UNIT-2

Chapter 2: Cloud Service Models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Comparison and use cases of service models. Cloud Platform and Tools: Introduction to popular cloud platforms (AWS, Azure, Google Cloud).

Security in Cloud Computing, Security challenges and threats in the cloud, Identity and access management, Data privacy and protection, Compliance and legal issues in the cloud

Cloud Service Models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS)

1. IAAS: Infrastructure As A Service (IAAS) is means of delivering computing infrastructure as on-demand services. It is one of the three fundamental cloud service models. The user purchases servers, software data center space, or network equipment and rent those resources through a fully outsourced, on-demand service model. It allows dynamic scaling and the resources are distributed as a service. It generally includes multiple-user on a single piece of hardware.
It totally depends upon the customer to choose its resources wisely and as per need. Also, it provides billing management too.

2. PAAS: Platform As A Service (PAAS) is a cloud delivery model for applications composed of services managed by a third party. It provides elastic scaling of your application which allows developers to build applications and services over the internet and the deployment models include public, private and hybrid.
Basically, it is a service where a third-party provider provides both software and hardware tools to the cloud computing. The tools which are provided are used by developers. PAAS is also known as Application PAAS. It helps us to organize and maintain useful applications and services. It has a well-equipped management system and is less expensive compared to IAAS.

3. SAAS: Software As A Service (SAAS) allows users to run existing online applications and it is a model software that is deployed as a hosting service and is accessed over Output Rephrased/Re-written Text the internet or software delivery model during which software and its associated data are hosted centrally and accessed using their client, usually an online browser over the web. SAAS services are used for the development and deployment of modern applications.

Difference between IAAS, PAAS and SAAS :

Basis Of	IAAS	PAAS	SAAS
Stands for	Infrastructure as a service.	Platform as a service.	Software as a service.

Basis Of	IAAS	PAAS	SAAS
Uses	IAAS is used by network architects.	PAAS is used by developers.	SAAS is used by the end user.
Access	IAAS gives access to the resources like virtual machines and virtual storage.	PAAS gives access to run time environment to deployment and development tools for application.	SAAS gives access to the end user.
Model	It is a service model that provides virtualized computing resources over the internet.	It is a cloud computing model that delivers tools that are used for the development of applications.	It is a service model in cloud computing that hosts software to make it available to clients.
Technical understanding.	It requires technical knowledge.	Some knowledge is required for the basic setup.	There is no requirement about technicalities company handles everything.
Popularity	It is popular among developers and researchers.	It is popular among developers who focus on the development of apps and scripts.	It is popular among consumers and companies, such as file sharing, email, and networking.
Percentage rise	It has around a 12% increment.	It has around 32% increment.	It has about a 27 % rise in the cloud computing model.
Usage	Used by the skilled developer to develop unique applications.	Used by mid-level developers to build applications.	Used among the users of entertainment.
Cloud services.	Amazon Web Services, sun, vCloud Express.	Facebook, and Google search engine.	MS Office web, Facebook and Google Apps.

Basis Of	IAAS	PAAS	SAAS
Enterprise services.	AWS virtual private cloud.	Microsoft Azure.	IBM cloud analysis.
Outsourced cloud services.	Salesforce	Force.com, Gigaspaces.	AWS, Terremark
User Controls	Operating System, Runtime, Middleware, and Application data	Data of the application	Nothing
Others	It is highly scalable and flexible.	It is highly scalable to suit the different businesses according to resources.	It is highly scalable to suit the small, mid and enterprise level business

Advantages of IaaS

- The resources can be deployed by the provider to a customer's environment at any given time.
- Its ability to offer the users to scale the business based on their requirements.
- The provider has various options when deploying resources including virtual machines, applications, storage, and networks.
- It has the potential to handle an immense number of users.
- It is easy to expand and saves a lot of money. Companies can afford the huge costs associated with the implementation of advanced technologies.
- Cloud provides the architecture.
- Enhanced scalability and quite flexible.
- Dynamic workloads are supported.

Disadvantages of IaaS

- Security issues are there.
- Service and Network delays are quite a issue in IaaS.

Advantages of PaaS –

- Programmers need not worry about what specific database or language the application has been programmed in.
- It offers developers the to build applications without the overhead of the underlying operating system or infrastructure.
- Provides the freedom to developers to focus on the application's design while the platform takes care of the language and the database.
- It is flexible and portable.
- It is quite affordable.
- It manages application development phases in the cloud very efficiently.

Disadvantages of PaaS

- Data is not secure and is at big risk.
- As data is stored both in local storage and cloud, there are high chances of data mismatch while integrating the data.

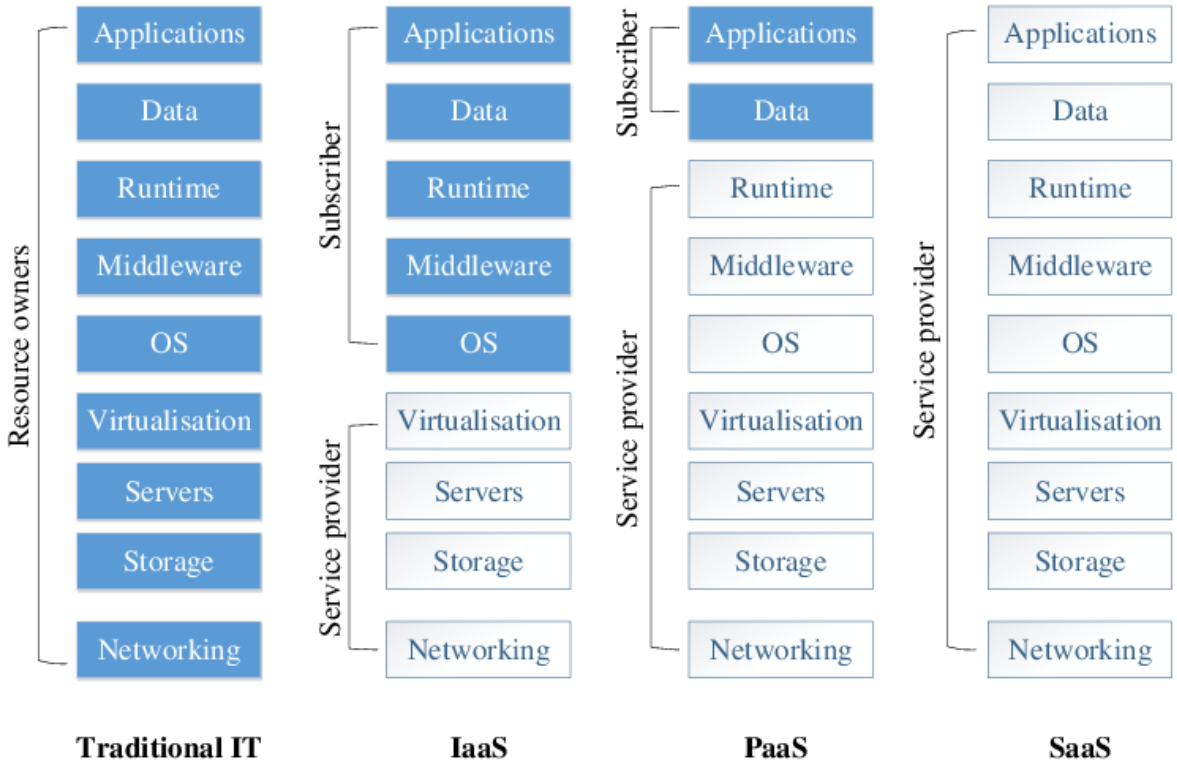
Advantages of SaaS

- It is a cloud computing service category providing a wide range of hosted capabilities and services. These can be used to build and deploy web-based software applications.
- It provides a lower cost of ownership than on-premises software. The reason is it does not require the purchase or installation of hardware or licenses.
- It can be easily accessed through a browser along a thin client.
- No cost is required for initial setup.
- Low maintenance costs.
- Installation time is less, so time is managed properly.

Disadvantages of SaaS

- Low performance.
- It has limited customization options.
- It has security and data concerns.

Comparison and use cases of service models



Cloud Platform and Tools: Introduction to popular cloud platforms (AWS, Azure, Google Cloud)

PRODUCT	aws	Microsoft Azure	Google Cloud Platform
Virtual Servers	Instances	VMs	VM Instances
Platform-as-a-Service	Elastic Beanstalk	Cloud Services	App Engine
Serverless Computing	Lambda	Azure Functions	Cloud Functions
Docker Management	ECS	Container Service	Container Engine
Kubernetes Management	EKS	Kubernetes Service	Kubernetes Engine
Object Storage	S3	Block Blob	Cloud Storage
Archive Storage	Glacier	Archive Storage	Coldline
File Storage	EFS	Azure Files	ZFS / Avere
Global Content Delivery	CloudFront	Delivery Network	Cloud CDN
Managed Data Warehouse	Redshift	SQL Warehouse	Big Query

Jelvix Source: res.cloudinary.com jelvix.com

Cloud computing has revolutionized the way organizations work, and advancing us to a new technology era. Amazon Web Services, Microsoft Azure, and Google Cloud Platform are the top cloud service providers that dominate the worldwide cloud market.
Nowadays, most enterprises are moving towards the cloud and even multi-cloud environments to harness the benefits offered by cloud computing, such as:

- Decreased CapEx
- Reduced infrastructure maintenance
- Increased availability

- Scalability

Of course, the Big 3 cloud providers possess the experience and expertise to provide a reliable and feature-rich cloud platform. But, before committing to a specific cloud platform, you must do your due diligence and compare each platform to fully understand their capabilities and differences.

Amazon Web Services (AWS)

The current market leader of the cloud computing platforms, Amazon Web Services is a subsidiary of Amazon.com, Inc. AWS is the most mature cloud platform offering a wide range of services to practically everyone: individual developers, large enterprises, and even governments.
AWS started its life as an internal cloud offering. By 2006, it had evolved into a publicly available cloud platform with services like Amazon S3 cloud storage and elastic compute cloud (EC2). AWS now offers more than 200 fully featured services to cater to any demand and serve millions of users.

Prominent AWS customers include:

- Expedia
- Netflix
- Coinbase
- Formula 1
- Coca Cola
- Intuit
- Airbnb
- Lyft
- Coursera
- Food and Drug Administration (FDA)

Google Cloud Platform (GCP)

The Google Cloud Platform is the cloud offering by none other than Google. GCP is part of the overarching Google Cloud.

Available to the general public beginning in 2010, the Google Cloud Platform currently offers over 100 services spanning computing, networking, big data, and more. Today GCP consists of services including Google Workspace, enterprise Android, and Chrome OS.

Compared to AWS and Azure, GCP is the smallest of the Big 3 cloud providers. Yet it offers a robust set of cloud services to power and support any kind of application.

Notable GCP customers include:

- Toyota
- Unilever
- Nintendo
- Spotify
- The Home Depot
- Target
- Twitter
- Paypal
- UPS

Microsoft Azure

Microsoft Azure is the second-largest cloud platform. Debuting in 2010, Azure has evolved into a cloud platform with more than 200 products and services. Today, it is among the fastest-growing cloud platforms.

As Microsoft offers Azure, it provides a wide array of services tailored particularly for Microsoft-centric enterprises—making the switch to a cloud or a hybrid-cloud environment smooth for many organizations. In use by more than 95% of Fortune 500 companies, Microsoft Azure has a proven track record in catering to enterprise users.

Importantly, Azure is not limited to Windows-based services. It also supports open-source languages, technologies, and platforms, giving anyone the freedom to build and support any application.

Well-known Azure customers include:

- DAIMLER AG
- McKesson Group
- Asos
- Center of Disease Control (CDC) – US
- National Health Service (NHS) – UK

- HSBC
- Starbucks
- Walgreens
- 3M
- HP
- Mitsubishi Electric
- Renault

Security in Cloud Computing

Cloud security is the set of control-based security measures and technology protection, designed to protect online stored resources from **leakage, theft**, and **data loss**. Protection includes data from **cloud infrastructure, applications**, and **threats.** Security applications uses a software the same as **SaaS (Software as a Service)** model.

How to manage security in the cloud?

Cloud service providers have many methods to protect the data.

Firewall is the central part of cloud architecture. The firewall protects the network and the perimeter of end-users. It also protects traffic between various apps stored in the cloud.

Access control protects data by allowing us to set access lists for various assets. For example, you can allow the application of **specific employees** while restricting others. It's a rule that employees can access the equipment that they required. We can keep essential documents which are stolen from **malicious insiders** or hackers to maintaining strict access control.

Benefits of Cloud Security System

We understand how the cloud computing security operates to find ways to benefit your business.

Cloud-based security systems benefit the business by:

- Protecting the Business from Dangers
- Protect against internal threats
- Preventing data loss
- Top threats to the system include **Malware, Ransomware**, and
- Break the Malware and Ransomware attacks
- Malware poses a severe threat to the businesses.

More than **90%** of malware comes via email. It is often reassuring that employee's download malware without analysingit. Malicious software installs itself on the network to steal files or damage the content once it is downloaded.

Ransomware is a malware that hijacks system's data and asks for a financial ransom. Companies are reluctant to give ransom because they want their data back.

Data redundancy provides the option to pay a ransom for your data. You can get that was stolen with **minimal** service interruption.

Many cloud data protection solutions identify **malware** and **ransomware**. Firewalls keep malicious email out of the inbox.

DDoS Security

Distributed Denial of Service (DDoS)is flooded with requests. Website slows down the downloading until it crashes to handle the number of requests.

DDoS attacks come with many serious side effects. Most of the companies suffering from **DDoS** attacks lose **$ 10,000** to **$ 100,000**. Many businesses damage reputation when customers lose confidence in the brand. If confidential customer data is lost through any DDoS attack, we may face challenges.

The severity of these side effects, some companies shut down after the DDoS attacks. It is to be noted that the last DDoS attack lasted for **12** days.

Cloud security service monitors the cloud to identify and prevent attacks. The cloud service providers protectthe cloud service users in real time.

Threat to detect

Cloud computing detects advanced threats by using endpoint scanning for threats at the **device level**.

Difference between Cloud Security and Traditional IT Security

Cloud security	Traditional IT Security
Quick scalable	Slow scaling
Efficient resource utilization	Lower efficiency
Usage-based cost	Higher cost
Third-party data centres	In-house data centres
Reduced time to market	Longer time to market
Low upfront infrastructure	High Upfronts costs

Top 7 Advanced Cloud Security Challenges

It becomes more challenging when adopting modern cloud approaches Like: **automated cloud integration**, and **continuous deployment (CI/CD)** methods, distributed serverless architecture, and short-term assets for tasks such as a service and container.

Some of the advanced cloud-native security challenge and many layers of risk faced by today's cloud-oriented organizations are below:

1. Enlarged Surface

Public cloud environments have become a large and highly attractive surface for hackers and disrupt workloads and data in the cloud. Malware, zero-day, account acquisition and many malicious threats have become day-to-day more dangerous.

2. Lack of visibility and tracking

Cloud providers have complete control over the infrastructure layer and cannot expose it to their customers in the **IaaS** model. The lack of visibility and control is further enhanced in the **SaaS** cloud models. Cloud customers are often unable to identify their cloud assets or visualize their cloud environments effectively.

3. Ever-changing workload

Cloud assets are dynamically demoted at scale and velocity. Traditional security tools implement protection policies in a flexible and dynamic environment with an ever-changing and short-term workload.

4. DevOps, DevSecOps and Automation

Organizations are adopting an automated **DevOps** **CI/CD** culture that ensures the appropriate security controls are **identified** and **embedded**in the development cycle in code and templates. Security-related changes implemented *after* the workload is deployed to production can weaken the organization's security posture and lengthen the time to market.

5. Granular privileges and critical management

At the application level, configured keys and privileges expose the session to security risks. Often cloud user roles are loosely configured, providing broad privileges beyond therequirement. An example is allowing untrained users or users to delete or write databases with no business to delete or add database assets.

6. Complex environment

These days the methods and tools work seamlessly on public cloud providers, private cloud providers, and on-premises manage persistent security in hybrid and multi-cloud environments-it including geographic Branch office edge security for formally distributed organizations.

7. Cloud Compliance and Governance

All the leading cloud providers have known themselves best, such as **PCI 3.2, NIST 800-53, HIPAA** and **GDPR**.

It gives the poor visibility and dynamics of cloud environments. The compliance audit process becomes close to mission impossible unless the devices are used to receive compliance checks and issue real-time alerts.

Cloud Computing Security Architecture

Security in cloud computing is a major concern. Proxy and brokerage services should be employed to restrict a client from accessing the shared data directly. Data in the cloud should be stored in encrypted form.

Security Planning

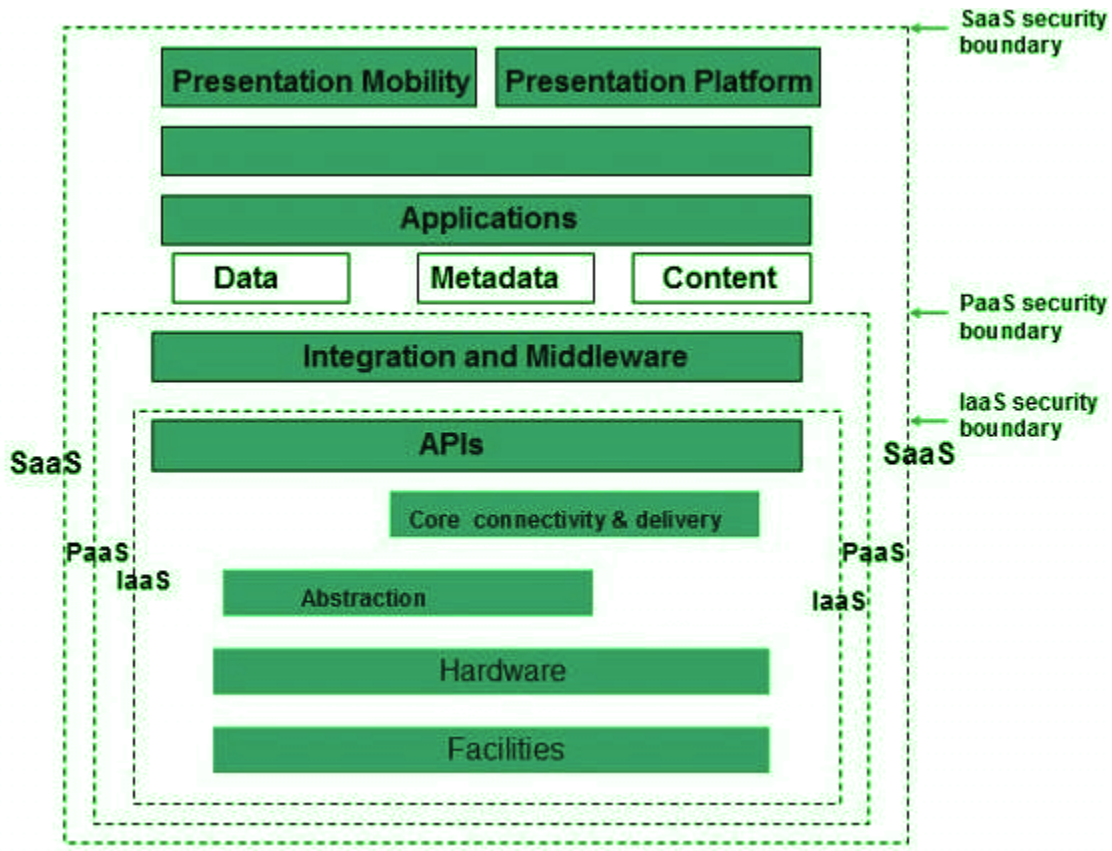
Before deploying a particular resource to the cloud, one should need to analyze several aspects of the resource, such as:

- A select resource needs to move to the cloud and analyze its sensitivity to risk.
- Consider cloud service models such as **IaaS, PaaS,**and These models require the customer to be responsible for Security at different service levels.
- Consider the cloud type, such as **public, private, community**, or
- Understand the cloud service provider's system regarding data storage and its transfer into and out of the cloud.
- The risk in cloud deployment mainly depends upon the service models and cloud types.

Understanding Security of Cloud

Security Boundaries

The **Cloud Security Alliance (CSA)** stack model defines the boundaries between each service model and shows how different functional units relate. A particular service model defines the boundary between the service provider's responsibilities and the customer. The following diagram shows the **CSA stack model:**



Cloud Governance and Its Need

- It is the set of policies or principles that act as the guidance for the adoption use, and management of cloud technology services.
- It is an ongoing process that must sit on top of existing governance models.
- It is a set of rules you create to monitor and amend as necessary in order to control costs, improve efficiency, and eliminate security risks.

Need for Cloud Governance :

By implementing cloud governance, organizations can avoid the following issues as follows.

1. Security and privacy risks :

- This issue may arise due to unauthorized downloads/ installation of software, storage of illegal data, and access to restricted sites by users.
- Cloud Governance solutions cover multiple cloud security components. For example, Encryption, Security groups, Audit trails, Application access rules, Access controls.

. Vendor lock-in :

- Many vendors opt for this, as this clause causes organizations to depend on the cloud service provider (or vendor) for products and services.
- This can be avoided by making changes to the SLA suitably and reduce dependencies on a single vendor, thus ensuring freedom to the organization.

3. Cloud Sprawl :

- This happens when employees of different departments use different programs and cloud infrastructure from third-party providers without involving the IT department and getting necessary approvals.
- If not detected and restricted, crowd sprawl may lead to fragmented, redundant, inefficient, and unmanaged cloud programs sitting on the enterprise cloud and unnecessarily creating trouble.

4. Shadow IT and unwarranted usage of cloud resources :

- This happens when employees in various departments do not follow the rules and regulations as imposed by the IT department on cloud usage resulting in security breaches and fragmented control throughout the organization.
- This leads to not getting sufficient results from the cloud in the long run.

5. Lack of data portability and interoperability :

- This happens when the cloud service provider or the inbuilt cloud infrastructure is incapable of connecting well with other software and products outside the organization.
- This may also lead to modules not compatible with each other and hence chaos in the cloud due to an inefficient system.

Cloud Security governance Deployment Framework

standards have also been considered.

Figure 2. Cloud SSDLC: Cloud Security Governence Deployment

Virtual machine security in cloud computing

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.

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.

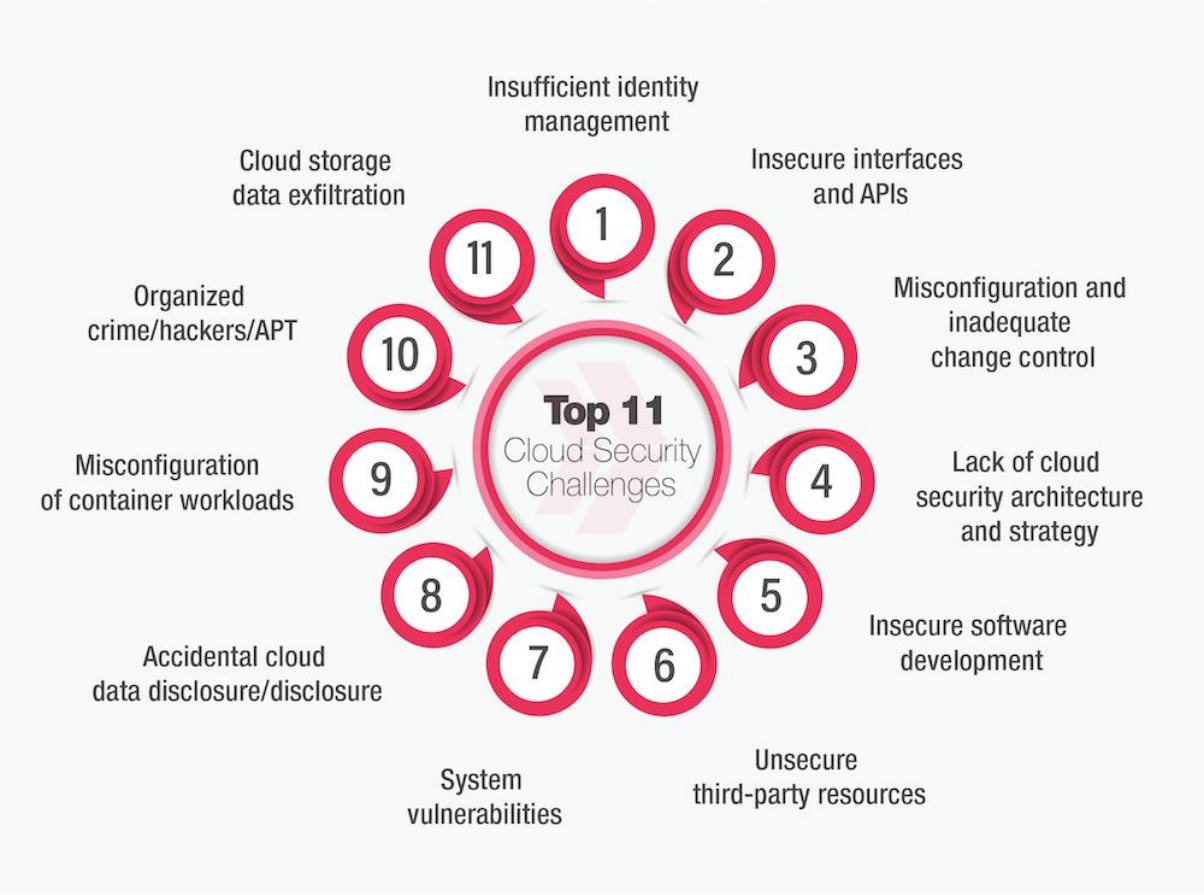
Separate Management APIs to Protect the Network

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 challenges and threats in the cloud



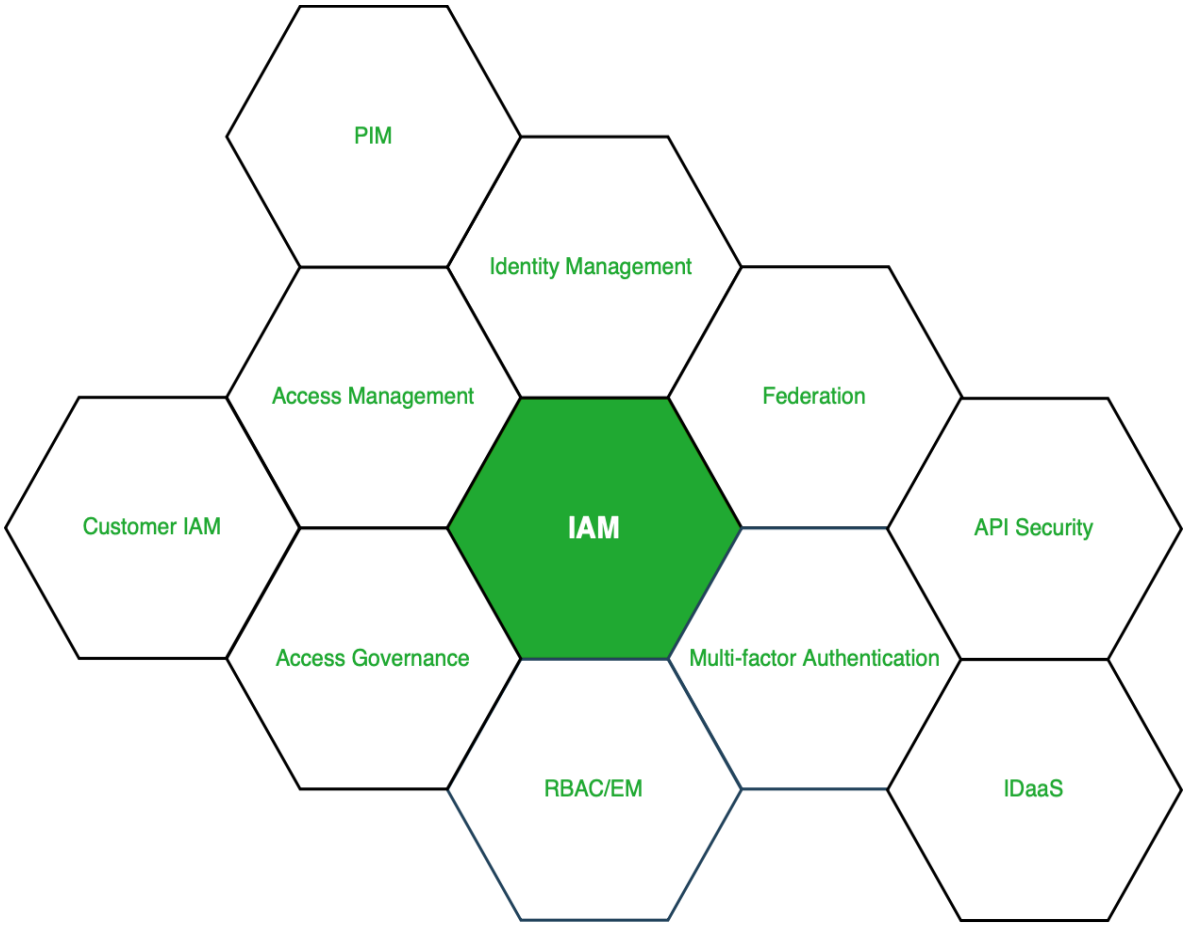
Main Cloud Security Issues and Threats in 2023

Misconfiguration, Unauthorized Access, Insecure Interfaces/APIs, Hijacking of Accounts, Lack of Visibility, External Sharing of Data, Malicious Insiders, Cyberattacks

Denial of Service Attacks, Data Loss/Leakage, Data Privacy/Confidentiality, Accidental Exposure of Credentials, Incident Response, Legal and Regulatory Compliance, Data Sovereignty/Residence/Control, Protecting the Cloud.

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. And so 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 IAM

- Users

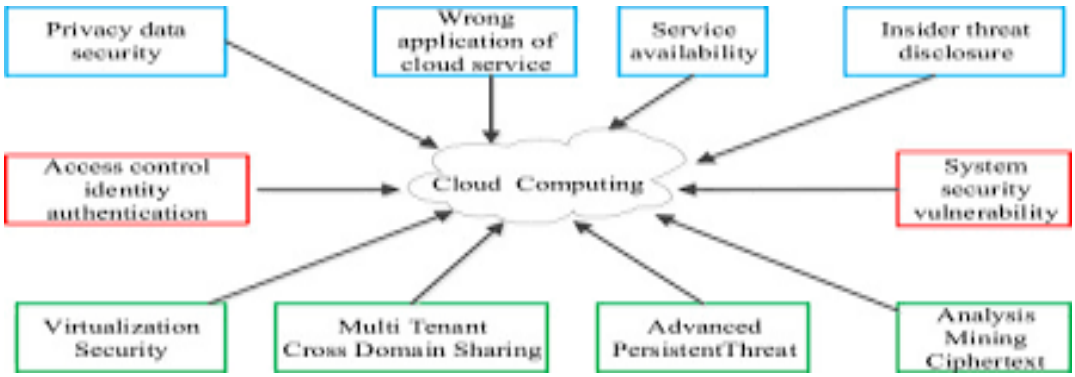
- Roles
- Groups
- Policies

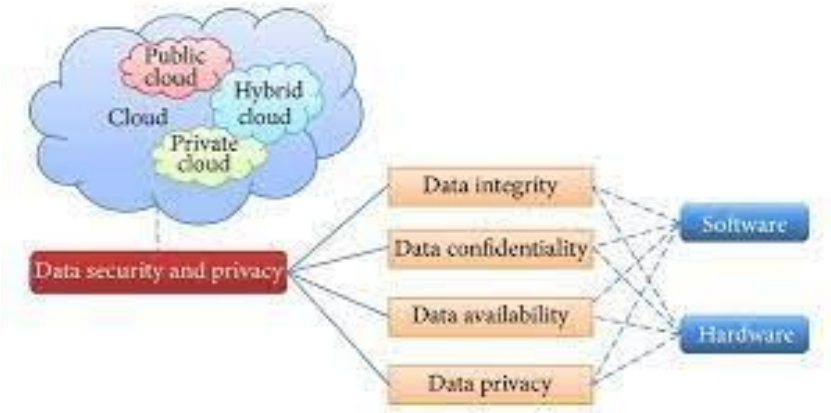
With these new applications being created over the cloud, mobile and on-premise can hold sensitive and regulated information. It's no longer acceptable and feasible to just create an Identity server and provide access based on the requests. In current times an organization should be able to track the 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.

Services By IAM

- Identity 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)

Data privacy and protection





Data privacy in cloud computing is the practice of **collecting, storing, transferring and sharing data over the cloud without putting the privacy of personal data at risk**

1. Cloud data security is the practice of protecting data and other digital information assets from security threats, human error, and insider threats

2. Data security and privacy are inevitable requirements of cloud environments

3. To successfully protect and secure data in cloud environments, companies must know which data they have and where it's located, which data is exposed, how it's exposed, and potential risks, which applications are being accessed and by whom, what's happening inside their applications, and which data they need to protect and at what level4.

Compliance and legal issues in the cloud

3. Legal implications of cloud computing

As mentioned above, like any other technology, cloud computing offers mar advantages, but it also raises many potential legal and regulatory issues. Howeve when using a private cloud, customers can negotiate a particular risk within the term and conditions of their contracts. The remaining models of cloud computing offe customers or users less negotiation power, leaving the customer to bear the legal risk.