Cybersecurity Management
Cloud computing security

Marc Ruiz & Raul Roca

marc.ruiz-ramirez@upc.edu

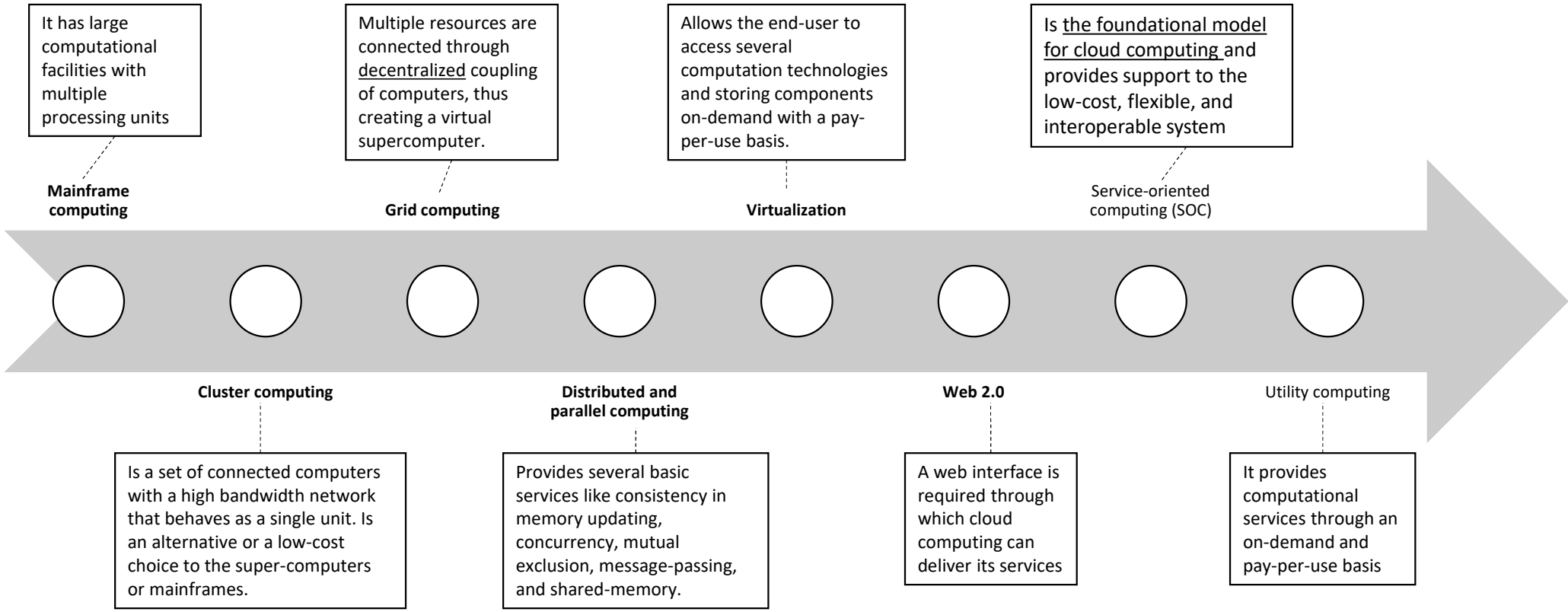
Objectives

- Know the main concepts of cloud computing.
- Know the history and underlying technologies of Cloud Computing
- Know the NIST definition of Cloud Computing
- Know the definitions and characteristics of Cloud Computing
- Know the main cloud security concepts
- Understand the taxonomy of cloud attacks
- Understanding the OWASP Top 10 Cloud Security Risks
- Understand the main Cloud Computing standards
- Know the NIST Cloud Reference Model
- Learn the NIST recommendations for cloud security
- Work on the concepts of cloud security with examples

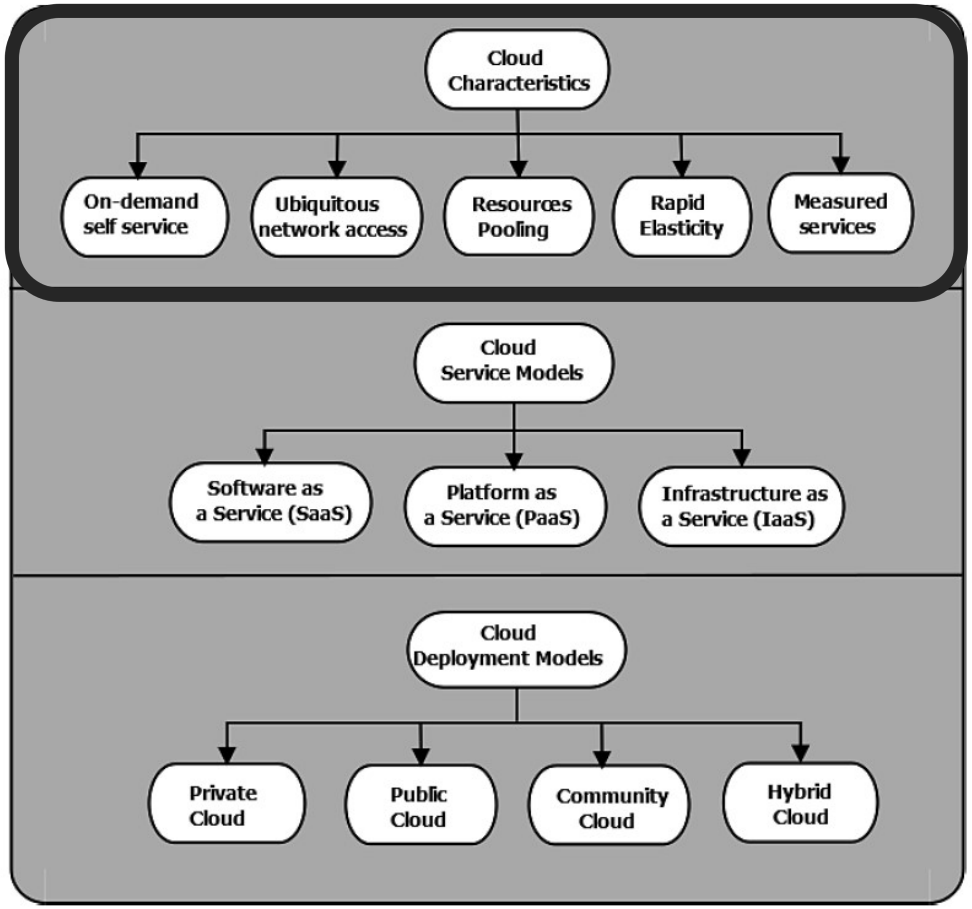
Contents

- Cloud Computing
  - History and Underlying Technologies
  - NIST definition
  - Definitions and Characteristics
- Cloud Security
  - Concepts
  - A Taxonomy of Attacks
  - OWASP Top 10 Cloud Security Risks
  - Standards
  - NIST Cloud Reference Model
  - NIST Recommendations for Cloud Security
  - Examples

Cloud Computing.
History and Underlying Technologies



Cloud Computing. Definitions and Characteristics



- **NIST definition**
  - *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*

Cloud Computing.
NIST definition

- **NIST definition**
  - *"Cloud computing is a model for enabling **ubiquitous, convenient,** on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*
- **Ubiquitous and convenient**
  - Designed →quickly and easily request services
  - Services → accessible from anywhere → with a network connection.

Cloud Computing.
NIST definition

- **NIST definition**
  - *"Cloud computing is a model for enabling ubiquitous, convenient,* ***on-demand*** *network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*
- **On-demand**
  - Customer requests are fulfilled immediately
  - Infinite pool of resources waiting for their requests

Cloud Computing.
NIST definition

- **NIST definition**
  - *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a **shared pool** of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*
- **Shared pool of resources**.
  - They use **multitenancy** → many different customers share access to the same physical resources.
  - CSP → is responsible for implementing isolation controls

Cloud Computing.
NIST definition

- **NIST definition**
  - *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of* ***configurable*** *computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*
- **Highly configurable**
  - The customer can tailor their use of cloud resources to meet their own specific business objectives.

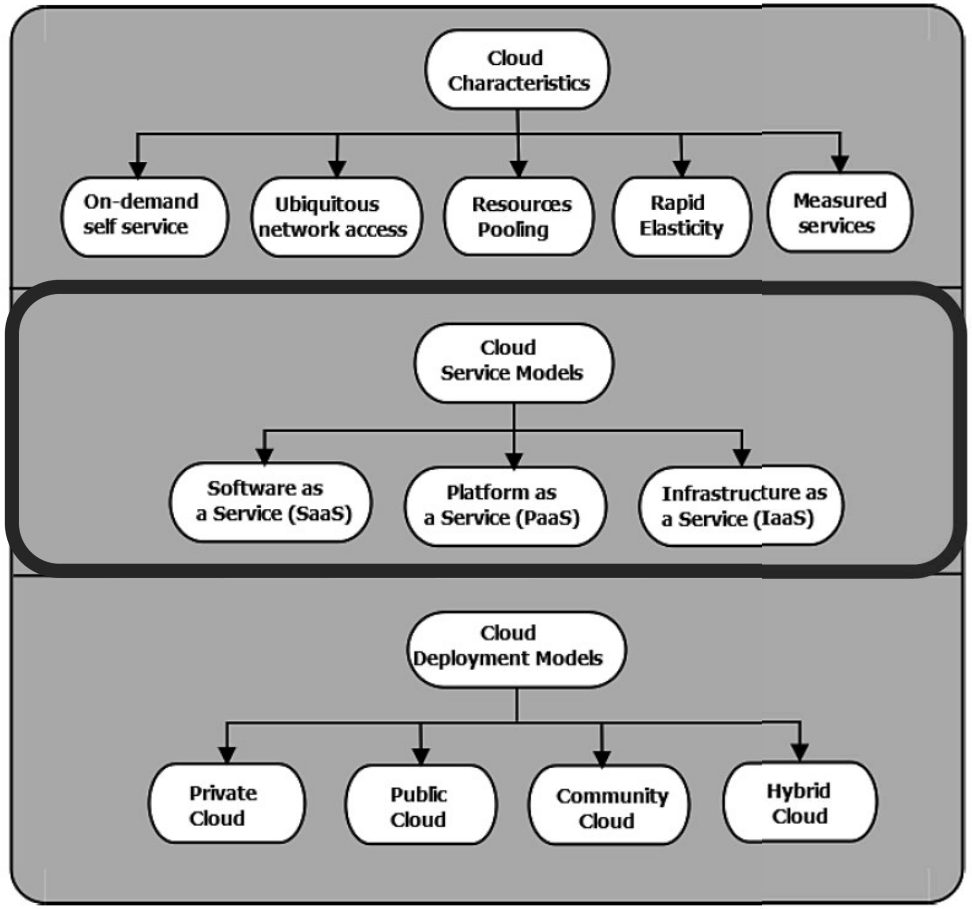
Cloud Computing.
NIST definition

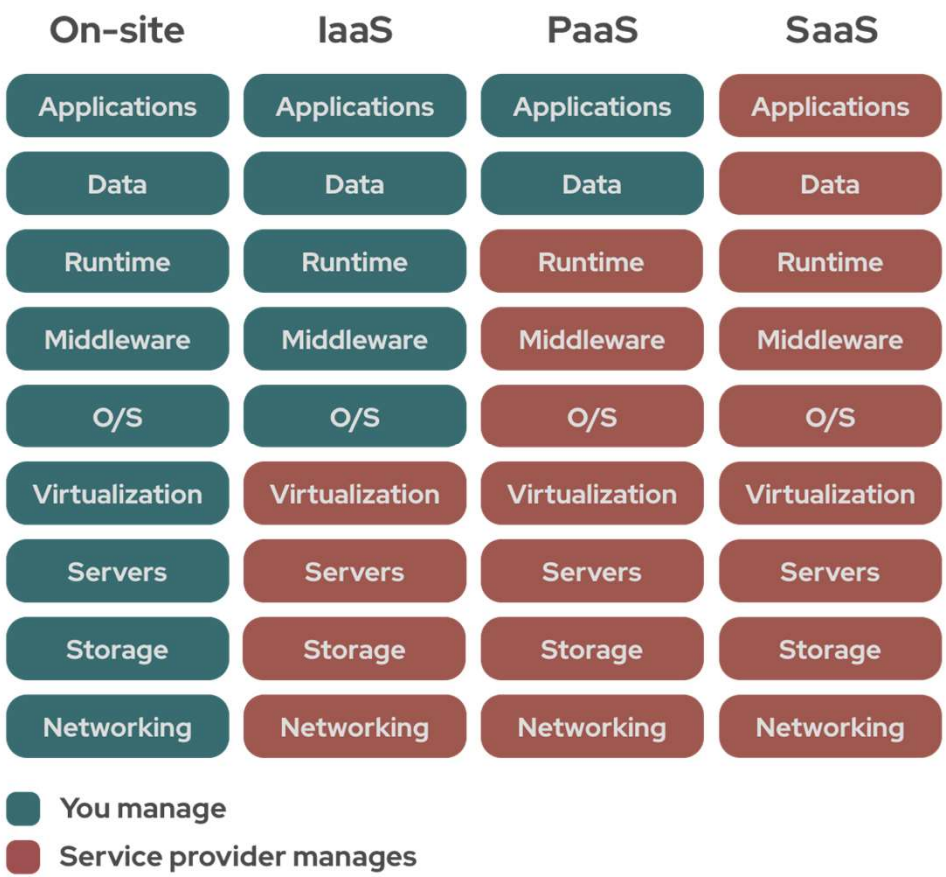
- **NIST definition**
  - *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be* ***rapidly*** **provisioned and released** *with minimal management effort or service provider interaction."*
- **Rapidly provisioned & Rapidly released**
  - No need resource → Release resource → No pay for Resource
  - Immediately

Cloud Computing.
NIST definition

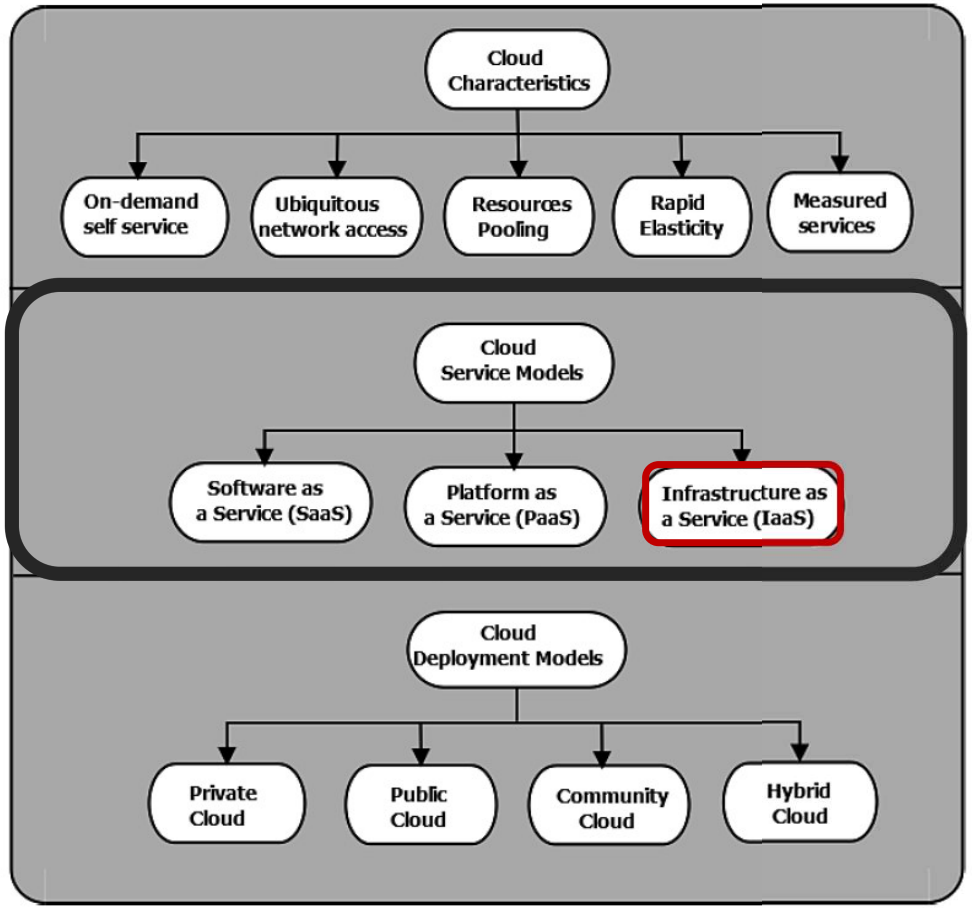
- **NIST definition**
  - *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with* ***minimal management*** *effort or service provider interaction."*
- **Require minimal management effort from the customer**
  - Customers transfer many responsibilities
    - from their own IT teams → the CSP.

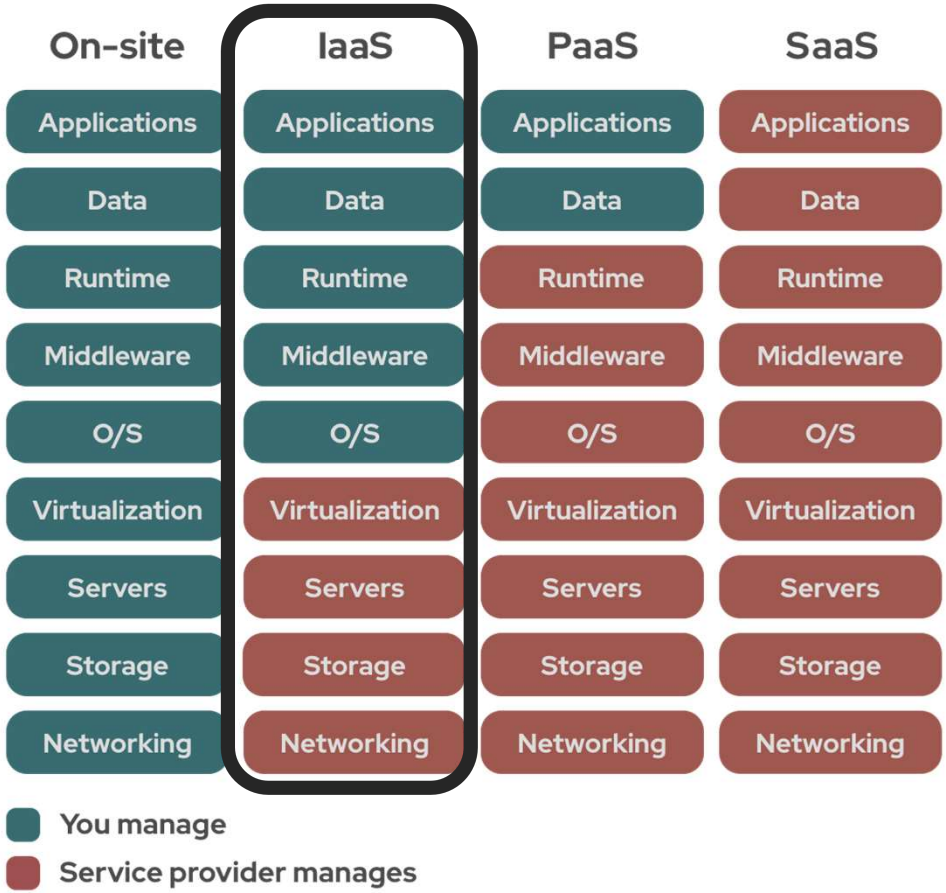
Cloud Computing. Definitions and Characteristics



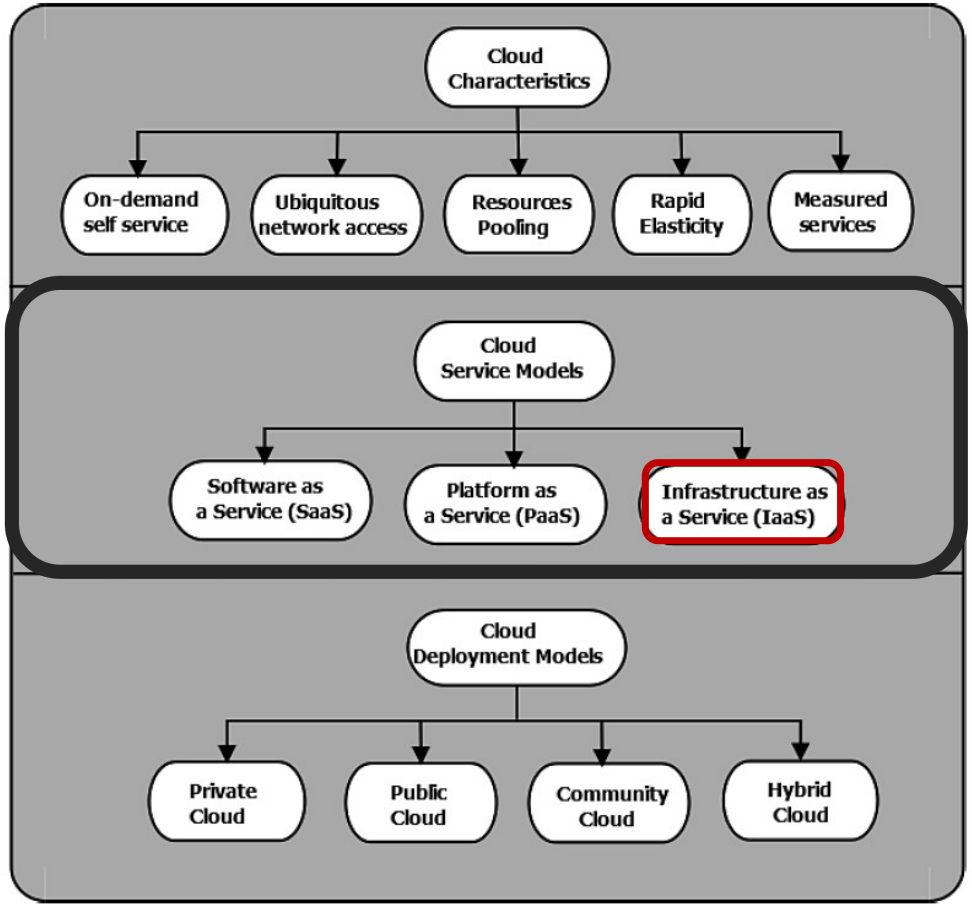


Cloud Computing. Definitions and Characteristics





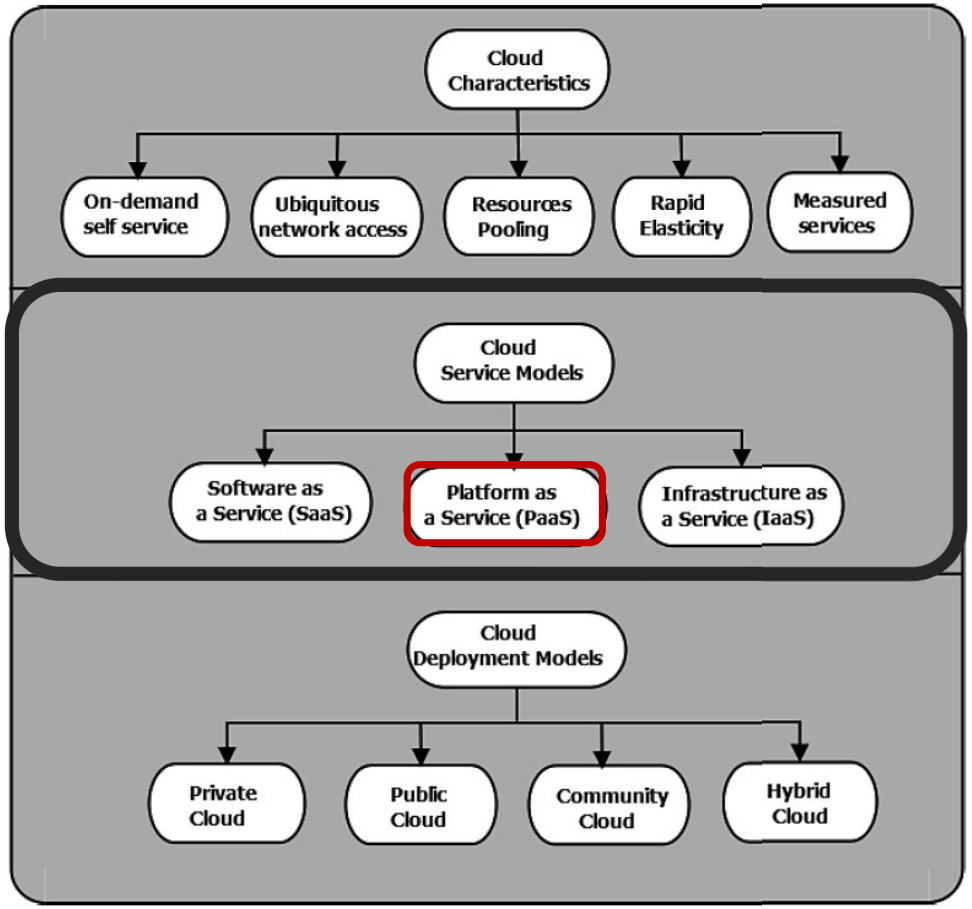
Cloud Computing. Definitions and Characteristics

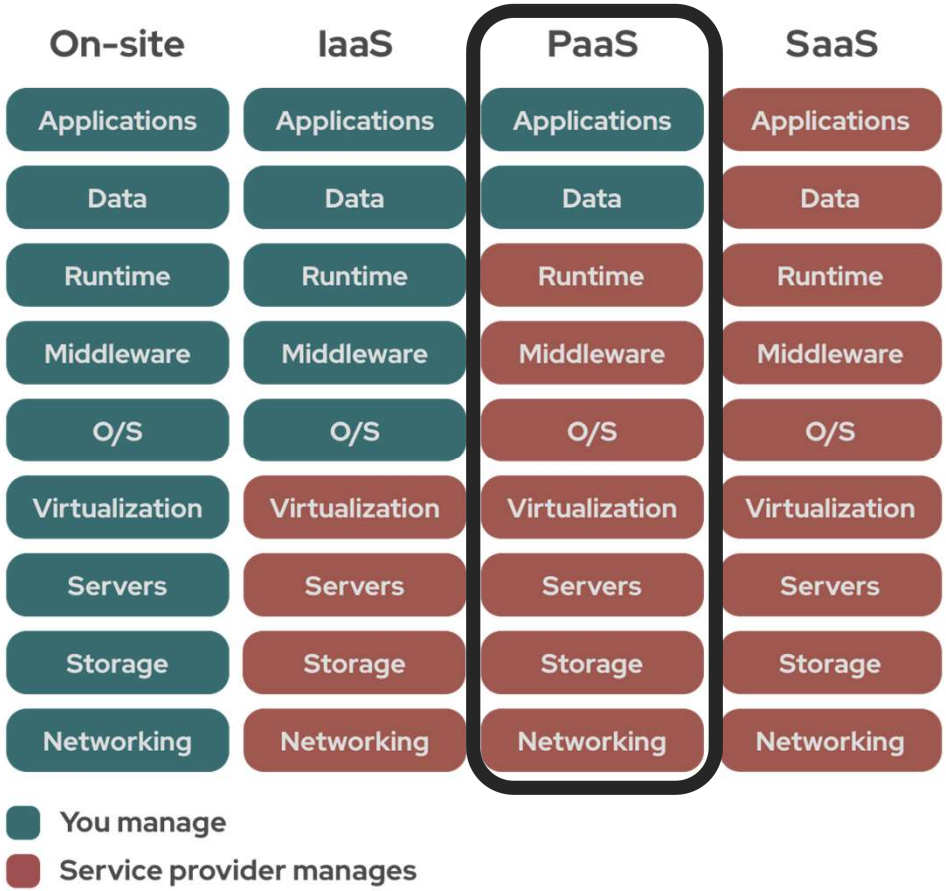


- Provides **VM** and other abstracted hardware and operating systems (**OSs**), which may be controlled through a service application programming interface (**API**).
- Enables subscribers to use on-demand fundamental IT resources, such as computing power, virtualization, data storage, and network.
- **Advantages**
  - Dynamic infrastructure scaling
  - Guaranteed uptime
  - Automation of administrative tasks
  - Elastic load balancing (ELB)
  - Policy-based services
  - Global accessibility
- **Disadvantages**
  - Software security is at high risk (third-party providers are more prone to attacks)
  - Performance issues and slow connection speeds

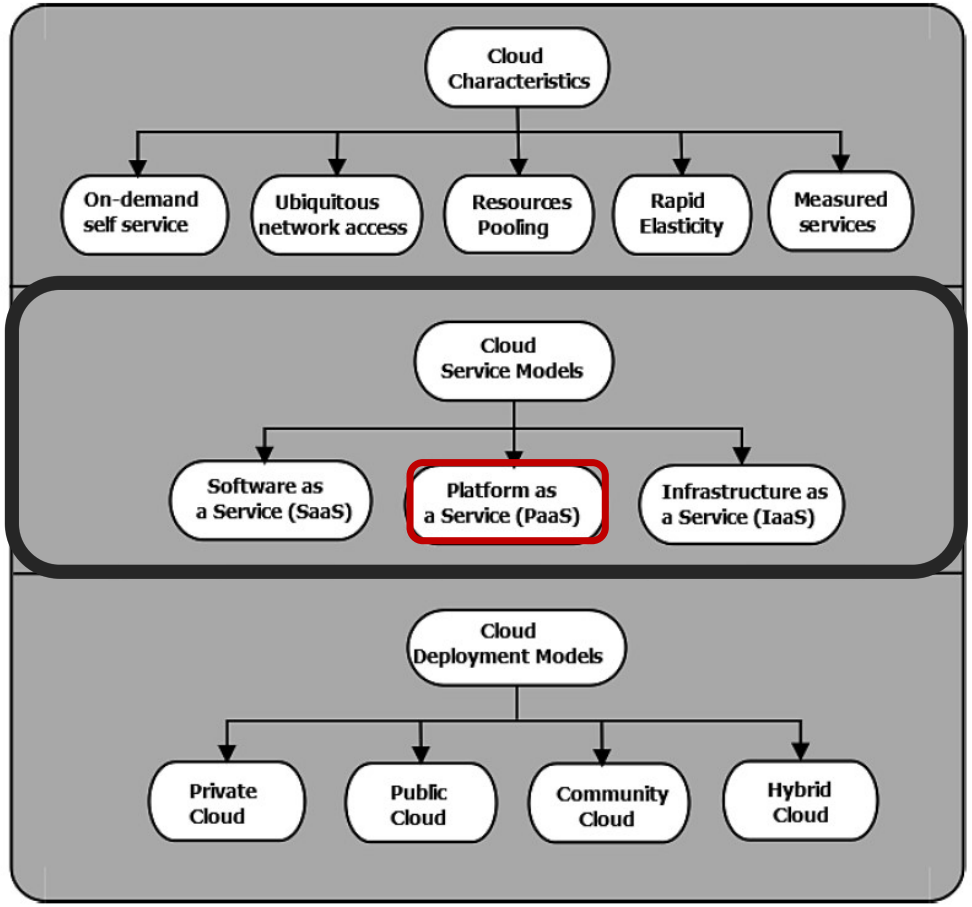
[Amazon Web Services]

Cloud Computing. Definitions and Characteristics





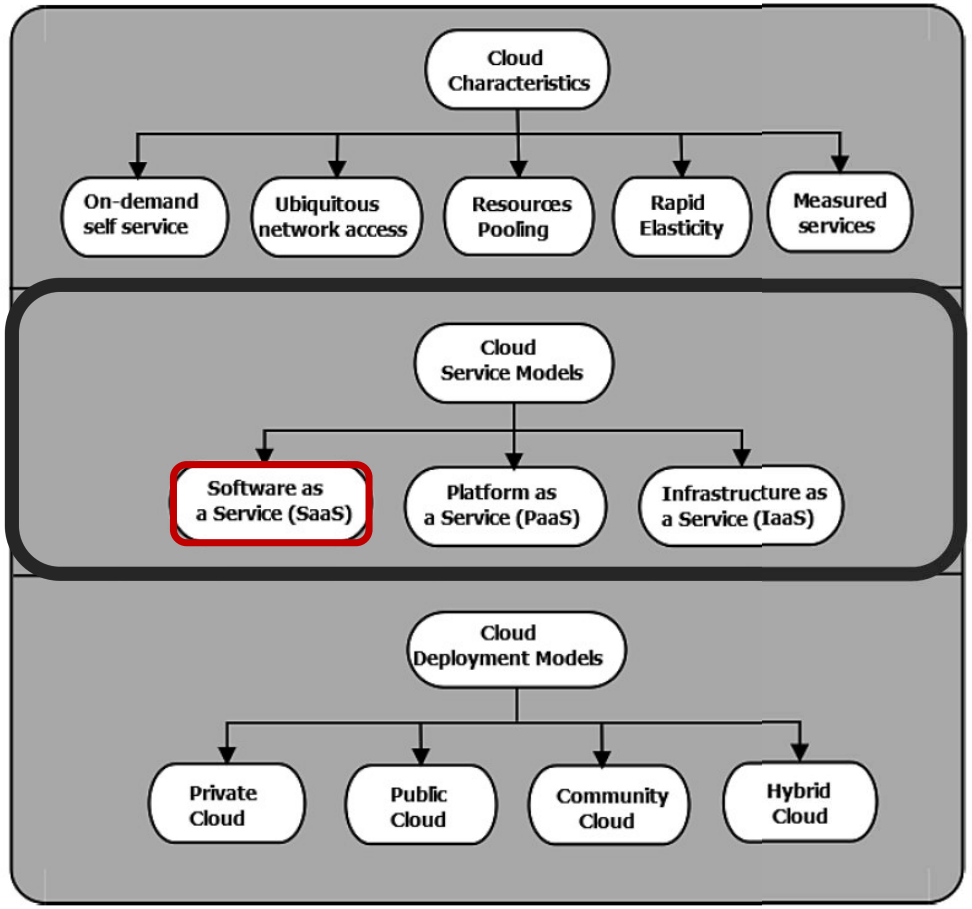
Cloud Computing. Definitions and Characteristics

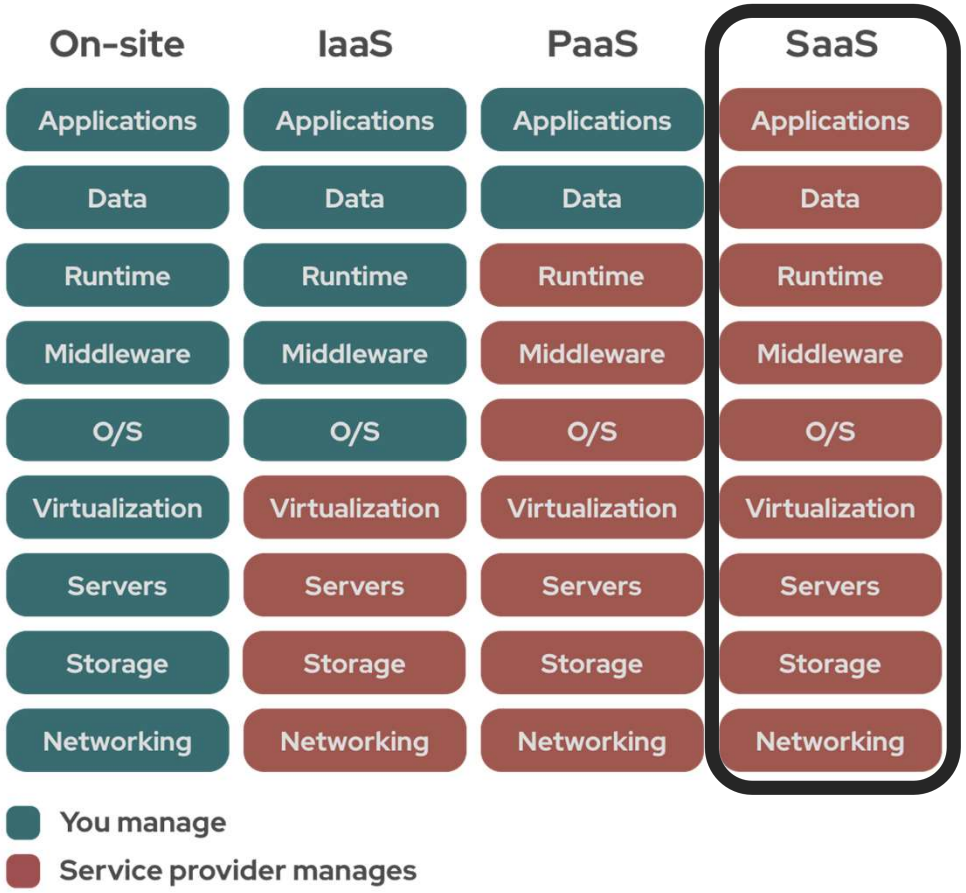


- Allows for the development of applications and services.
- This offers development tools, configuration management, and deployment platforms on-demand.
- Subscribers need not buy and manage the software and infrastructure underneath it but have authority over deployed applications and perhaps application hosting environment configurations.
- **Advantages**
  - Simplified deployment
  - Prebuilt business functionality
  - Lower security risk compared to laaS
  - Instant community
  - Pay-per-use model
  - Scalability
- **Disadvantages**
  - Vendor lock-in
  - Data privacy
  - Integration with the rest of the system applications

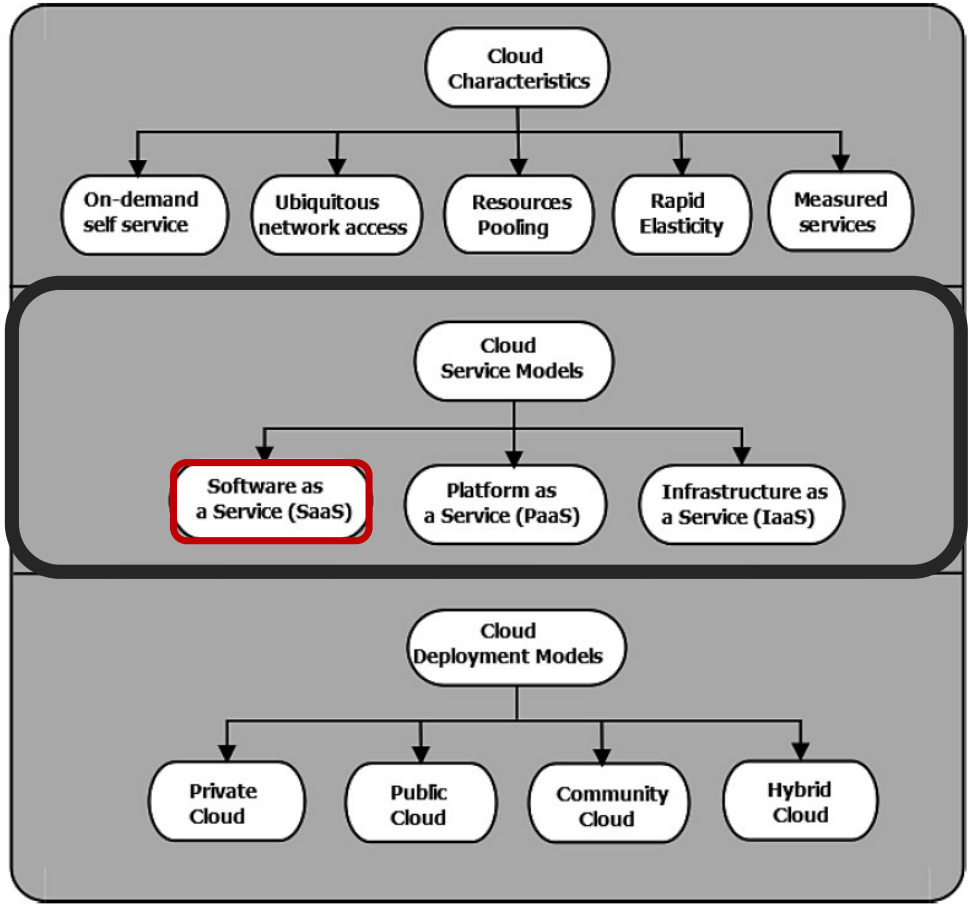
Google App Engine

Cloud Computing. Definitions and Characteristics





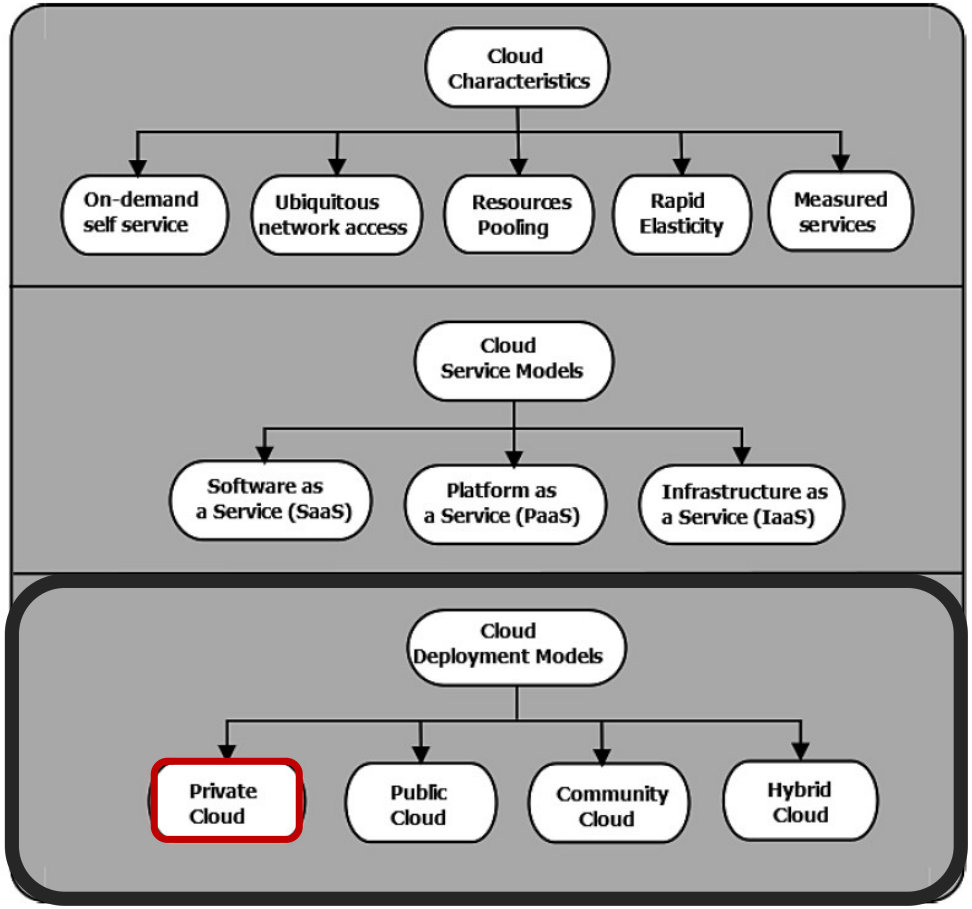
Cloud Computing. Definitions and Characteristics



- This cloud computing service offers application software to subscribers on-demand over the Internet.
- The provider charges for the service on a **pay-per-use** basis, by subscription, by advertising, or by sharing among **multiple users**
- **Advantages**
  - Low cost
  - Easy administration
  - Global accessibility
  - High compatibility (no specialized hardware or software is required)
- **Disadvantages**
  - Security and latency issues
  - Total dependency on the Internet
  - Switching between SaaS vendors is difficult

Microsoft 365

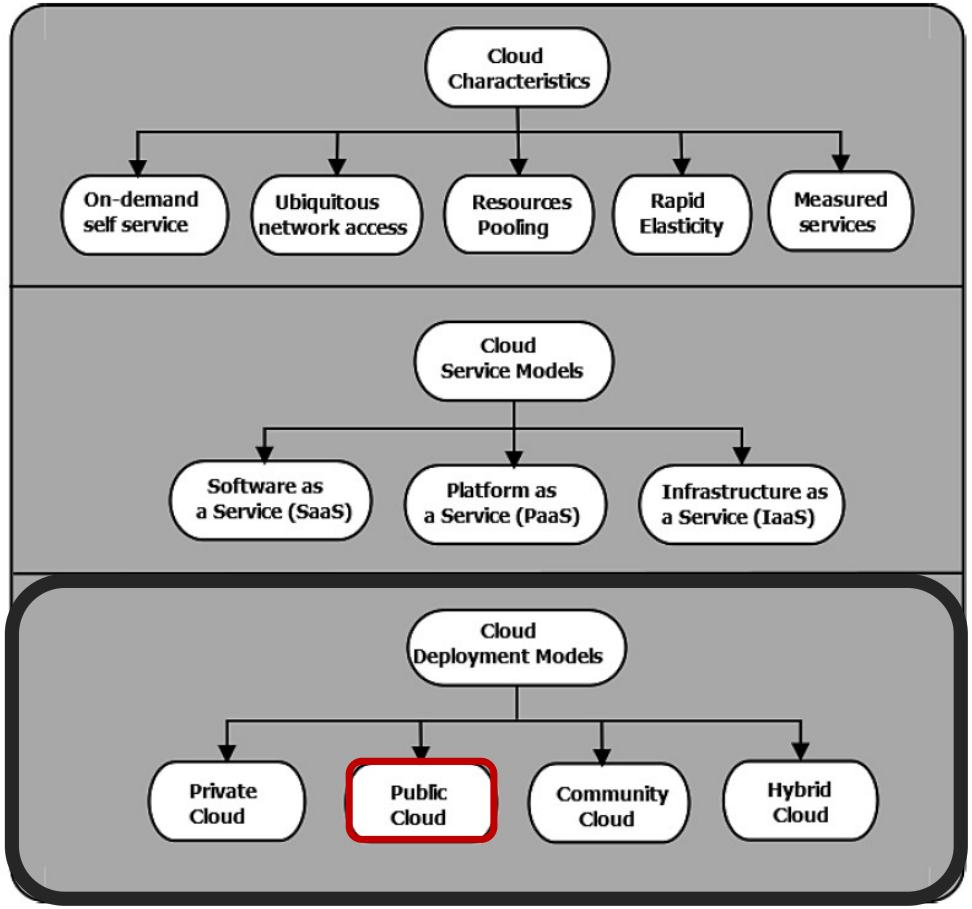
Cloud Computing. Definitions and Characteristics



- Cloud infrastructure operated by a single organization and implemented within a corporate firewall.
- Organizations deploy private cloud infrastructures to retain full control over corporate data
- **Advantages**
  - Security enhancement
  - Increased control over resources
  - High performance
  - Customizable hardware, network, and storage performances
- **Disadvantages**
  - High cost
  - On-site maintenance

E.g., BMC Software, VMware vRealize Suite, SAP Cloud Platform.

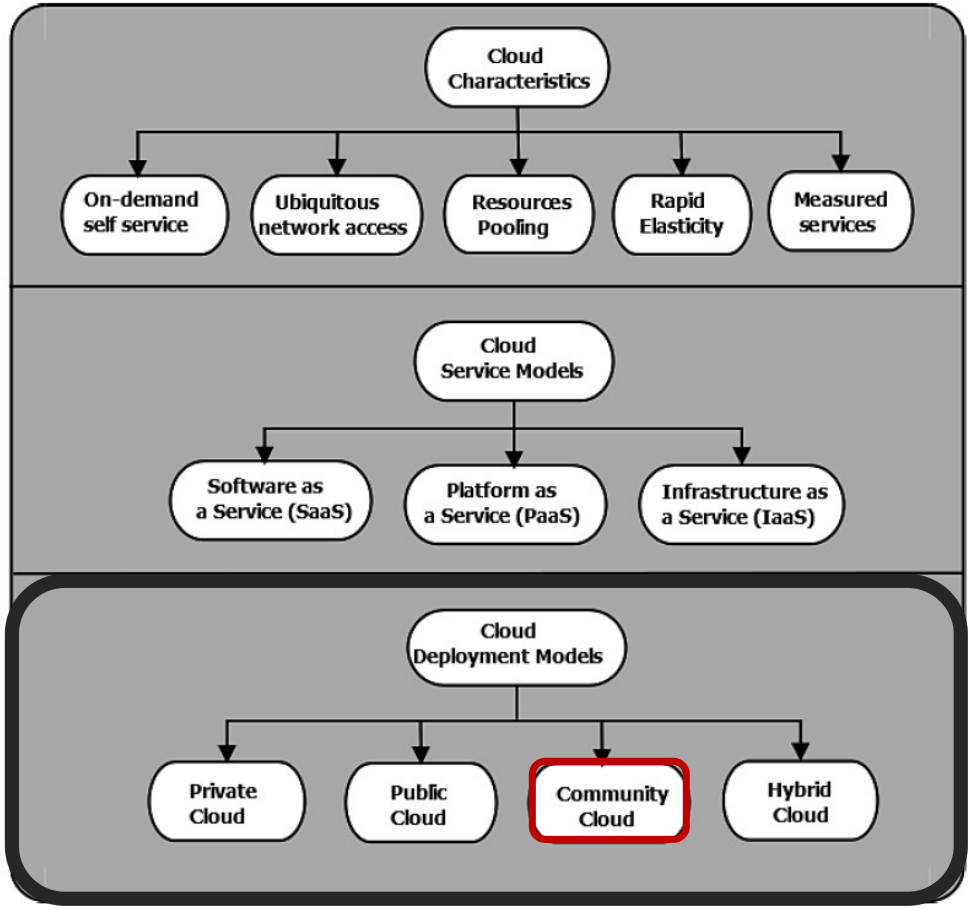
Cloud Computing. Definitions and Characteristics



- The provider makes services such as applications, servers, and data storage available to the public over the Internet.
- Based on a pay-per-usage model
- **Advantages**
  - Simplicity and efficiency
  - Low cost
  - Reduced time
  - No maintenance
  - No contracts
- **Disadvantages**
  - Security is not guaranteed
  - Lack of control
  - Slow speed

E.g., Amazon Elastic Compute Cloud (EC2), Google App Engine, Windows Azure Services Platform, IBM Bluemix.

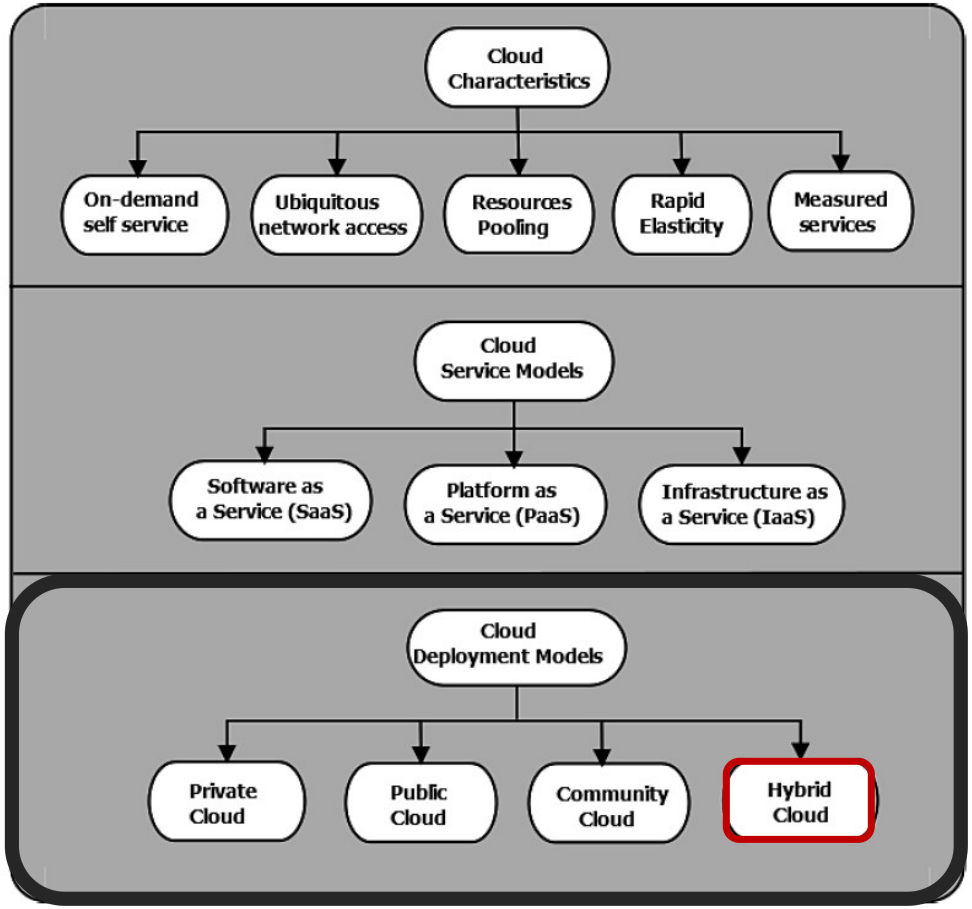
Cloud Computing. Definitions and Characteristics



- **Multi-tenant infrastructure** shared among organizations from a specific community.
- **Advantages**
  - Less expensive compared to the private cloud
  - Flexibility to meet the community's needs
  - Compliance with legal regulations
  - High scalability
  - Organizations can share a pool of resources from anywhere via the Internet
- **Disadvantages**
  - Competition between consumers in resource usage
  - Inaccurate prediction of required resources
  - Lack of legal entity in case of liability
  - Moderate security (other tenants may be able to access data)
  - Trust and security concerns between tenants

E.g., Optum Health Cloud, Salesforce Health Cloud.

Cloud Computing. Definitions and Characteristics



- Cloud environment comprised of two or more clouds (private, public, or community)
- **Advantages**
  - High scalability (contains both public and private clouds)
  - Offers both secure and scalable public resources
  - High level of security (comprises private cloud)
  - Allows to reduce and manage the cost according to requirements
- **Disadvantages**
  - Communication at the network level may be conflicted as it uses both public and private clouds
  - Difficult to achieve data compliance
  - Organization reliant on the internal IT infrastructure in case of outages (maintain redundancy across data centers to overcome)
  - Complex service level agreements (SLAs)

Example: An organization performs its critical activities on the private cloud (e.g., operational customer data) and non-critical activities on the public cloud.

Cloud Security

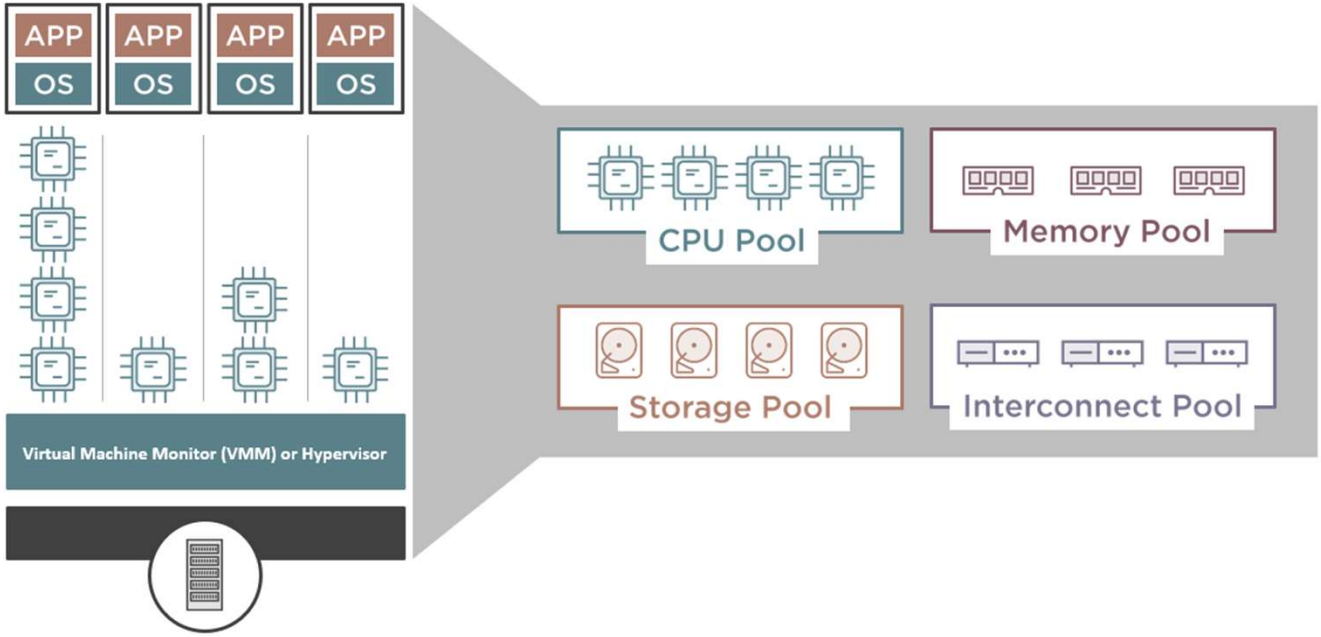
Cloud Security.
Concepts

- Some of the important security concepts associated with cloud are
  - Virtualization
  - Multi-tenancy
  - Data outsourcing
  - Trust management and meta security

Cloud Security.

Concepts. Virtualization

- It enables the extraction of computing resources, services, operating systems, and applications from the underlying infrastructure on which they run.



Cloud Security.

Concepts. Virtualization

2 key components of virtualization

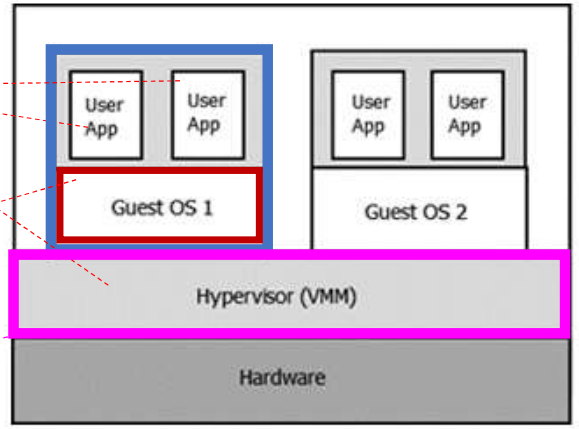
- **Virtual Machine (VM)**
  - Emulation of the physical resources
    - *RAM, virtual disk, virtual network interface card (vNIC), etc*
  - Runs an OS called as **guest OS**
- **Virtual Machine Monitor (VMM) or Hypervisor**
  - Runs above the HW or SW
  - Hides the complexity of physical HW
  - Allows the execution of multiple **guest OS** in same machine.
  - Can easily
    - Create
    - Delete
    - Run

    } different VMs having different OSes installed

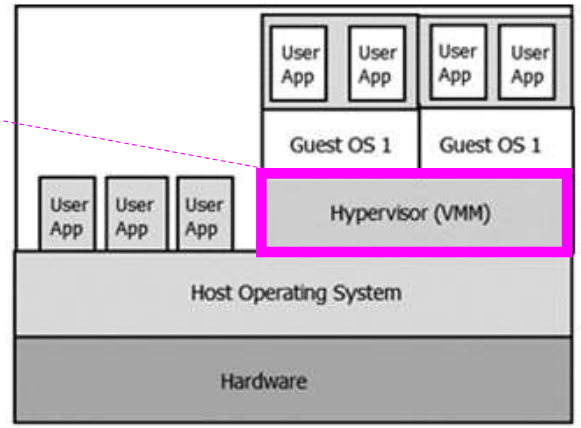
Is an essential requirement to provide the elastic and on-demand services in cloud computing!

A guest OS
- can host different applications
- Does not have direct access to HW.

There are two types of hypervisors



Bare Metal Hypervisor (called Type I)



Hosted Hypervisor (called Type II)

Cloud Security.

Concepts. Multi-tenancy

- **multi-tenancy (IaaS)**
  - sharing Hypervisor or VMM* among *n* VMs.
- **multi-tenancy (PaaS)**
  - allows **users** to share the same developing platform such as Java Virtual Machine (JVM) and .NET platform.
- **multi-tenancy (SaaS)**
  - enables the **provider** to share the app-software among multi-tenant users.

NOTE: ***Multi-tenancy***
provides benefits to the provider
expands the threat model (Cross VM side channel attack, DoS, etc.)

**Virtual Machine Monitor (VMM) or Hypervisor*

Cloud Security.

Concepts.Data outsourcing

- It refers to the transferring of the computing, security, and especially storage to **off-premise** third party organization which controls the off-premise infrastructure.
  - Reduce cost!
  - Disadvantages
    - Customer loss their physical control over data.
    - Causes privacy violation.

In order to resolve this issue, customers need to be very careful while selecting a **trusted CSP**

Cloud Security.

Concepts. Trust management

- The security of tenant's data
  - Relies on the security management policies implemented by CSP
  - Tenants must trust on them.

A trusted third-party (TTP) can authorize, audit the sensitive data of tenants and provides the security from illegitimate users.

Cloud Security.

Concepts. Metadata security

- Cloud Organizations also maintains the massive number of **metadata**
- **Metadata** contains sensitive information in different format.
- Security Actions
  - Data sanitization *(delete != doesn't exist) → carving*
  - Data separation *(hard disk being shared among multiple tenants)*
  - Data maintenance *(Maintaining the metadata along with the applications)*

Exercise: Read this lightweight post:
https://www.geeksforgeeks.org/what-is-wsdl-attack/

Example

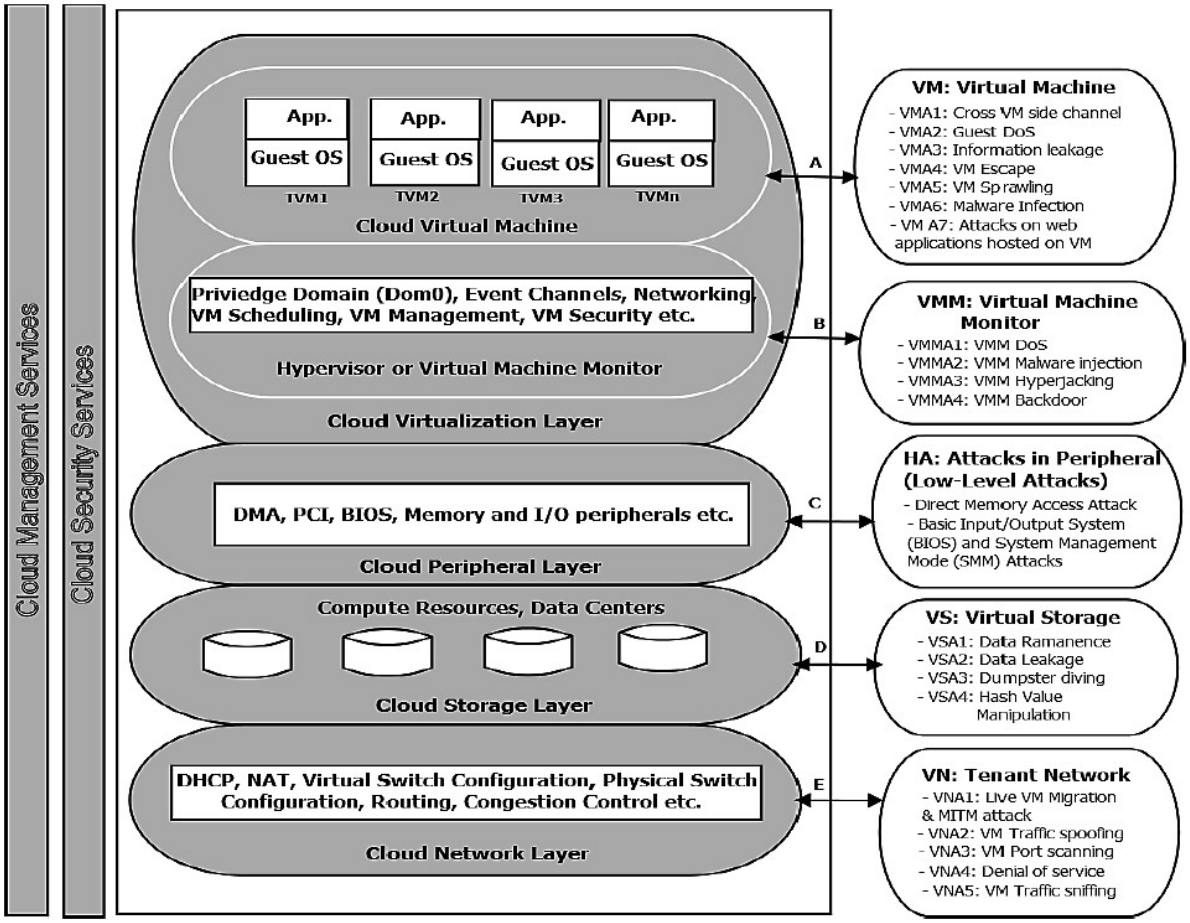
- WSDL is one of the examples of metadata.
- An attacker can exploit the WSDL and modify it.
- This may cause the leakage of the user's confidential data.

***metadata = "data about data"**

Classification based on the target component

Cloud Security. A Taxonomy of Attacks.

- Specific attacks in the virtual environment
  - Virtual machines-level attacks
  - Virtual machine monitor-level attacks
  - Peripheral–level attacks
  - Virtual storage-level attacks
  - Tenant network-level attacks

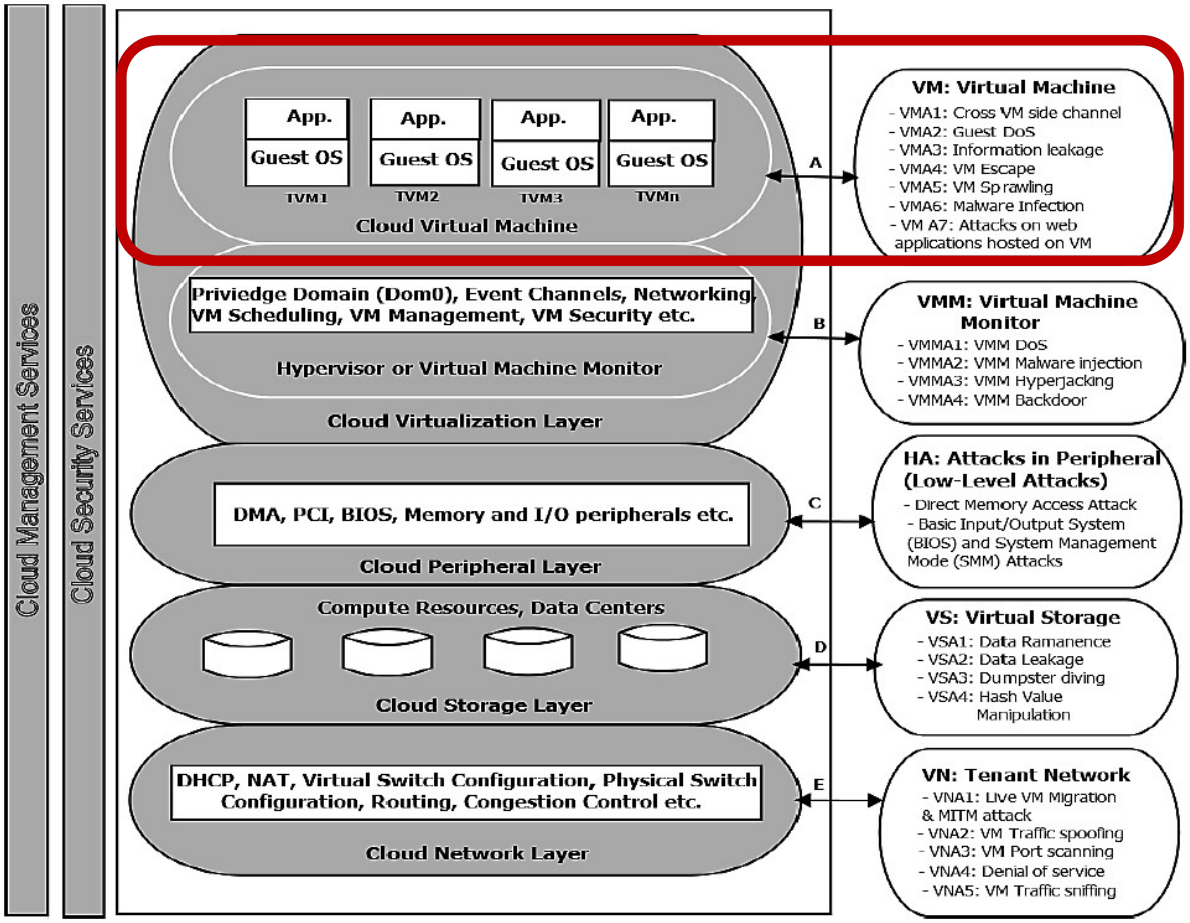


Cloud Security. A Taxonomy of Attacks.

VMAT: Virtual machines-level attacks

Classification based on the target component

- VMs are one of the most critical cloud resources
- VMs could be easily bypassed by attacker in cloud because of its easy accessibility.

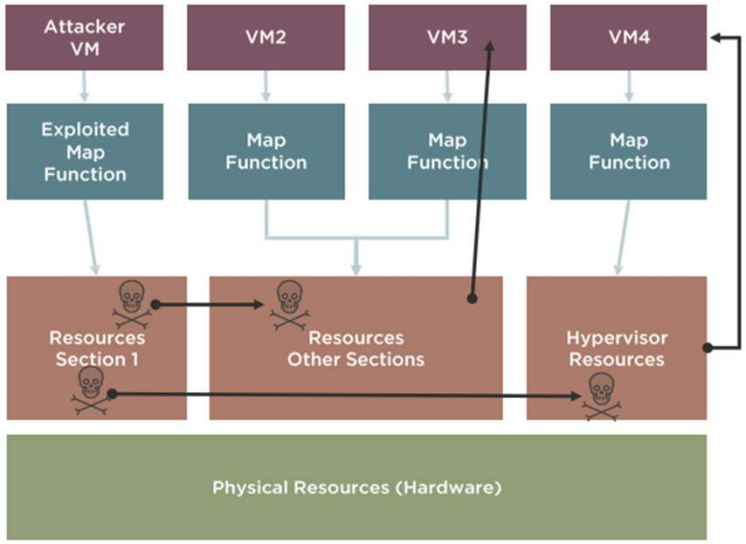


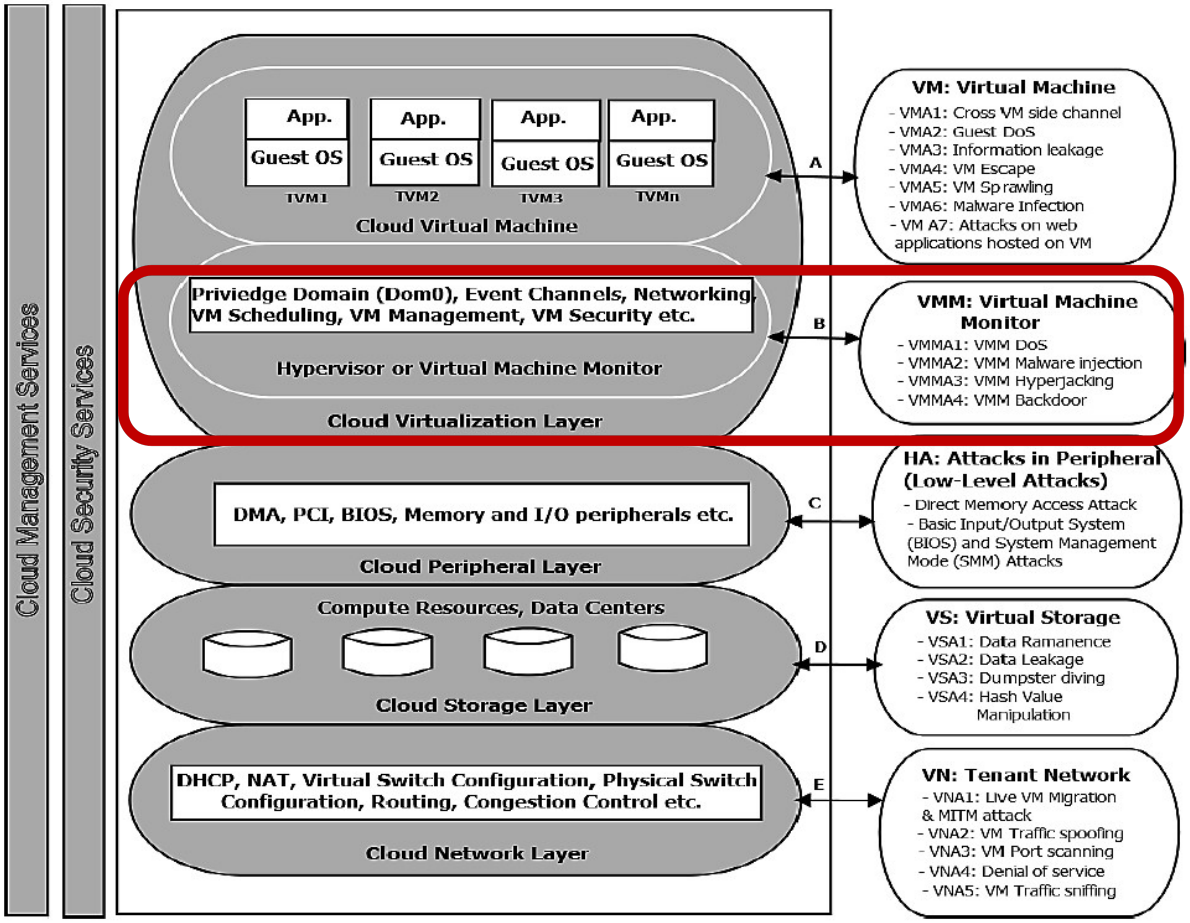
Cloud Security. A Taxonomy of Attacks.

VMMAT: Virtual machine monitor-level attacks

Classification based on the target component

- Attacker can also exploit the vulnerability present in the hypervisor code in taking control of VMM kernel.
- Once a VMM is compromised, it can perform harmful operations and gain access to the VM memory.



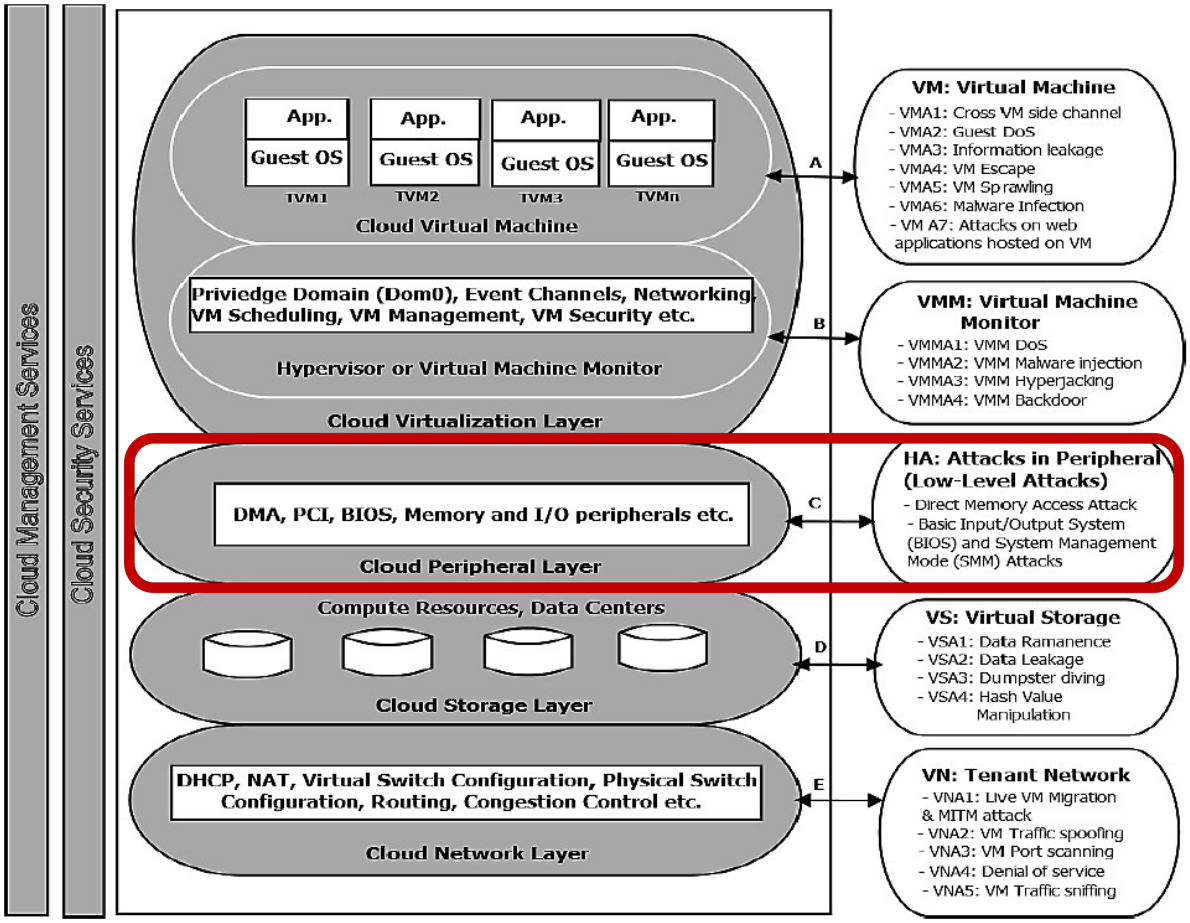


Cloud Security. A Taxonomy of Attacks.

HWAT: Peripheral–level attacks

Classification based on the target component

- Once an attacker has physical access to a memory, he/she can launch hardware threats.
- Some of such threats which target the integrity of the tenant's data and are launched at the peripheral-level.

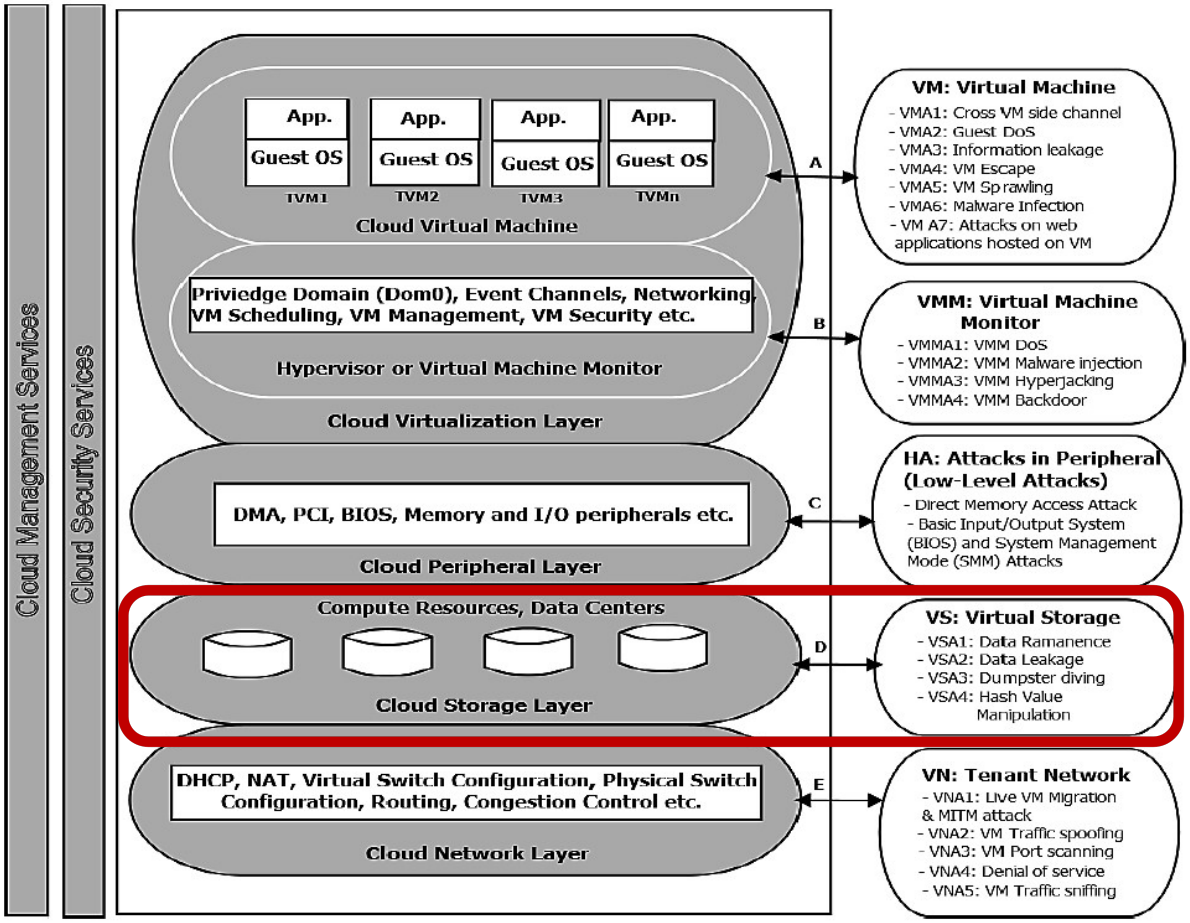


Cloud Security. A Taxonomy of Attacks.

VSWAT: Virtual storage-level attacks

Classification based on the target component

- The sharing of physical storage among many tenants can be exploited.

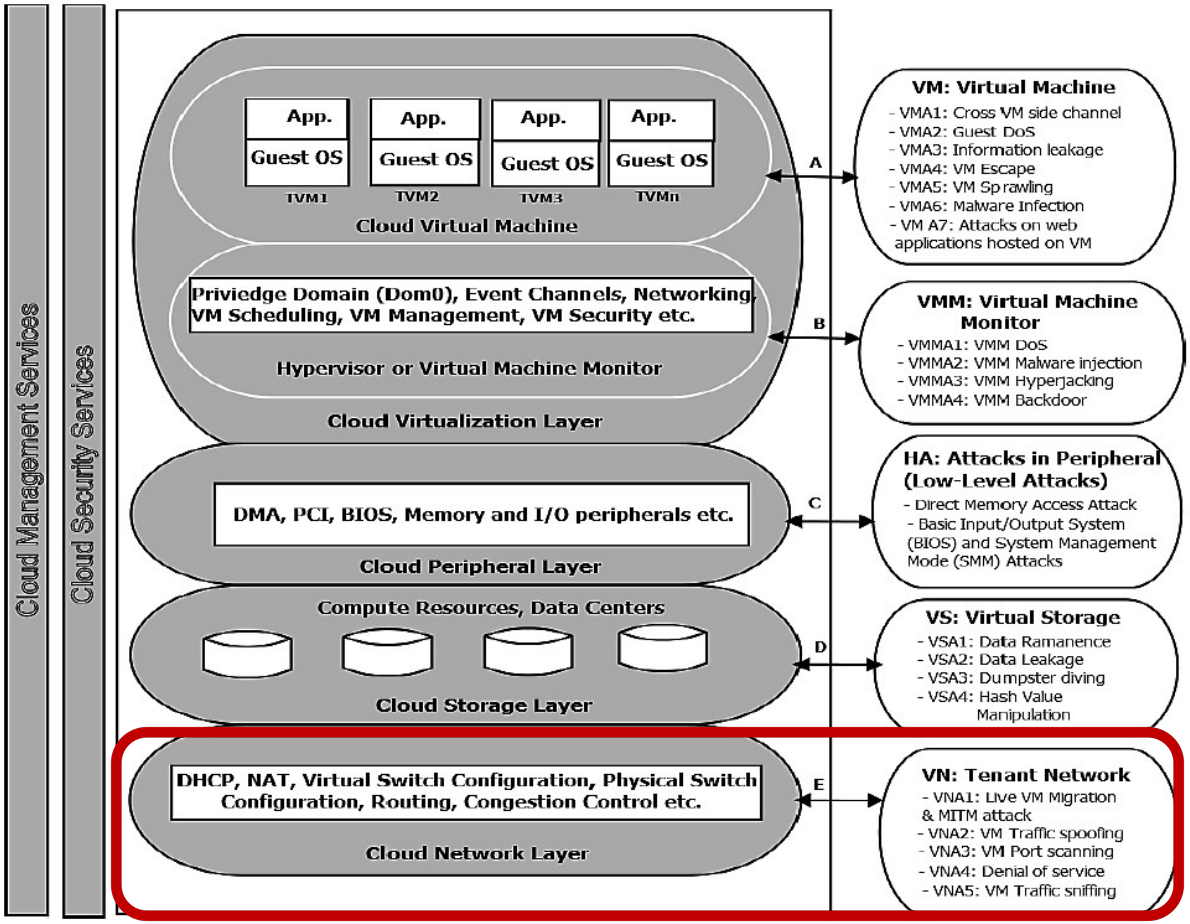


Cloud Security. A Taxonomy of Attacks.

TENAT: Tenant network-level attacks

Classification based on the target component

- Network attacks are also possible in the cloud environment which targets the network vulnerabilities.



Cloud Security. OWASP Top 10 Cloud Security Risks.

- **Create by OWASP***
- Develops & maintains top 10 cloud risks
- Serve as a quick list of top cloud risks
- Provide guidelines on mitigating the risks
- Easily Executable
- Most Damaging
- Incidence Frequency

Cloud Top 10 Risks
R1: Accountability & Data Risk
R2: User Identity Federation
R3: Regulatory Compliance
R4: Business Continuity & Resiliency
R5: User Privacy & Secondary Usage of Data
R6: Service & Data Integration
R7: Multi-tenancy & Physical Security
R8: Incidence Analysis & Forensics
R9: Infrastructure Security
R10: Non-production Environment Exposure

** The Open Web Application Security Project is an online community that produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security.*

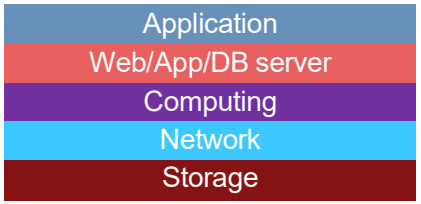
https://www.techiexpert.com/understanding-owasp-top-10-cloud-security-risks/

Cloud Security. OWASP Top 10 Cloud Security Risks.

R1 - Accountability and Data Ownership

- ***Organizations use the public cloud for hosting business services instead of a traditional data center.***

In traditional data center, the owning organization is responsible for security at all layers



You can outsource hosted services, but you cannot outsource responsibility

In a cloud, who is accountable for security at these layers?

Cloud Security. OWASP Top 10 Cloud Security Risks.
R2 - User Identity Federation

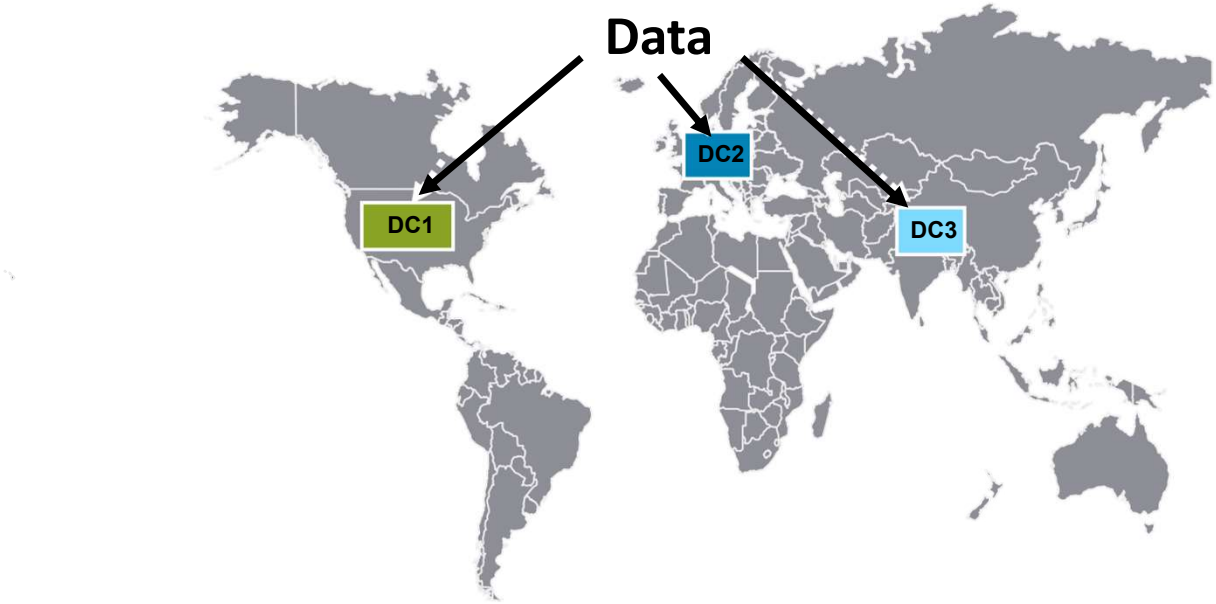
- Enterprises use services and applications of different cloud providers, creating multiple user identities and complicating the management of multiple user IDs and credentials.
- Cloud providers have less control over the user lifecycle /offboarding.

SECURITY RISKS

1. **Managing Identities across multiple providers**
2. **Less control over user lifecycle (off- boarding)**
3. **User experience**

Cloud Security. OWASP Top 10 Cloud Security Risks.
R3 – Regulatory Compliance

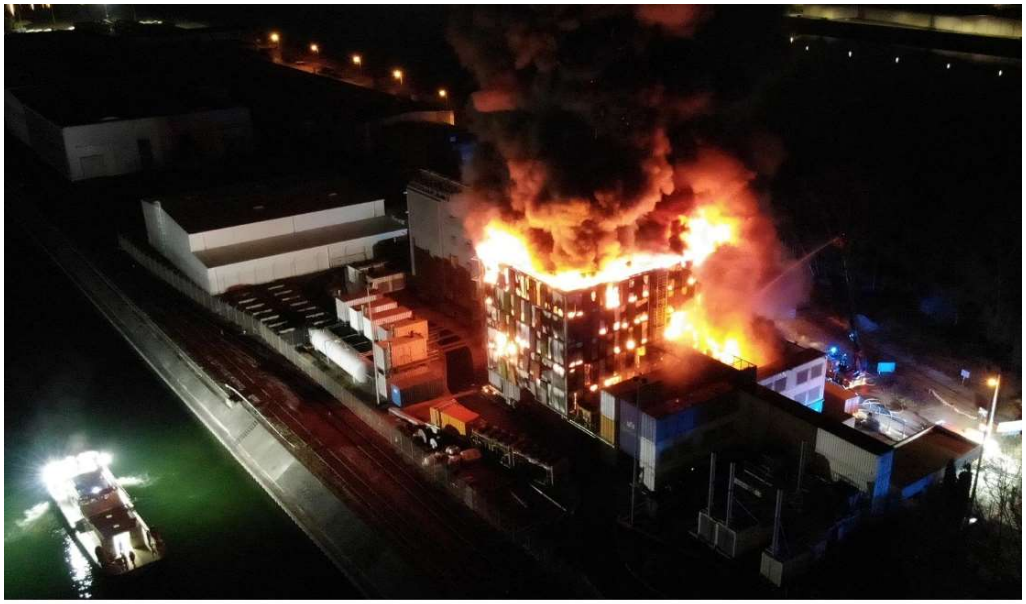
- Following regulatory compliance can be complex.
- Data that is secured in one country may not be secured in another country owing to the lack of transparency and different regulatory laws followed across various countries.



In EU…GDPR?

Cloud Security. OWASP Top 10 Cloud Security Risks.
R4 - Business Continuity and Resiliency

- Performing Business Continuity Planning (BCP) in an IT organization ensures that the business can be conducted in a disaster situation.
- When organizations use cloud services, there is a chance of risk or monetary loss if the CSP handles the BCP improperly.



THE BUSINESS STANDARD
Sunday
September 18, 2022

Fire destroys some servers at French data company OVHcloud

Fire destroyed the servers at French data company OVHcloud

Cloud Security. OWASP Top 10 Cloud Security Risks.
R5 - User Privacy and Secondary Usage of Data

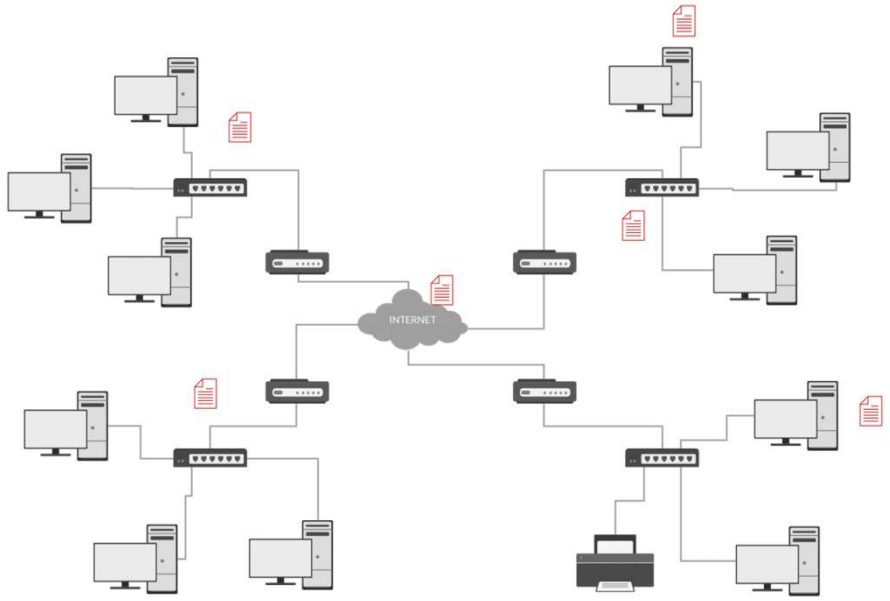
- The use of social websites poses a risk to personal data because they are stored in the cloud and most social application providers mine user data for secondary usage.
- The default share feature in social networking sites can jeopardize the privacy of user personal data.

De-identification of personal Information? → Anonymization
Terms of Service with providers: Responsibility on compliance? Geographical affinity?
Encrypted storage?
Policy Enactment?

Cloud Security. OWASP Top 10 Cloud Security Risks.

R6 - Service and Data Integration

- Organizations must ensure proper protection when proprietary data are transferred from the end-user to the cloud data center.
- **Unsecured data in transit** are susceptible to eavesdropping and interception attacks.



Data traverses through the internet between end users and cloud data centers.

How secure the integrations are ?

Encryption (keys, protocols, etc.) of the data in transit and rest?

Cloud Security. OWASP Top 10 Cloud Security Risks.
R7 - Multi Tenancy and Physical Security

- Cloud technology uses the concept of multi-tenancy for sharing resources and services among multiple clients, such as networking, databases.
- Inadequate logical segregation may lead to tenants interfering with each other's security features.

Data Encryption (per tenant key management)?
Controlled and coordinated Change Management?
Transparency/Auditability of Administrative Access?
Regular Third-Party Assessments?
Virtual Private Cloud (VPC)?

Cloud Security. OWASP Top 10 Cloud Security Risks.
R8 - Incidence Analysis and Forensic Support

- When a security incident occurs, investigating applications and services hosted at a cloud provider can be challenging because event logs are distributed across multiple hosts and data centers located at several countries and governed by different laws and policies.
- Owing to the distributed storage of logs across the cloud, law enforcing agencies may face problem in forensics recovery.

Implications to Traditional Forensics ?
Comprehensive logging?
Without compromising Performance?
Dedicated Forensic VM Images?

Cloud Security. OWASP Top 10 Cloud Security Risks.
R9 – Infrastructure Security

- Configuration baselines of the infrastructure should comply with the industry best practices because there is constant risk of malicious actions.
- Misconfiguration of infrastructure may allow network scanning for vulnerable applications and services to retrieve information, such as active unused ports and default passwords and configurations.

Segregation of duties and role based administrative privileges?
Third party audits and app vulnerability assessments?'
Tiered architecture with appropriate security controls between them?
Hardening – Networks, OS, Apps, etc. ?

Cloud Security. OWASP Top 10 Cloud Security Risks.

R10 - Non-Production Environment Exposure

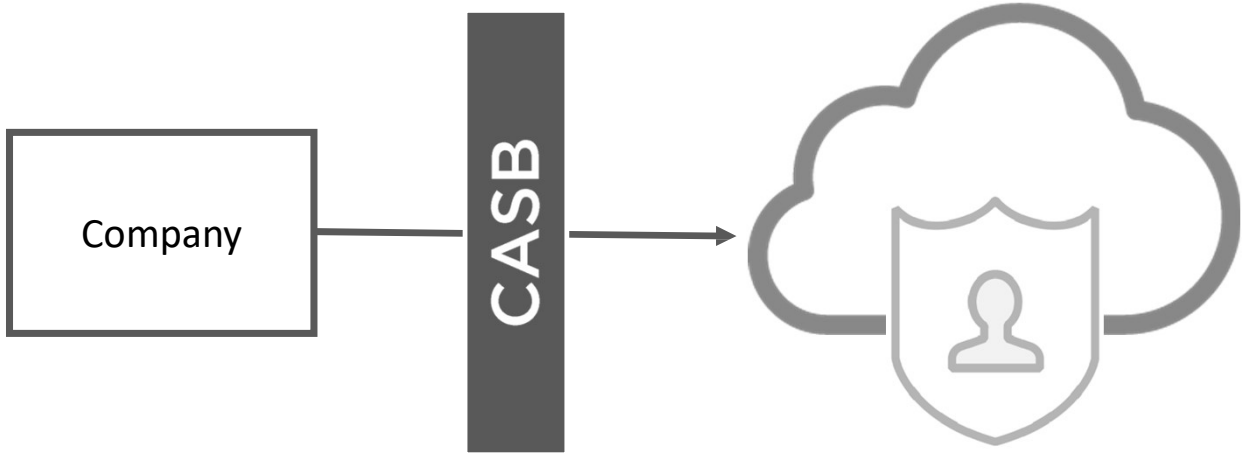
- Non-production environments are used for application design and development and to test activities internally within an organization.
- Using non-production environments increases the risk of unauthorized access, information disclosure, and information modification.

Security flaws
Typical non-prod environment use generic authentication credentials
Data copied to non-prod from its production equivalent
High risk of an unauthorized user getting access to the nonproduction environment
Use multi layers of authentication?
Non-prod data is not identical to production?
Don’t use cloud for developing a highly sensitive app in the cloud!

Cloud Security.

Cloud Access Security Broker (CASB)

- On-premises or in the cloud
- Place between the company (consumer) and the cloud provider
- Ensure policies are enforced when accessing cloud-based assets
  - Authentication / Single sign-on
  - credential mapping
  - Device profiling
  - Logging



Cloud Security.

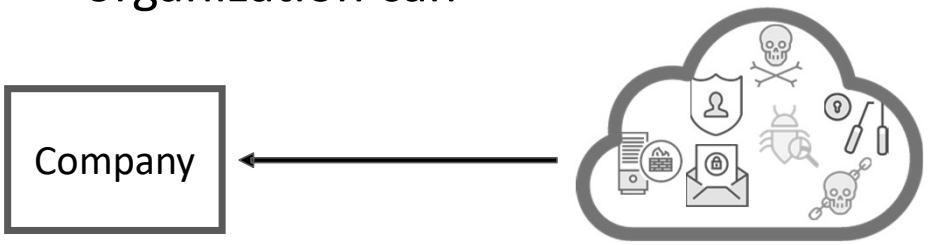
Security as a Service (SECaaS)

- Cloud providers that can offer security services cheaper or more effectively than on-premises:
  - Authentication
  - Antivirus malware spyware
  - Intrusion detection
  - Pentesting
  - SIEM

Cloud Security.
SECaaS vs CASB

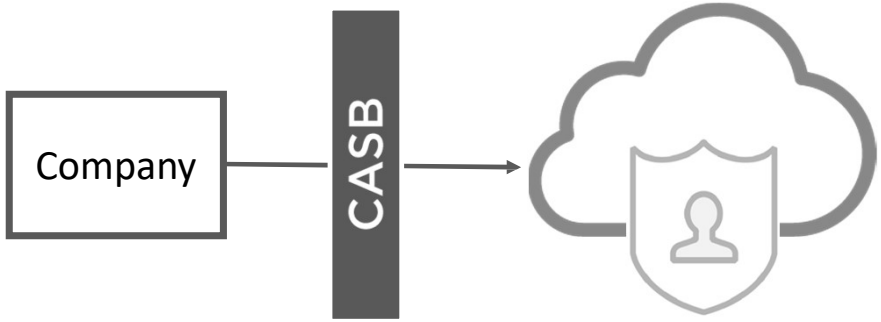
SECaaS

- Cloud providers offer their services, infrastructure, resources, etc., to extend into a company's network
- They provide the security services typically at a cheaper Total Cost of Ownership (TCO) than the customers organization can



CASB

- Sits between a customer's network and the cloud, acting as a broker or services gateway
- Enforces the customer organizations policies when access anything in the cloud



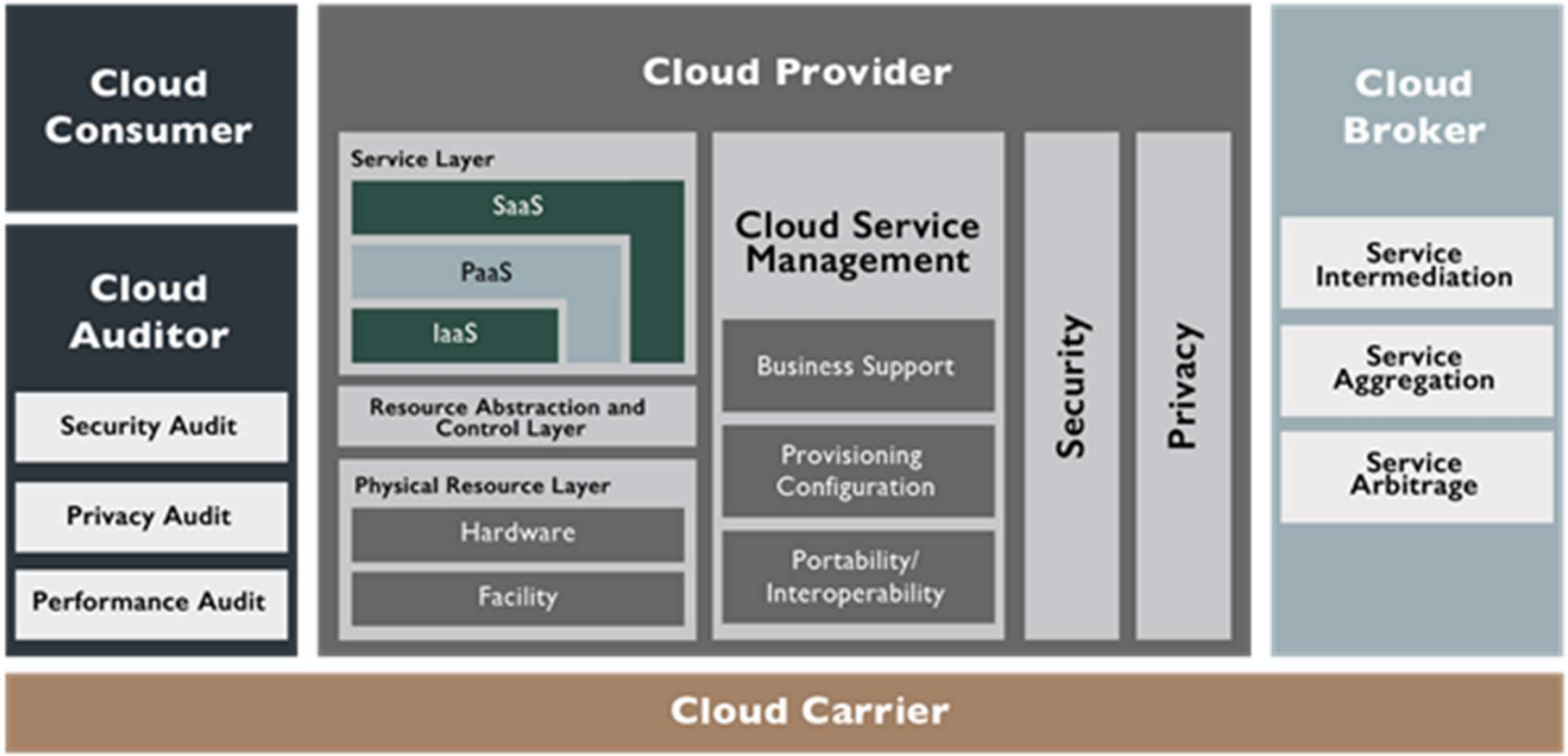
Cloud Security.

Standards

- Information technology infrastructure library (ITIL)
- Control objectives for information and related technology (COBIT)
- ISO/IEC 20000
- Statement on standards for attestation engagement (SSAE)
- Cloud security alliance (CSA) cloud controls matrix

Cloud Security

NIST Cloud Reference Model



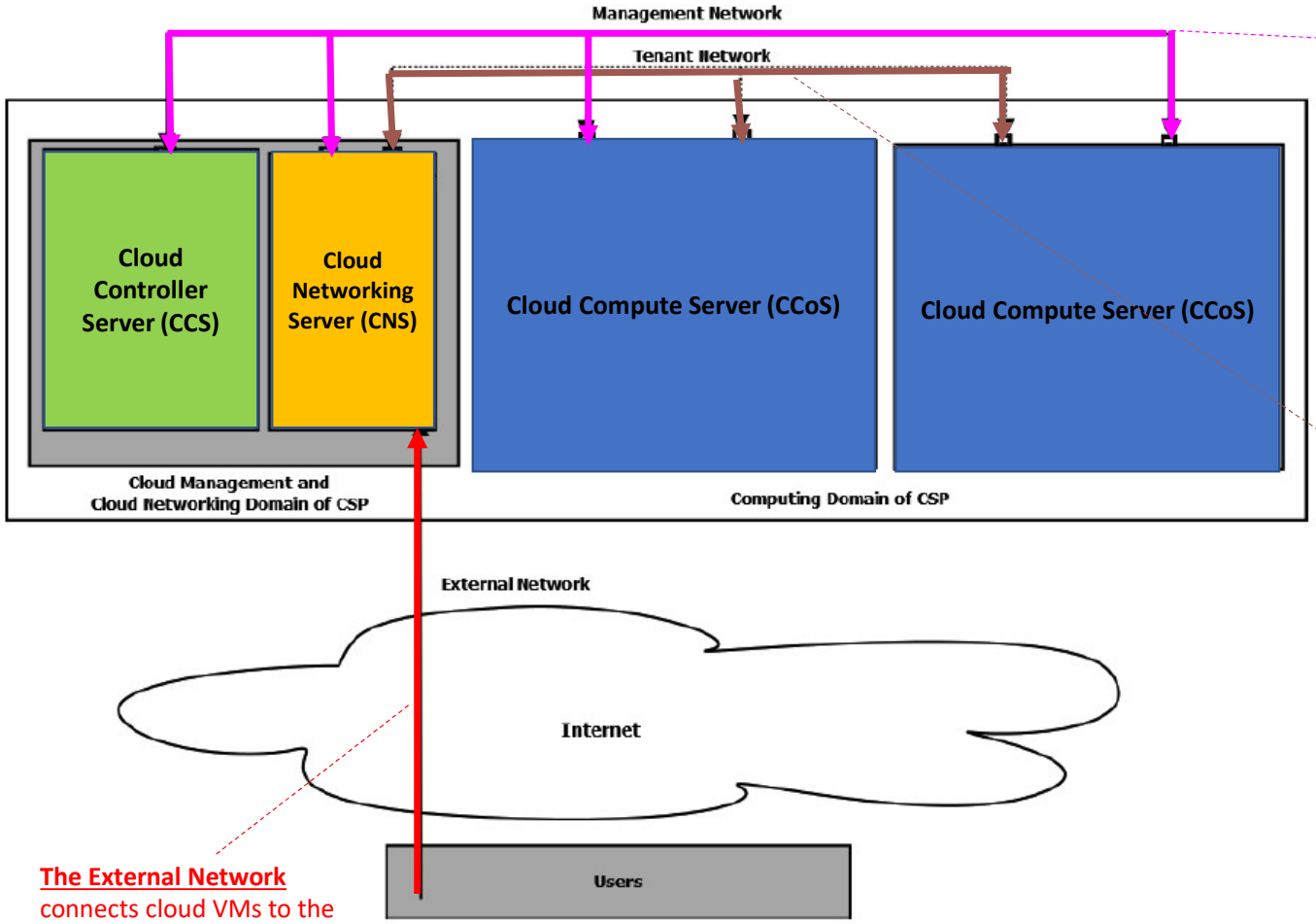
Cloud Security.

NIST Recommendations for Cloud Security

- Assess the risk posed to the client's data, software, and infrastructure.
- Select an appropriate deployment model according to needs.
- Ensure audit procedures are in place for data protection and software isolation.
- Renew SLAs in case of security gaps between the organization's security requirements and cloud provider's standards.
- Establish appropriate incident detection and reporting mechanisms.
- Analyze the security objectives of the organization.
- Enquire about who is responsible for data privacy and security issues in the cloud.

Attack Examples

Threat Model. Basic architecture of cloud environment



The Management Network: deals with carrying the data corresponding to management commands such as allocating, destroying, creating, and resuming Tenant Virtual Machines (TVM).

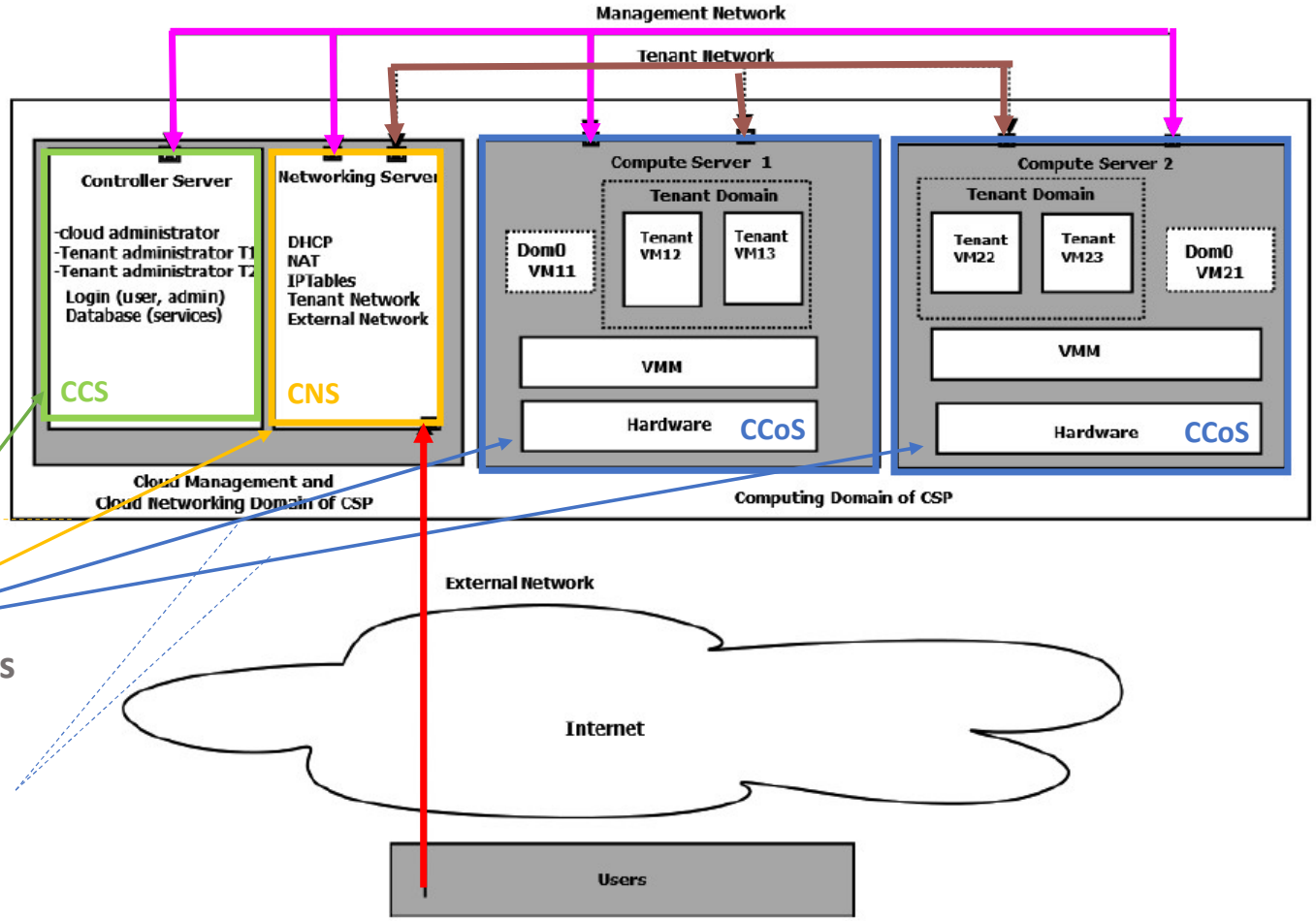
The Tenant Network

- Carries the tenant's data and ensures the end-to-end transportation.
- Each tenant network connects a set of VMs and is vulnerable to the threats.

The servers are interconnected together through three different networks

The External Network connects cloud VMs to the external users via Internet

Threat Model. Basic architecture of cloud environment



Handle all management-related work.

Manages the network, routes the packets, and allocates IPs to the nodes, etc.

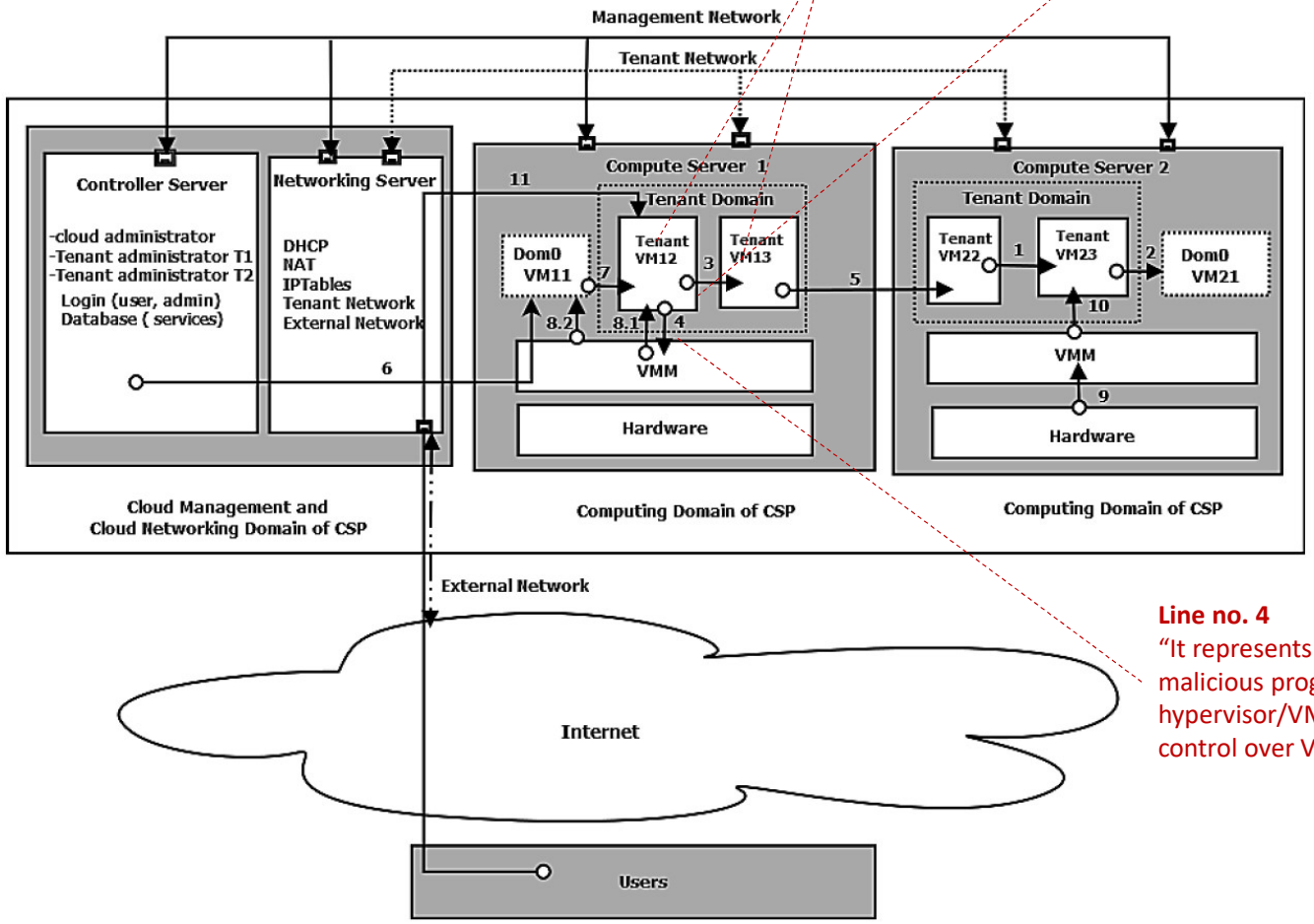
Cloud Servers Types

The user VMs are hosted in CCoS server

Threat Model.
Diagram explanation

VM12 and VM13
are running in the same physical machine

Line no. 3
"It represents that malicious program running VM12 can access and run some malware in the collocated VM13."



Line no. 4
"It represents that VM12 can run some malicious programs to gain access to hypervisor/VMM memory and take control over VMM."

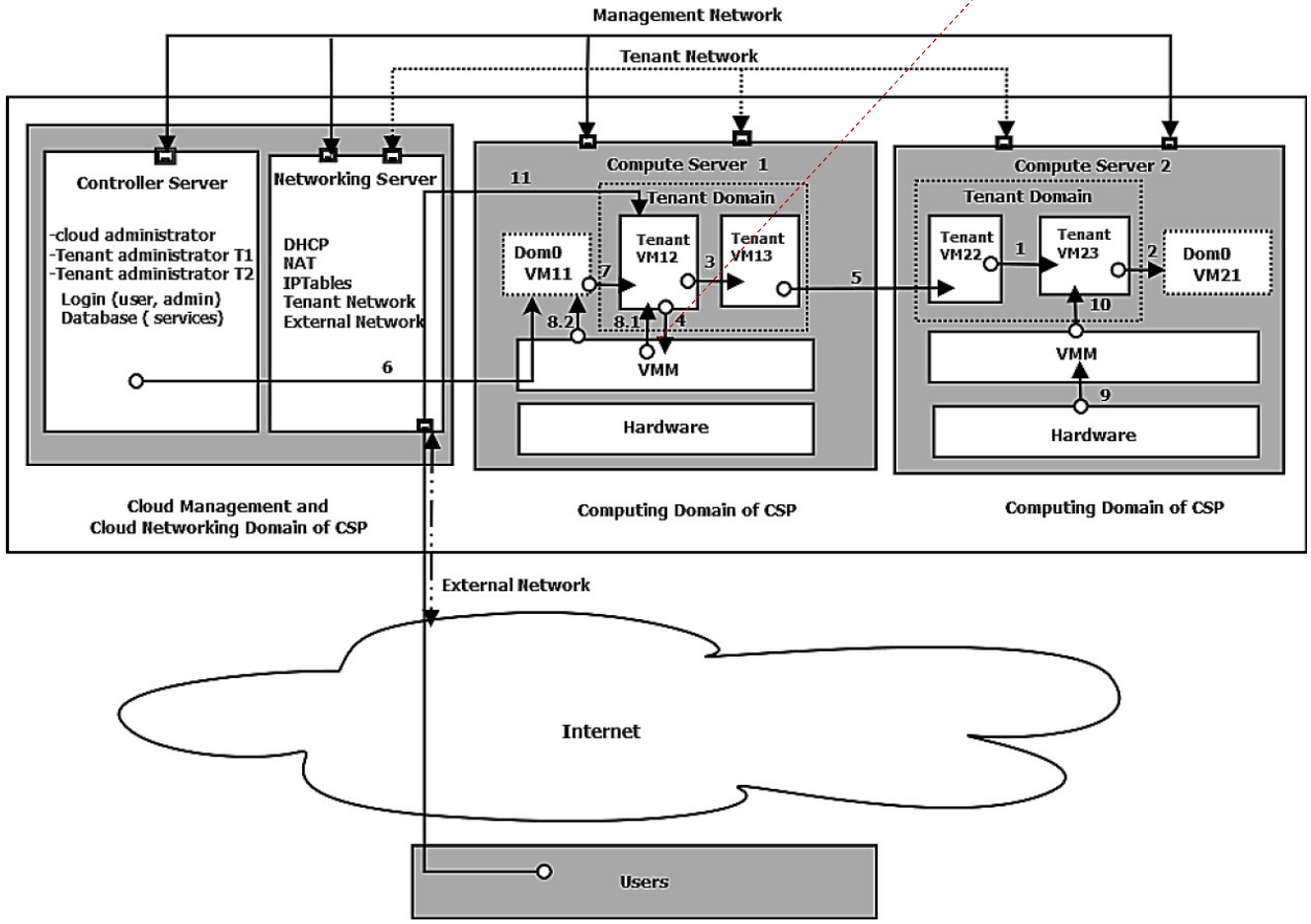
Each arrow line is pointing the:
Attack Source (empty circle)
Attack Destination (arrow sign)

Threat Model.

Scenario 1: VM-VM attack

- Attacker becomes successful in bypassing the access of another TVM
- Attacker can execute the rootkit malwares in guest machine in order to gain the root access of the victim machine.
- A rootkit can hide the intrusions and executes with higher privileges of guest OS.
- Such malware can cause the harm to the victim VM.
- Some of rootkits are evasive in nature and can subvert the security analyzer running inside the victim VM.

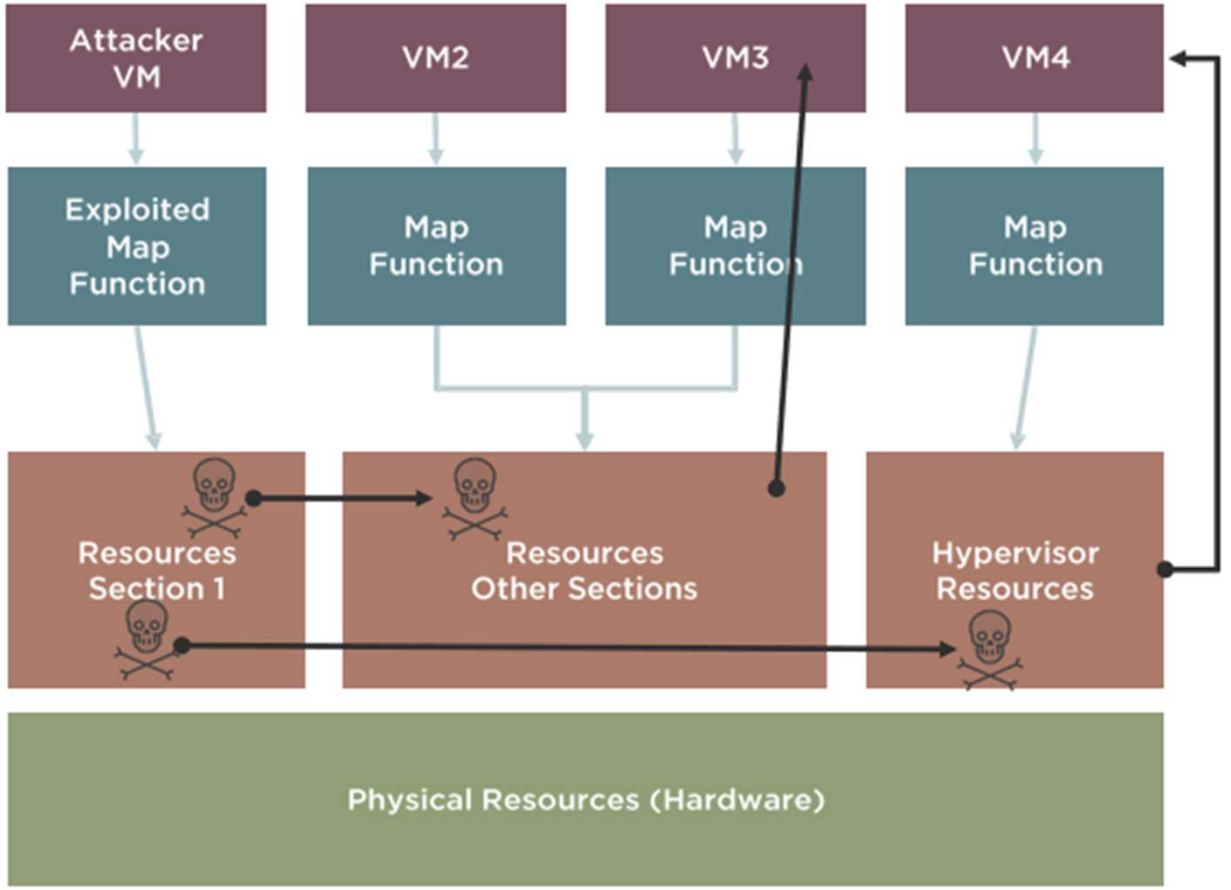
Line no. 1
A Tenant Virtual Machine (TVM)'s user can try to access another TVM maliciously by using the privilege escalation techniques.



Threat Model.

Scenario 2: VM Escape

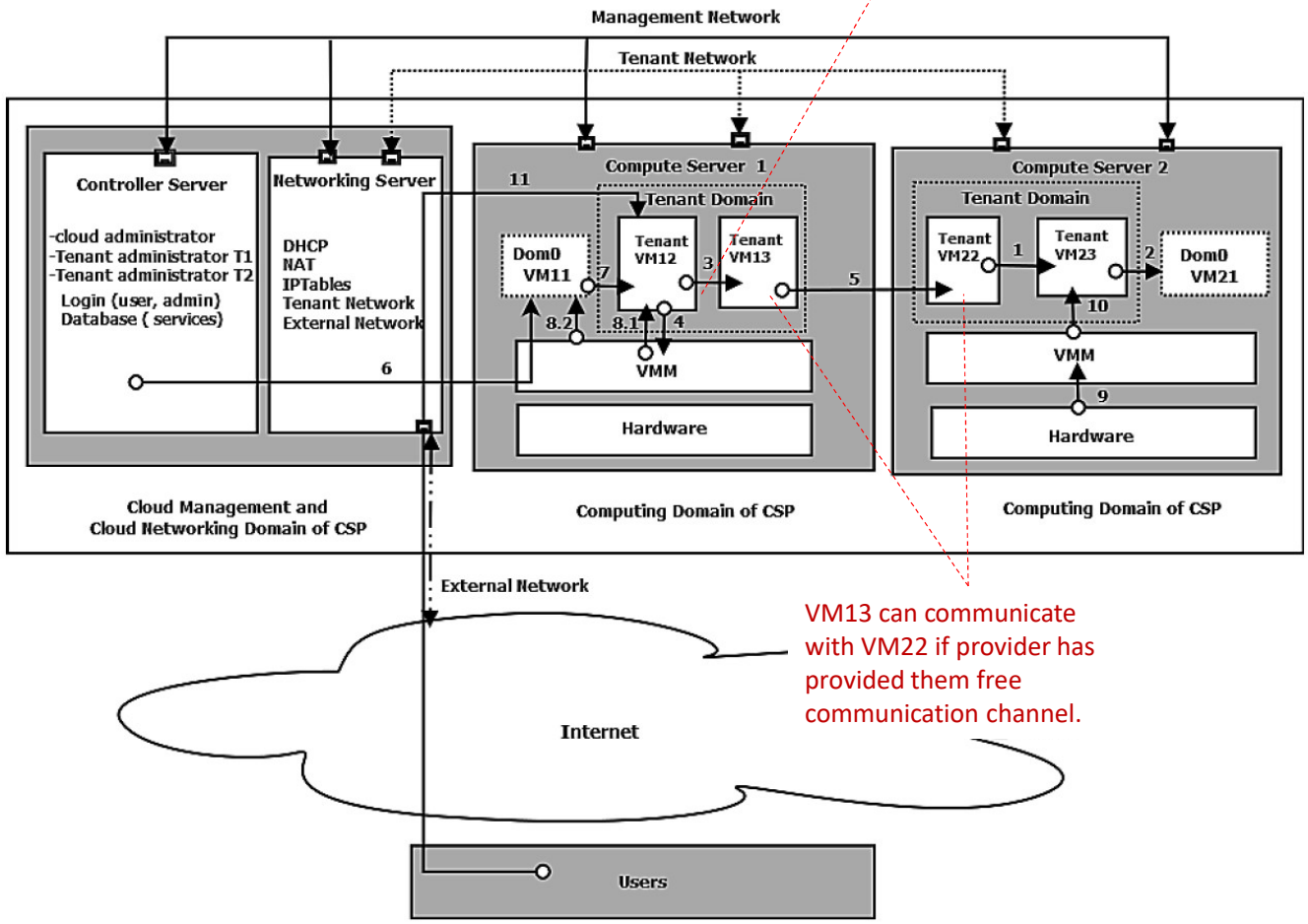
1. Malware tries to bypass the root access of the allocated VM
2. Malware runs the advanced malicious code to cross the memory boundaries beyond the access of the VM.
3. The attacker can be successful in gaining the root access of the privileged domain of VMM by executing such malwares.
4. Any compromise at the hypervisor- level can breach the security of all the VMs running above it.
5. VM Escape is one such attack.



Threat Model.

Scenario 3: Channel exploited by the malicious tenant

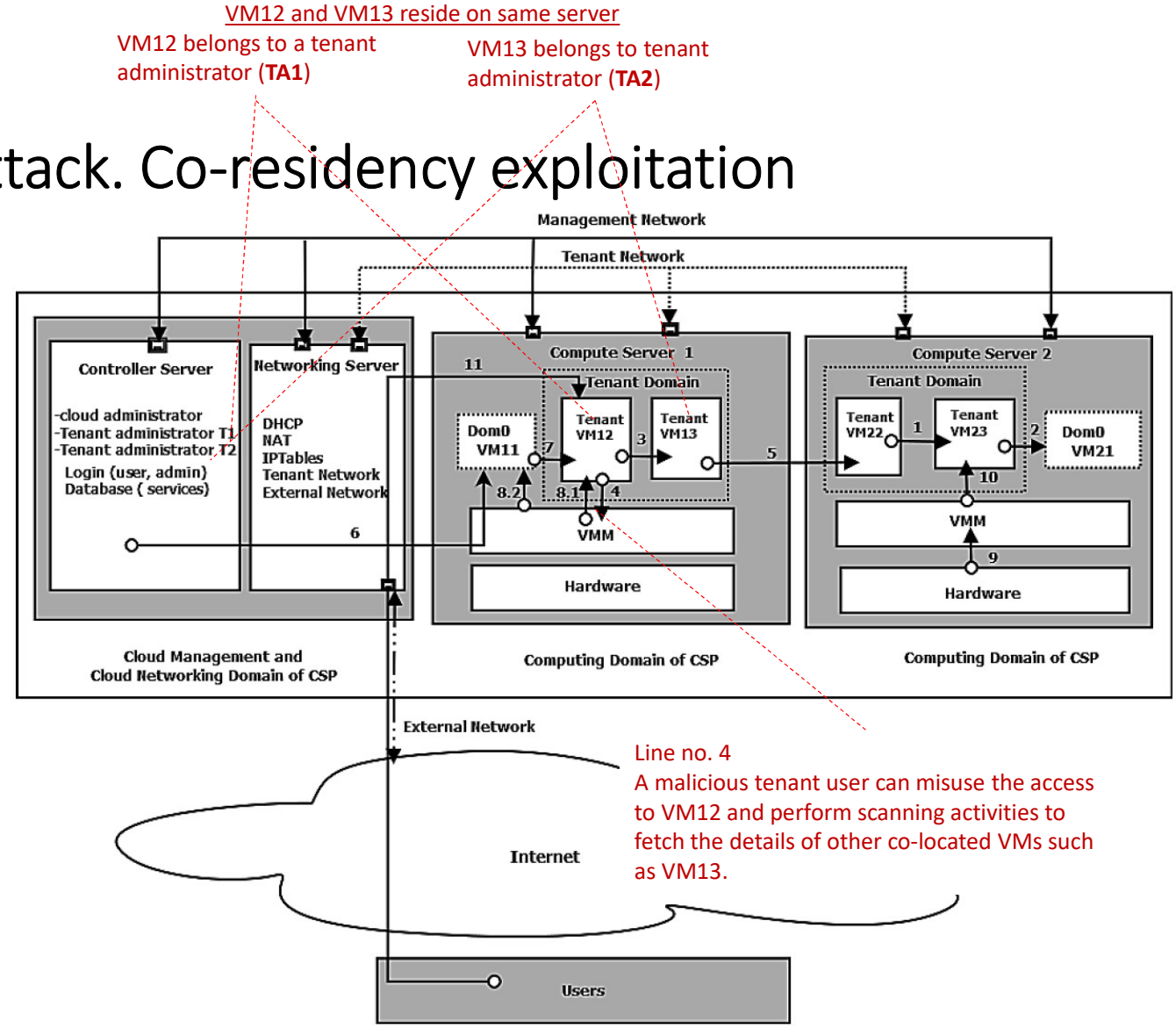
- TVMs can communicate with each other.
- The network resource starvation at the VM may become cause of DoS to other co-located VMs.
- The service denial can also lead to the violation in services level agreement (SLA).



Threat Model.

Scenario 4: VM to VM attack. Co-residency exploitation

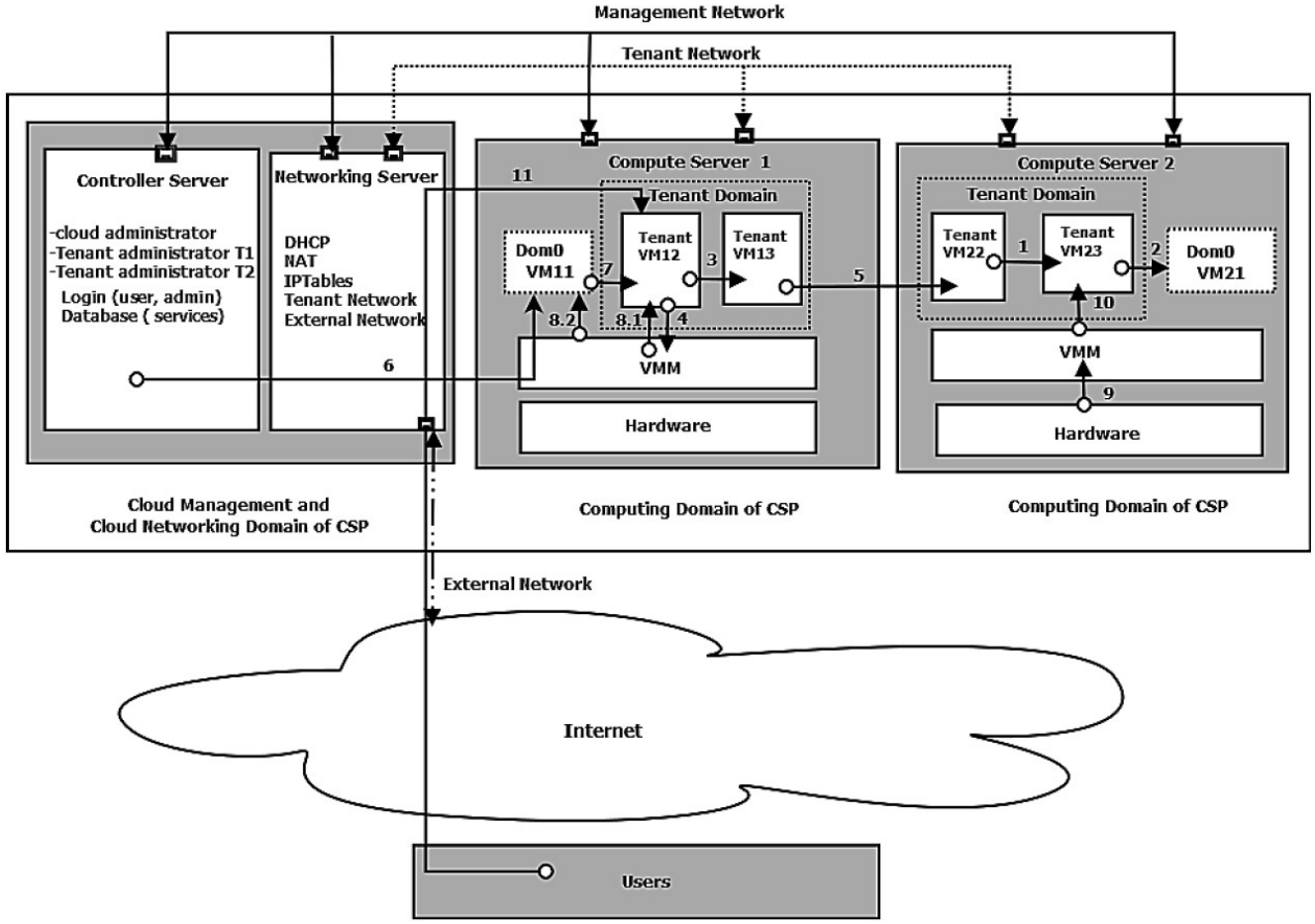
- Tenant VMs of different tenant administrator can be allocated on same physical server.
- The **co-residency** can be exploited by the attacker and co-located VM can become the victim of attack.



Threat Model.

Scenario 5: DoS at the network level

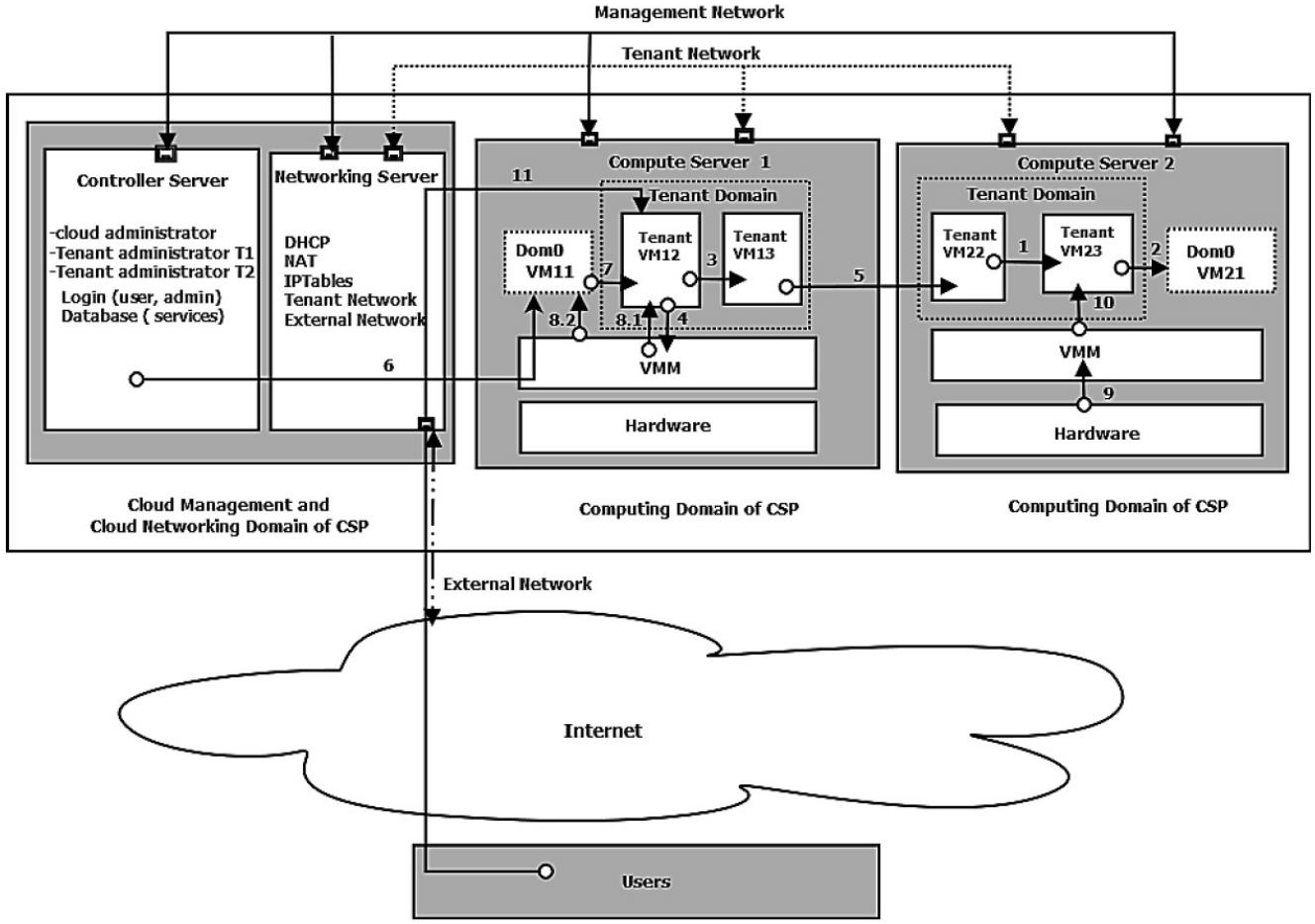
- A malicious tenant can generate IP/MAC spoofed network traffic of the victim VM and flood such packets in the network.
- All the VMs will now reply to the victim machine causing the network resource congestion at the victim server.
- It will cause DoS at the network level and may lead to clashes between CSP and victim user



Threat Model.

Scenario 6: Attack to Cloud Networking Server

- CNS is now the victim of attack
- All the inbound and out-bound network traffic passes through CNS.
- Attacks that degrade the performance of cloud services
  - Flooding
  - Scanning
  - Brute force
- Once CNS goes down
  - none of the cloud services can be provisioned to the customers



Other related technologies that you might be interested

- Container Technology
  - What is a Container?
  - Containers Vs. Virtual Machines
  - What is Docker? And Docker Networking?
  - Microservices Vs. Docker
  - Container Orchestration
  - What is Kubernetes? Kubernetes Platforms?
  - Kubernetes Vs. Docker
  - Container Security Challenges
- Serverless Computing
  - Serverless Vs. Containers
  - Serverless Computing Frameworks

References

- *R. Buyya, C. Vecchiola, and S. T. Selvi, Mastering cloud computing: founda-tions and applications programming. Newnes, 2013.*
- *D. F. Parkhill, Challenge of the computer utility. Addison-Wesley, 1966.*
- *F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, "Nist cloud computing reference architecture," NIST special publication, vol. 500, no. 2011, p. 292, 2011.*
- *L. Savu, "Cloud computing: Deployment models, delivery models, risks and research challenges," in 2011 International Conference on Computer and Management (CAMAN). IEEE, 2011, pp. 1–4.*
- *International Journal of Computer Network and Information Security, vol. 6, no. 3, p. 20, 2014.*
- *B. Wilder, Cloud architecture patterns: using microsoft azure. O'Reilly Media, Inc., 2012.*
- *N. Vasić, M. Barisits, V. Salzgeber, and D. Kostic, "Making cluster applications energy-aware," in Proceedings of the 1st workshop on Automated control for Datacenters and Clouds, 2009, pp. 37–42.*
- *Cloud Security. Attacks, Techniques, Tools, and Challenges. Preeti Mishra, Emmanuel S Pilli, R C Joshi. First edition published 2022 by CRC Press*
- *H. Baron, S. Heide, S. Mahmud, J. Yeoh, "Cloud security complexity: Challenges in managing security in hybrid and multi-cloud environments," Cloud Security Alliance, Tech. Rep., 2019.*
- *https://owasp.org/www-pdf-archive/Cloud-Top10-Security-Risks.pdf*
- *https://faun.pub/owasp-cloud-top-10-db4a3a8e0a8f*