



1. Art Applications

Cloud computing offers various art applications for quickly and easily design attractive cards, booklets, and images. Some most commonly used cloud art applications are given below:

ii. Vistaprint

Vistaprint allows us to easily design various printed marketing products such as business cards, Postcards, Booklets, and wedding invitations cards.

iii. Adobe Creative Cloud

Adobe creative cloud is made for designers, artists, filmmakers, and other creative professionals. It is a suite of apps which includes PhotoShop image editing programming, Illustrator, InDesign, TypeKit, Dreamweaver, XD, and Audition.

2. Business Applications

Business applications are based on cloud service providers. Today, every organization requires the cloud business application to grow their business. It also ensures that business applications are 24*7 available to users.

There are the following business applications of cloud computing -

i. MailChimp

MailChimp is an email publishing platform which provides various options to design, send, and save templates for emails.

iii. Salesforce

Salesforce platform provides tools for sales, service, marketing, e-commerce, and more. It also provides a cloud development platform.

iv. Chatter

Chatter helps us to share important information about the organization in real time.

v. Bitrix24

Bitrix24 is a collaboration platform which provides communication, management, and social collaboration tools.

vi. Paypal

vii. Slack

Slack stands for Searchable Log of all Conversation and Knowledge. It provides a user-friendly interface that helps us to create public and private channels for communication.

viii. Quickbooks

Quickbooks works on the terminology "Run Enterprise anytime, anywhere, on any device." It provides online accounting solutions for the business. It allows more than 20 users to work simultaneously on the same system.

3. Data Storage and Backup Applications

Cloud computing allows us to store information (data, files, images, audios, and videos) on the cloud and access this information using an internet connection. As the cloud provider is responsible for providing security, so they offer various backup recovery application for retrieving the lost data.

A list of data storage and backup applications in the cloud are given below -

i. Box.com

Box provides an online environment for secure content management, workflow, and collaboration. It allows us to store different files such as Excel, Word, PDF, and images on the cloud. The main advantage of using box is that it provides drag & drop service for files and easily integrates with Office 365, G Suite, Salesforce, and more than 1400 tools.

ii. Mozy

Mozy provides powerful online backup solutions for our personal and business data. It schedules automatically back up for each day at a specific time.

iii. Joukuu

Joukuu provides the simplest way to share and track cloud-based backup files. Many users use joukuu to search files, folders, and collaborate on documents.

iv. Google G Suite

Google G Suite is one of the best cloud storage and backup application. It includes Google Calendar, Docs, Forms, Google+, Hangouts, as well as cloud storage and tools for managing cloud apps. The most popular app in the Google G Suite is Gmail. Gmail offers free email services to users.

4. Education Applications

Cloud computing in the education sector becomes very popular. It offers various online distance learning platforms and student information portals to the students. The advantage of using cloud in the field of education is that it offers strong virtual classroom environments, Ease of accessibility, secure data storage, scalability, greater reach for the students, and minimal hardware requirements for the applications.

There are the following education applications offered by the cloud -

i. Google Apps for Education

Google Apps for Education is the most widely used platform for free web-based email, calendar, documents, and collaborative study.

ii. Chromebooks for Education

Chromebook for Education is one of the most important Google's projects. It is designed for the purpose that it enhances education innovation.

iii. Tablets with Google Play for Education

It allows educators to quickly implement the latest technology solutions into the classroom and make it available to their students.

iv. AWS in Education

AWS cloud provides an education-friendly environment to universities, community colleges, and schools.

5. Entertainment Applications

Entertainment industries use a multi-cloud strategy to interact with the target audience. Cloud computing offers various entertainment applications such as online games and video conferencing.

i. Online games

Today, cloud gaming becomes one of the most important entertainment media. It offers various online games that run remotely from the cloud. The best cloud gaming services are Shaow, GeForce Now, Vortex, Project xCloud, and PlayStation Now.

ii. Video Conferencing Apps

Video conferencing apps provides a simple and instant connected experience. It allows us to communicate with our business partners, friends, and relatives using a cloud-based video conferencing. The benefits of using video conferencing are that it reduces cost, increases efficiency, and removes interoperability.

6. Management Applications

Cloud computing offers various cloud management tools which help admins to manage all types of cloud activities, such as resource deployment, data integration, and disaster recovery. These management tools also provide administrative control over the platforms, applications, and infrastructure.

Some important management applications are -

i. Toggl

Toggl helps users to track allocated time period for a particular project.

iii. Outright

Outright is used by management users for the purpose of accounts. It helps to track income, expenses, profits, and losses in real-time environment.

iv. GoToMeeting

GoToMeeting provides Video Conferencing and online meeting apps, which allows you to start a meeting with your business partners from anytime, anywhere using mobile phones or tablets. Using GoToMeeting app, you can perform the tasks related to the management such as join meetings in seconds, view presentations on the shared screen, get alerts for upcoming meetings, etc.

7. Social Applications

Social cloud applications allow a large number of users to connect with each other using social networking applications such as Facebook, Twitter, Linkedln, etc.

There are the following cloud based social applications -

Facebook is a social networking website which allows active users to share files, photos, videos, status, more to their friends, relatives, and business partners using the cloud storage system. On Facebook, we will always get notifications when our friends like and comment on the posts.

ii. Twitter

Twitter is a social networking site. It is a microblogging system. It allows users to follow high profile celebrities, friends, relatives, and receive news. It sends and receives short posts called tweets.

iii. Yammer

Yammer is the best team collaboration tool that allows a team of employees to chat, share images, documents, and videos.

iv. LinkedIn

LinkedIn is a social network for students, freshers, and professionals.