22AIE305: CLOUD COMPUTING

Mainframe Computing
Aforementioned core memory, mass-storage devices, computer graphics systems (for plotting the aircraft)

SMP/open Systems
Pool of homogeneous processors, independent administered software

Distributed Computing
web-based application, multitier architecture

Grid Computing
Providing virtualization of distributed computing resources

Cloud Computing
IaaS, PaaS, SaaS

60s, 70s | 80s,90s | Late 90s | Early 2000 | Late 2000

NIST definition of Cloud

- Cloud computing is a model for enabling convenient, resource pooling, ubiquitous, on-demand access which can be easily delivered with different types of service provider interaction by clients using Pay as You Go (PAYG) model.

Essential Characteristics of Cloud (NIST)

On-demand self-service: "A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider."

Broad network access: "Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (for example, mobile phones, tablets, laptops, and workstations)."

Essential Characteristics of Cloud (NIST)

Resource pooling: "The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Examples of resources include storage, processing, memory, and network bandwidth."

Rapid elasticity: "Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time."

Essential Characteristics of Cloud (NIST)

Measured service: "Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (for example, storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service."

Table 1 The pros and cons of public, private, and hybrid clouds

Cloud development models	Advantages	Disadvantages
Public cloud	Scalability and reliability with on-demand resources	Can be unreliable
	Easy to use	Less secure
Private cloud	Organization-specific	More costly
	Customizable	Requires IT expertise
Hybrid cloud	Flexible infrastructure	Lack of visibility
	Cost controls	Potential challenges in application and data integration
	Faster speeds	

Service-oriented architecture (SOA)

- A service-oriented architecture enables agility and scalability in the cloud.
- Microservices are a variant of SOA in which an application is composed of a collection of loosely coupled, modular services.
- Containers are increasingly popular among developers as a preferred technology for efficiently deploying microservices, and these technologies are being used side by side.

Cloud Computing Security Challenges

- Data Privacy/Confidentiality
- Unauthorized Access
- Hijacking of Accounts
- Legal & Regulatory Compliance
- Lack of Visibility in Security
- External Sharing of Data
- Misconfiguration
- Unsecure Third-party Resources

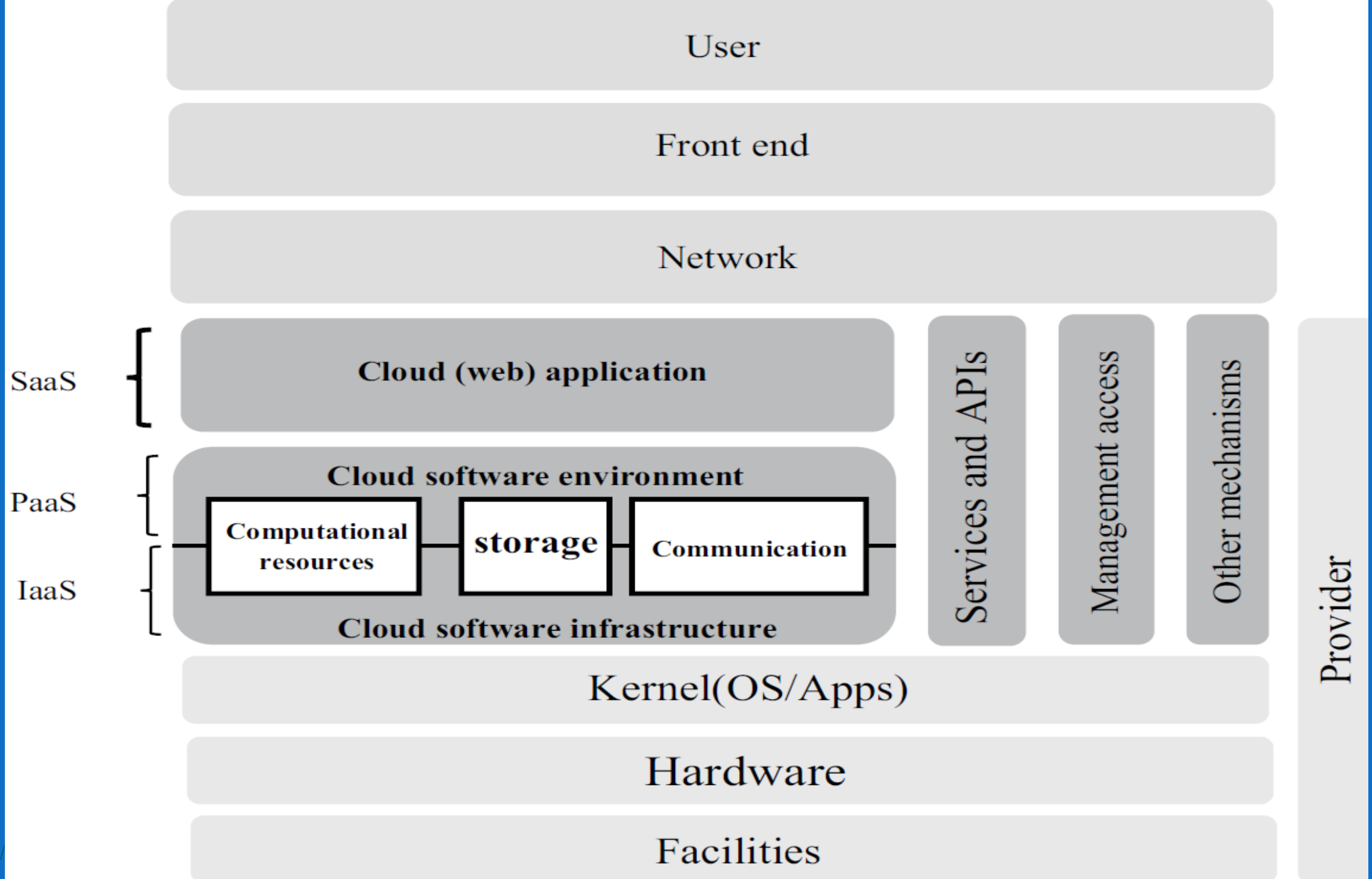
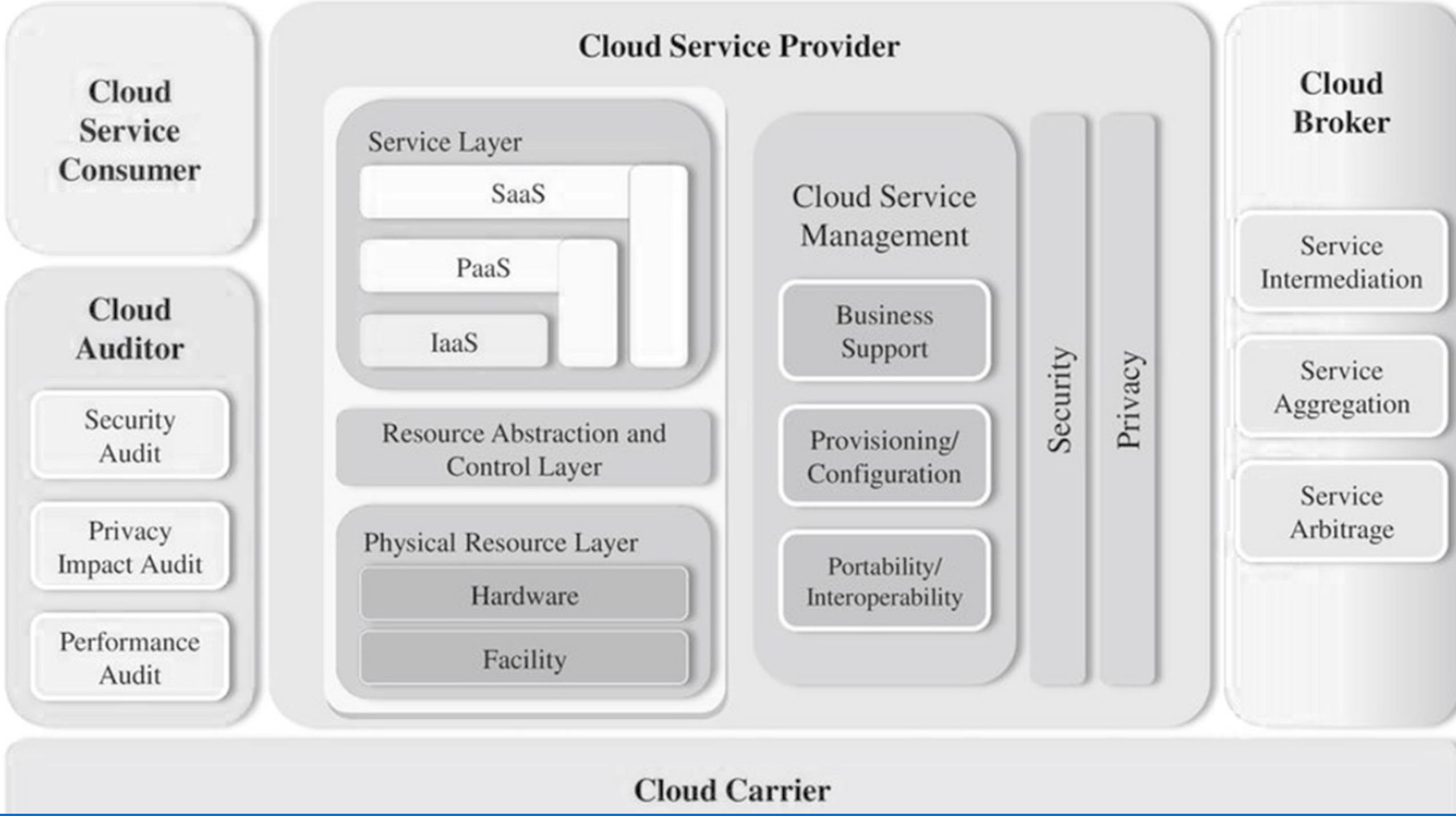

User
Front end
Network
SaaS
Cloud (web) application
PaaS
Cloud software environment
Computational resources
storage
Communication
IaaS
Cloud software infrastructure
Services and APIs
Management access
Other mechanisms
Provider
Kernel(OS/Apps)
Hardware
Facilities

Table 2 Security services and mechanisms

Security services	Security mechanisms	Some examples
Confidentiality	Data encryption (cryptography, quantum cryptography), secure sockets layer (SSL)	Symmetric cryptographic mechanisms (AES, CBC, etc.) asymmetric mechanisms (RSA, DSA, etc.), post-quantum cryptography
Integrity	Hash functions, message signature, message authentication code	Hash functions (SHA-256, MD5, etc.), message authentication codes (HMAC), public blockchains [ethereum (platform)]
Availability	Intrusion detection and prevention systems, firewalls, packet filters	Signature-based intrusion detection, statistical anomaly-based intrusion detection, etc.
Authentication	Digital signature, secure sockets layer (SSL), endorsing certificate	HMAC, CBC-MAC, ECDSA, certified signatures, SSL certificate
Non-repudiation	Digital signatures, notary, public, and private blockchains	Email tracking, capturing unique biometric information and other data about the sender or signer

Table 3 Different actors in cloud computing

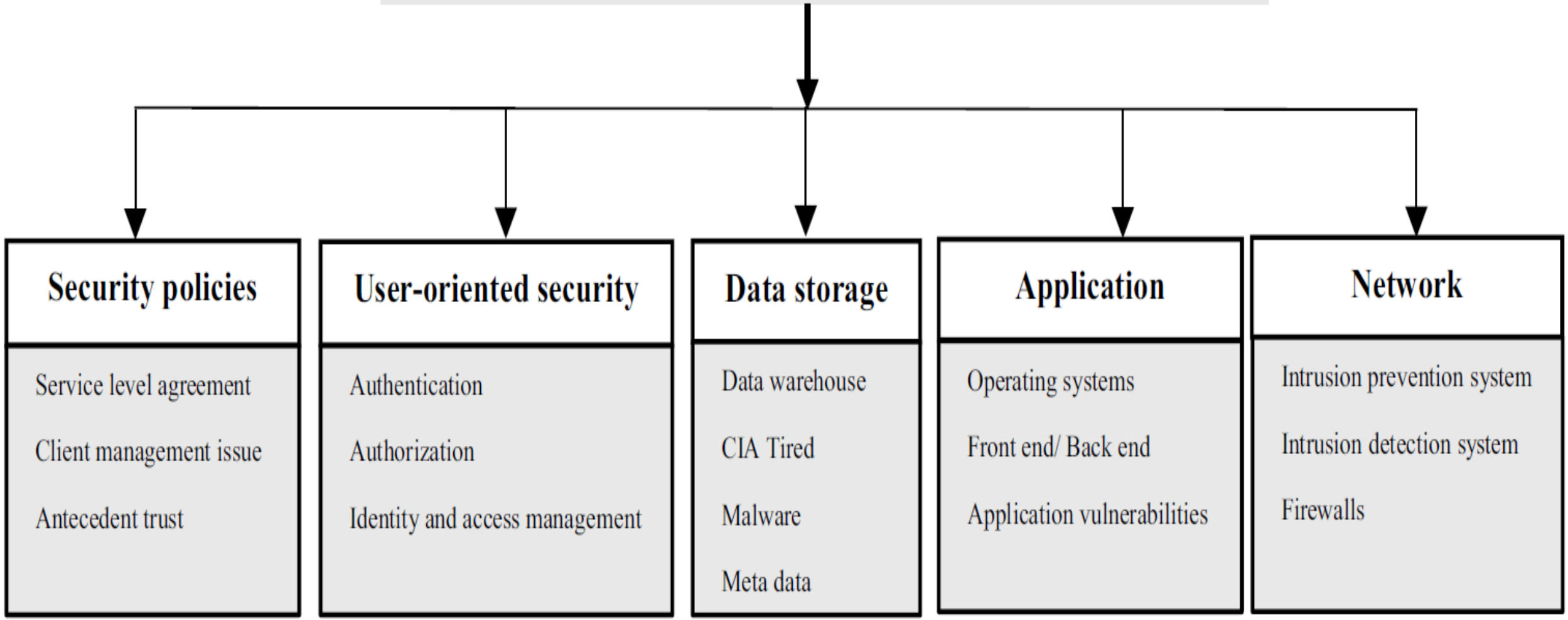
Actor	Definition
Cloud consumer	A person or organization that maintains a business relationship with, and uses service from, cloud providers
Cloud provider	A person, organization, or entity responsible for making a service available to interested parties
Cloud auditor	A party that can conduct an independent assessment of cloud services, information system operations, performance and security of the cloud implementation
Cloud broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between cloud providers and cloud consumers
Cloud carrier	An intermediary that provides connectivity and transport of cloud services from cloud providers to cloud consumers

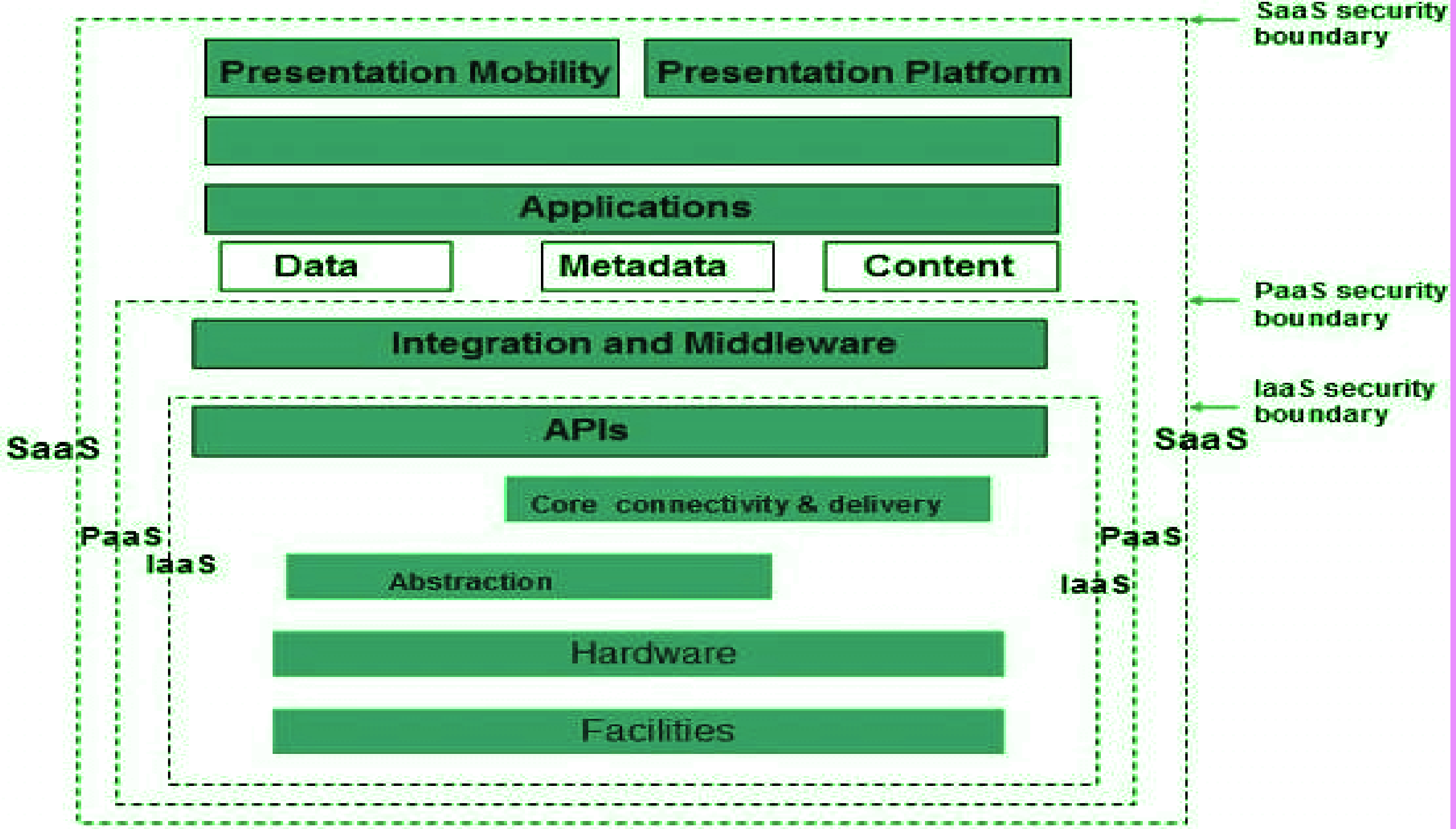

Cloud Service Consumer
Cloud Auditor
Security Audit
Privacy Impact Audit
Performance Audit
Cloud Service Provider
Service Layer
SaaS
PaaS
IaaS
Resource Abstraction and Control Layer
Physical Resource Layer
Hardware
Facility
Cloud Service Management
Business Support
Provisioning/ Configuration
Portability/ Interoperability
Security
Privacy
Cloud Broker
Service Intermediation
Service Aggregation
Service Arbitrage
Cloud Carrier

Security on the Cloud

- Unauthorized Access
- Client Account Hijacking
- Vulnerabilities
- Data Privacy/Confidentiality
- Legal and Regulatory Compliance
- Third-party Resources
- Wrong configuration issues

Cloud security issues classification




SaaS security boundary
Presentation Mobility
Presentation Platform
Applications
Data
Metadata
Content
PaaS security boundary
Integration and Middleware
IaaS security boundary
APIs
SaaS
SaaS
Core connectivity & delivery
PaaS
IaaS
PaaS
Abstraction
IaaS
Hardware
Facilities

Key Points to CSA Model

- IaaS is the most basic level of service, with PaaS and SaaS next two above levels of services.
- Moving upwards, each service inherits the capabilities and security concerns of the model beneath.
- IaaS provides the infrastructure, PaaS provides the platform development environment, and SaaS provides the operating environment.
- IaaS has the lowest integrated functionality and security level, while SaaS has the highest.
- This model describes the security boundaries at which cloud service providers' responsibilities end and customers' responsibilities begin.
- Any protection mechanism below the security limit must be built into the system and maintained by the customer.

Unauthorized Access

- Unauthorized access to data is one of the most common cloud security problems businesses face. The cloud provides a convenient way for companies to store and access data, which can make data vulnerable to cyber threats. Security and cloud computing threats can include unauthorized access to user data, theft of data, and malware attacks.
- To protect their data from these threats, businesses must ensure that only authorized users can access it. Another security feature businesses can implement is encrypting sensitive data in the cloud. It will help ensure that only authorized users can access it. By implementing security measures such as encryption and backup procedures, businesses can safeguard their data from unauthorized access and ensure its integrity.

Client Account Hijacking

- Hijacking of user accounts is one of the major cloud security issues. Using cloud-based applications and services will increase the risk of account hijacking. As a result, users must be vigilant about protecting their passwords and other confidential information to stay secure in the cloud.
- Users can protect themselves using strong passwords, security questions, and two-factor authentication to access their accounts. They can also monitor their account activity and take steps to protect themselves from unauthorized access or usage. This will help ensure that hackers cannot access their data or hijack their accounts. Overall, staying vigilant about security and updating your security measures are vital to the security of cloud computing.
- 61% of companies fear AI-powered attacks compromise sensitive data
- Firewall-as-a-service (FWaaS) offers the same protection as traditional firewalls.

Identity Theft

- Cloud account hijacking is a common tactic in identity theft schemes in which the attacker uses the stolen account information to carry out the malicious or unauthorized activity. In fact, when cloud account hijacking occurs, an attacker typically uses stolen credentials to impersonate the account owner.
- Using stolen credentials, attackers may gain access to critical areas of cloud computing services, compromising the confidentiality, integrity, and availability of those services.

Vulnerabilities

- Companies need to protect their data from unauthorized access and theft. To ensure that their systems are vulnerable only to authorized sources, businesses must implement security measures such as strong authentication, data loss prevention (DLP), data breach detection, and data breach response.
- With cloud computing, visibility is vital, and businesses must regularly audit security operations and procedures to detect vulnerabilities and threats before they become a real problem.
- By taking the necessary precautions and implementing security in cloud computing, organizations can ensure that their data remains secure in this cloud-based environment.

Malicious insider/Local Intrusions

- A malicious insider is a current or former employee or any business partner that has or had authorized access to information system creates a threat if he or she intentionally misused that access to negatively impact the security and privacy aspects of the information system. Malicious insider is a person that gains access to an organization's network, system, or data and releases this information without permission by the organization.

Attacker Capability: Malicious Insiders

- At the client site
  - Learn passwords/authentication information
  - Gain control of the VMs
- At the cloud provider
  - Log client communication data and packets
  - Can read unencrypted data
  - Can possibly peek into VMs, or make copies of VMs
  - Can monitor network communication, application patterns
  - Why?
    - Gain information about client data
    - Gain information on client behavior
    - Sell the information or use itself

Distributed denial-of-service attacks

- DDoS attacks are able to make significant risks to cloud customers and providers, including reputation damage and exposure of customer data.
- DDoS refers to the deployment of a large numbers of Internet bots, anywhere from hundreds to hundreds of thousands. These bots are designed to attack a single server, network, or application with an overwhelming number of requests, packets, or messages, thereby denying service to legitimate users such as employees or customers.

Resource depletion attack

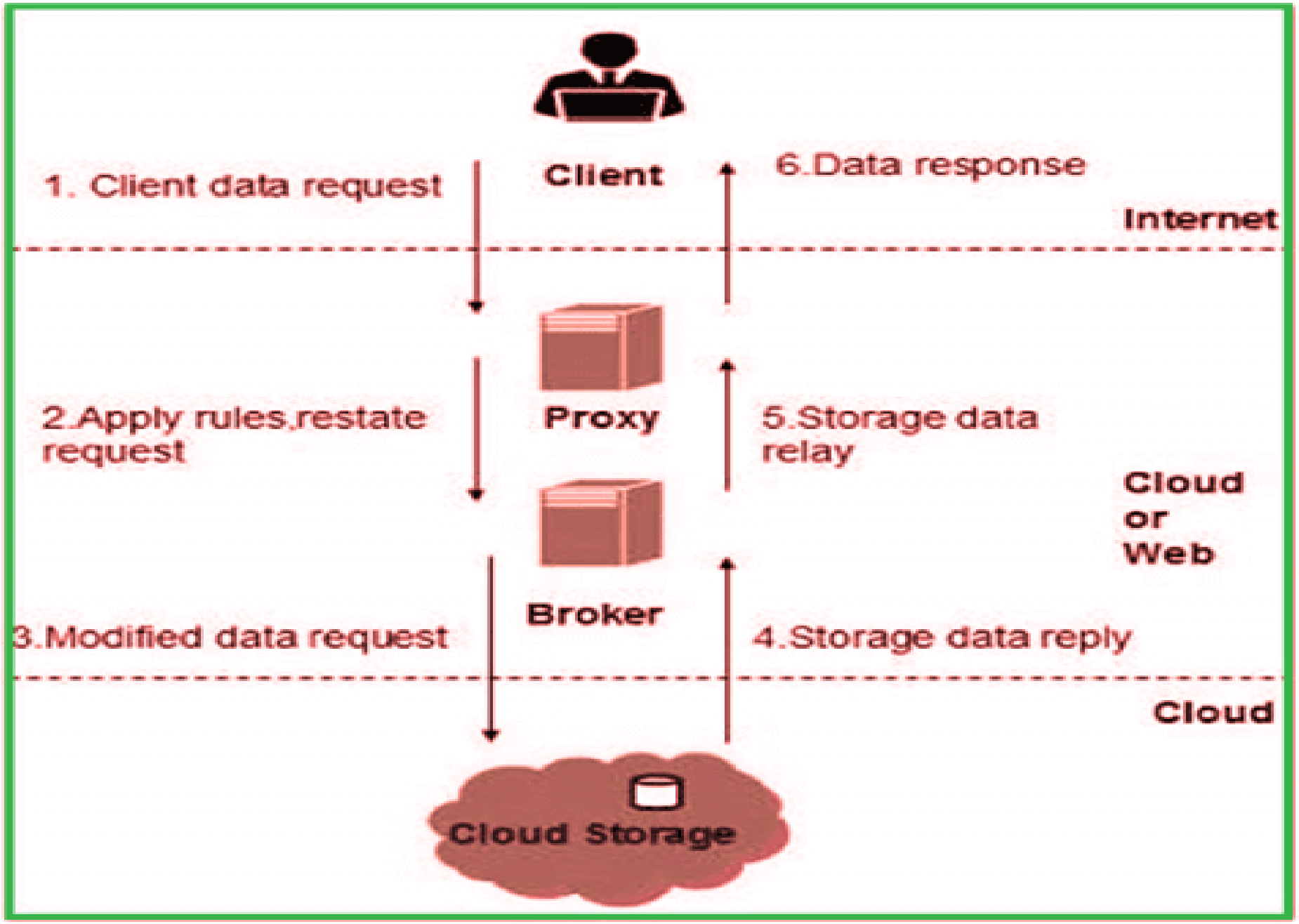
- Resource depletion attack is the attack that uses a compromised node involving in generating more network traffic which consumes the energy of the nodes.
- Resource depletion attacks at the routing protocol layer, trying to disable networks by exhausting the energy of the nodes. Attackers are able to exhaust any computational resources like cloud resources, such as network bandwidth, memory, and other computing capabilities

Injection Attacks

- Attackers can inject code or query into a program, or by injecting one or multiple malware onto a computer in order to modify a database.
- A code injection attack appears in different forms relying on the execution context of the application and the location of the programming flaw that leads to the attack

Path Traversal Attacks

- The main aim of path traversal attack is to access files or directories that are stored outside the web-root folder.
- This attack accesses arbitrary files and directories stored on the file system by manipulating variables that reference files with “dot-dot-slash” sequences.
- In addition, this type of attacks tends to access critical system files including application source code or configuration.


Client
1. Client data request
6.Data response
Internet
Proxy
2.Apply rules,restate request
5.Storage data relay
Cloud or Web
Broker
3.Modified data request
4.Storage data reply
Cloud
Cloud Storage

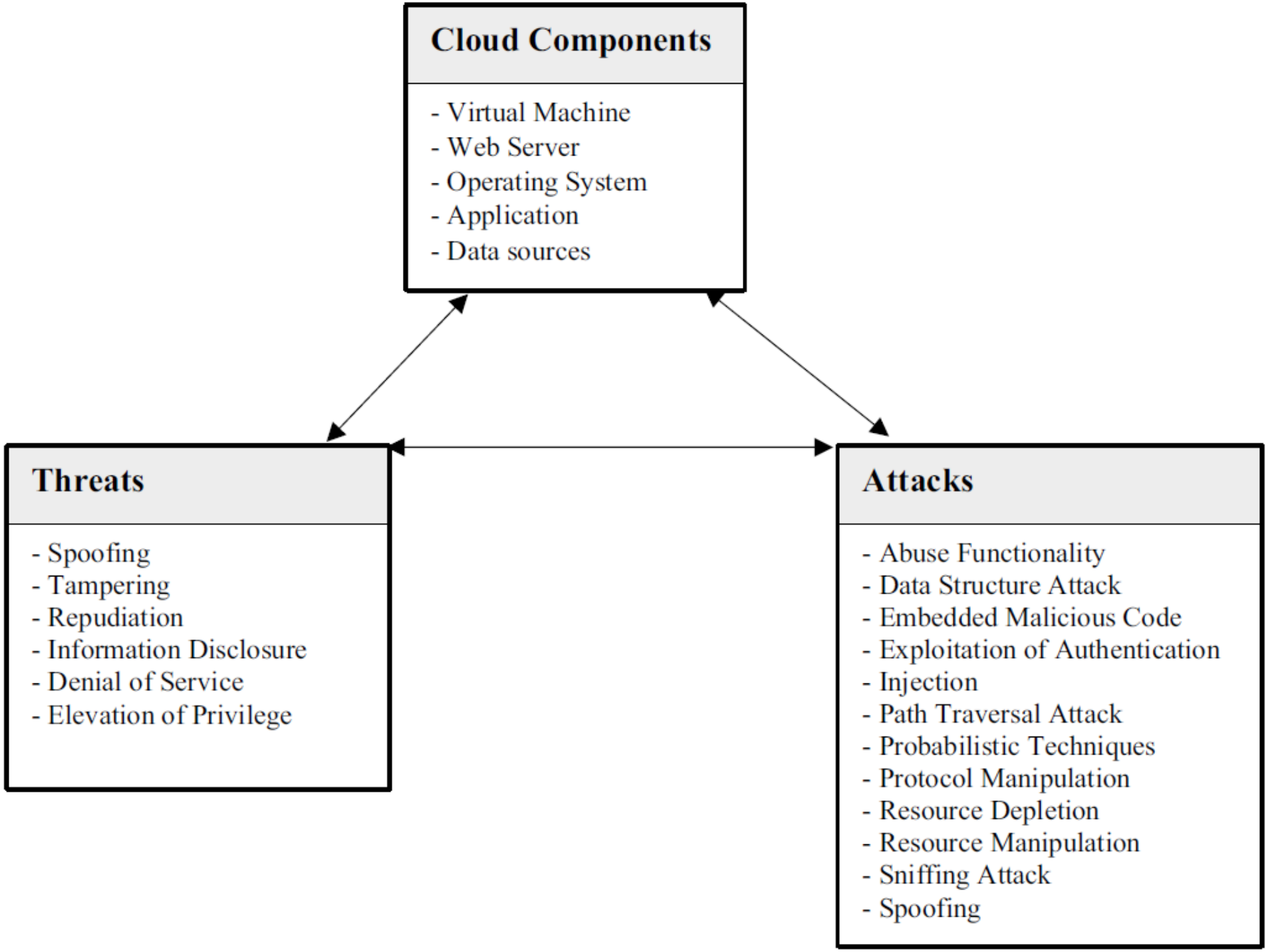

Cloud Components
- Virtual Machine
- Web Server
- Operating System
- Application
- Data sources
Threats
- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege
Attacks
- Abuse Functionality
- Data Structure Attack
- Embedded Malicious Code
- Exploitation of Authentication
- Injection
- Path Traversal Attack
- Probabilistic Techniques
- Protocol Manipulation
- Resource Depletion
- Resource Manipulation
- Sniffing Attack
- Spoofing

Table 6 The STRIDE threat model

Threat	Desired property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiability
Information disclosure	Confidentiality
Denial of service	Availability
Elevation of privilege	Authorization

Denial of Service

- A denial-of-service attack is a security event that happens when an attacker prevents legitimate users from accessing particular services or resources. Valid users are denied from the service due to malicious activities caused by cyber attacks. DoS and DDoS attacks often use the vulnerability of how network protocols handle network traffic by transferring large numbers of packets to a vulnerable network service from different Internet Protocol (IP) addresses to overwhelm the service to deny legitimate users from accessing services or resources

Data Privacy/Confidentiality

- Data privacy and confidentiality are critical issues when it comes to cloud computing. With cloud computing, businesses can access their data from anywhere worldwide, raising concerns about securing cloud computing. Companies don't have control over who can access their data, so they must ensure that only authorized users can access it. Data breaches can happen when hackers gain access to company data. In the coming years, there will be even more data privacy and confidentiality issues due to the rise of big data and the increased use of cloud computing in business.
- Data privacy and confidentiality issues will continue to be essential concerns for businesses in the years ahead as data-intensive applications grow in popularity. Managed IT Services Charlotte experts helps to ensure proper security measures and data practice for a cloud-ready organization to avoid data breach risks.

Data Breach

- A data breach means releasing, viewing, stealing, or using protected or confidential information like personal information such as credit card numbers, Aadhar numbers for any purpose which was not authorized to do.
- In the event of a successful intrusion into the environment, encryption will prevent threat actors from accessing the actual data

Legal and Regulatory Compliance

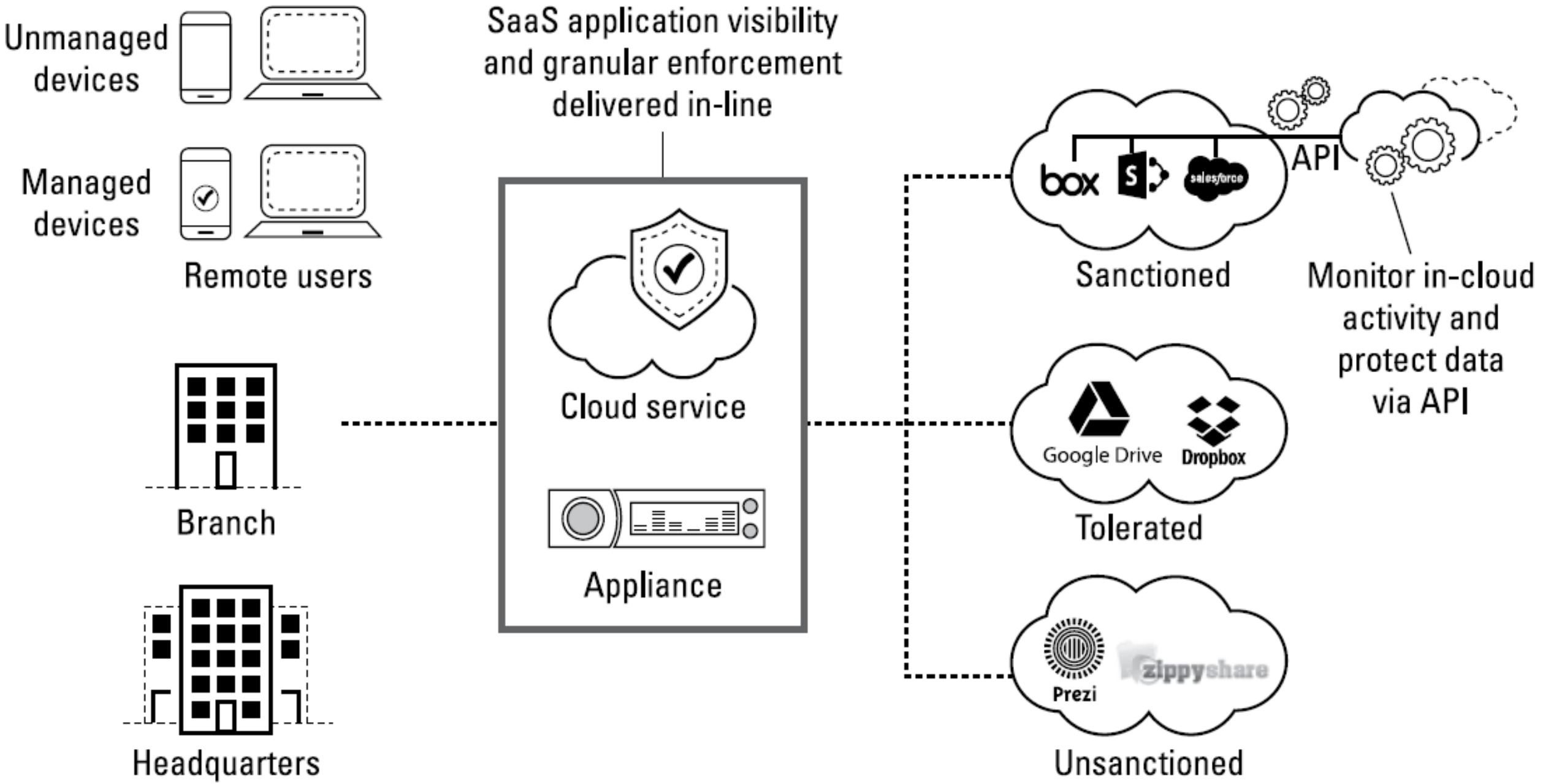
- Organizations must ensure data security for cloud and comply with legal and regulatory requirements to ensure the safety and integrity of their cloud-based systems. Cyber threats such as malware, data breaches, and phishing are just a few challenges organizations face when using cloud computing.
- To combat these cloud based security issues, it's vital to perform regular security audits, maintain up-to-date security configurations, implement robust authentication procedures, use strong passwords, use multi-factor authentication methods, and regularly update software and operating systems.
- While cloud computing can increase the risk of cyberattacks, organizations that are diligent about their security posture can stay ahead of their competitors in this rapidly changing market.

Third-party Resources

- Third-party resources are applications, websites, and services outside the cloud provider's control. These resources may have cloud security vulnerabilities, and unauthorized access to your data is possible. Additionally, unsecured third-party resources may allow hackers to access your cloud data. These vulnerabilities can put your security at risk. Therefore, ensuring that only trusted, secure resources are used for cloud computing is essential. In addition, it will help ensure that only authorized individuals access data and reduce the risk of unauthorized data loss or breach.
- Unsecured third-party resources can pose a threat to cloud security, especially when interacting with sensitive data in cloud storage accounts. Hackers can access these resources to gain access to your cloud data and systems. Implementing strong security controls such as multi-factor authentication and enforcing strict password policies can help safeguard against this risk. In addition, by restricting access to only trusted resources, you can ensure that only authorized individuals access data and reduce the risk of unauthorized data loss or breach.

Wrong configuration issues

- Misconfiguration is the top cloud computing security challenge, as users must appropriately protect their data and applications in the cloud. Malware propagation across the network and sensitive data exposure often results from vulnerabilities in SaaS application usage or misconfigurations
- To prevent this cloud security threat, users must ensure their data is protected, and applications are configured correctly. It can be accomplished using a cloud storage service that offers security features such as encryption or access control. Additionally, implementing security measures such as authentication and password requirements can help protect sensitive data in the cloud. By taking these steps, users can increase the security of their cloud computing infrastructure and stay protected from cyber threats.

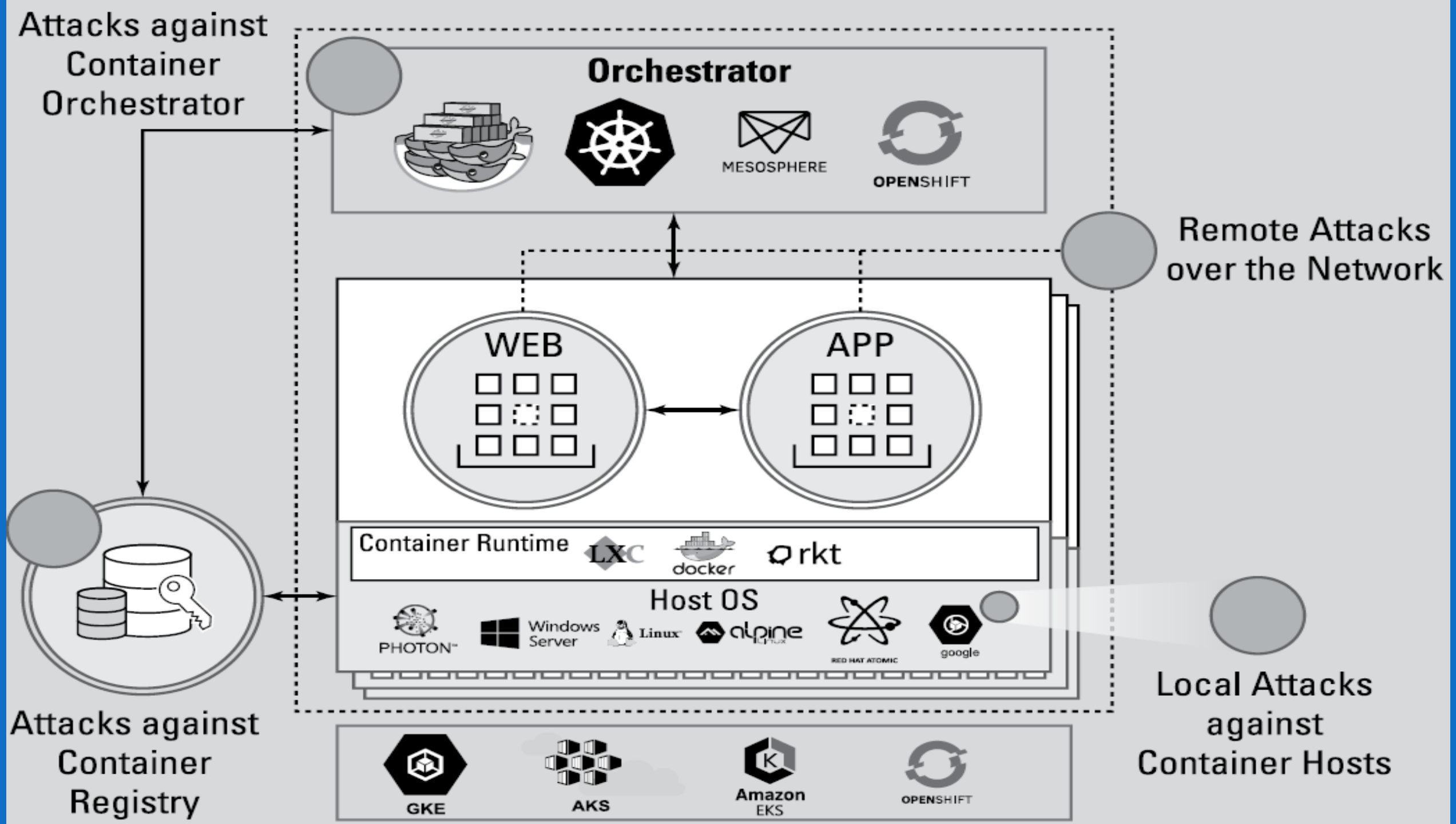

Unmanaged devices
Managed devices
Remote users
Branch
Headquarters
SaaS application visibility and granular enforcement delivered in-line
Cloud service
Appliance
box
salesforce
API
Sanctioned
Monitor in-cloud activity and protect data via API
Google Drive
Dropbox
Tolerated
Prezi
zippyshare
Unsanctioned

IaaS Shared Responsibility

- With an IaaS, a business purchases the infrastructure from a cloud provider, and the business typically installs their own OS, applications, and middleware.
- In an IaaS, the customer is usually responsible for the security associated with anything they own or install on the infrastructure.
- **IaaS Cloud Security Architecture Components**
- Components of secure cloud computing architecture in an IaaS cloud environment may include endpoint protection (EPP), a cloud access security broker (CASB), a vulnerability management solution, access management, and data and network

SaaS Shared Responsibility

- With SaaS, an organization purchases the use of a cloud-based application from a provider. Examples of SaaS include Office 365 or Salesforce. In a SaaS, the customer is typically only responsible for the security components associated with accessing the software, such as identity management, customer network security, etc. The software provider manages the security backend.
- **SaaS Cloud Security Architecture Components**
- SaaS security architecture components should include application security, identity and access management as well as a cloud access security broker (CASB) to facilitate visibility, access controls, and data protection using APIs, proxies, or gateways. Staying up-to-date with the latest patches for software services, API's etc. is important.


Attacks against Container Orchestrator
Orchestrator
MESOSPHERE
OPENSHIFT
Remote Attacks over the Network
WEB
APP
Container Runtime
LXC
docker
rkt
Host OS
PHOTON
Windows Server
Linux
alpine
RED HAT ATOMIC
google
Attacks against Container Registry
Local Attacks against Container Hosts
GKE
AKS
Amazon EKS
OPENSHIFT

PaaS Shared Responsibility

- With PaaS, a business purchases a platform from a provider to develop, run, and manage applications w/o developing or managing the underlying platform infrastructure required for the applications. An example of a PaaS is AWS. In a PaaS, a client is responsible for the security associated with application implementation, configurations, and permissions.
- **PaaS Cloud Security Architecture Components**
- A PaaS security architecture requires both standard cloud security architecture solutions, and common solutions, such as a Cloud Workload Protection Platform (CWPP).

Key Elements of a Cloud Security Architecture

- Several critical elements should be considered:
- Security at Each Layer
- Centralized Management of Components
- Redundant & Resilient Design
- Elasticity & Scalability
- Appropriate Storage for Deployments
- Alerts & Notifications
- Centralization, Standardization, and Automation

Public Cloud Security Responsibility

Security is on you	Applications (including operating system) and associated data deployed
	Account controls (access control, services enabled, and so on)
	Deployment architecture, configuration management, and so on
Security is on the provider	Worldwide footprint (regional presence and so on)
	Physical components (buildings, server hardware, resiliency, and so on)
	Compute infrastructure (network, database, storage, and so on)

Cloud security tools

- Cloud native tools
  These are offered by Cloud service providers in the form of services integrated within the cloud platform
- Examples are SecurityHub, GuardDuty from AWS, Security Command Center of GCP
- Third-party tools
  Outside vendors have lots of security tools
  Examples are Crowdstrike, Checkpoint, Fortigate,
- Open-source tools
  Freely available tools such as Prowler, Scoutsuite