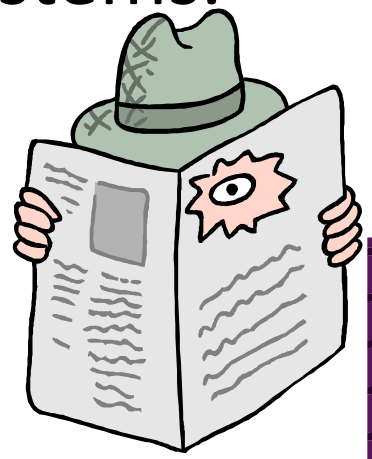
PMCA506L: Cloud Computing

Module 7 : Cloud Security and Cloud Data Storage

Courtesy : *Ming Lian , Dogules E Comer & Other Sources of Internet*

Threats & Attacks (Methods)

- Threats are acts performed by individuals with harmful intent, whose goal is to steal data, cause damage to or disrupt computing systems.



Organizing the threats using STRIDE

- **S**poofing identity
- **T**ampering with data
- **R**epudiation (refuse to do with, dispute)
- **I**nformation disclosure
- **D**enial of service
- **E**scalation of privilege

Spoofing identity

- illegally obtaining access and use of another person's authentication information
  - Man in the middle
  - URL phishing
  - Email address spoofing (email spam)

Tampering with data

- Malicious modification of the data
- Often hard and costly to detect
  - you might not find the modified data until some time has passed;
  - once you find one tampered item, you'll have to thoroughly check all the other data on your systems

Repudiation

- a legitimate transaction will be disowned by one of the participants
  - You sign a document first; and refused to confirm the signature
  - Need a trusted third party to mitigate

Information/data disclosure

- An attacker can gain access, without permission, to data that the owner doesn't want him or her to have.

Denial of service

- An explicit attempt to prevent legitimate users from using a service or system. It involves the overuse of legitimate resources.

- You can stop all such attacks by removing the resource used by the attacker, but then real users can't use the resource either.

Distributed Denial of Service (DDoS)

- A Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a flood of internet traffic.

- Unlike a traditional Denial of Service (DoS) attack, which is carried out from a single source, a DDoS attack involves multiple sources, often geographically distributed and controlled by different attackers or automated systems.

Escalation of privilege

- an unprivileged user gains privileged access.
  - E.g. unprivileged user who contrives a way to be added to the Administrators group
  - Escalation of privilege in the context of security refers to the situation where an attacker gains higher-level access or permissions than they are initially granted.
  - This unauthorized elevation allows the attacker to perform actions that were not intended by the system's designers or administrators.

Attackers

Who is the attacker?

- Insider?
  - Malicious employees at client
  - Malicious employees at Cloud provider
  - Cloud provider itself
- Outsider?
  - Intruders
  - Network attackers?

Attacker Capability: Malicious Insiders

- At client
  - Learn passwords/authentication information
  - Gain control of the VMs
- At cloud provider
  - Log client communication

Attacker Capability: Cloud Provider

- What can the attacker do?
  - Can read unencrypted data
  - Can possibly peek into VMs, or make copies of VMs
  - Can monitor network communication, application patterns

Attacker motivation: Cloud Provider

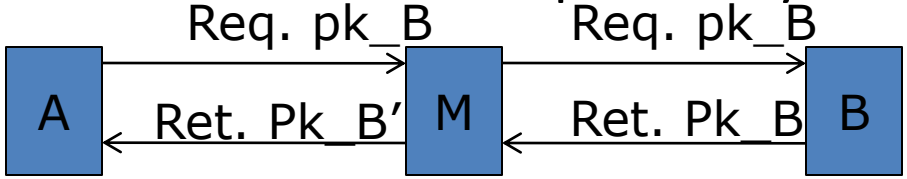
- Why?
  - Gain information about client data
  - Gain information on client behavior
  - Use the information to improve services
  - Sell the information to gain financial benefits

Attacker Capability: Outside attacker

- What can the attacker do?
  - Listen to network traffic (passive)
  - Insert malicious traffic (active)
  - Probe cloud structure (active)
  - Launch DoS

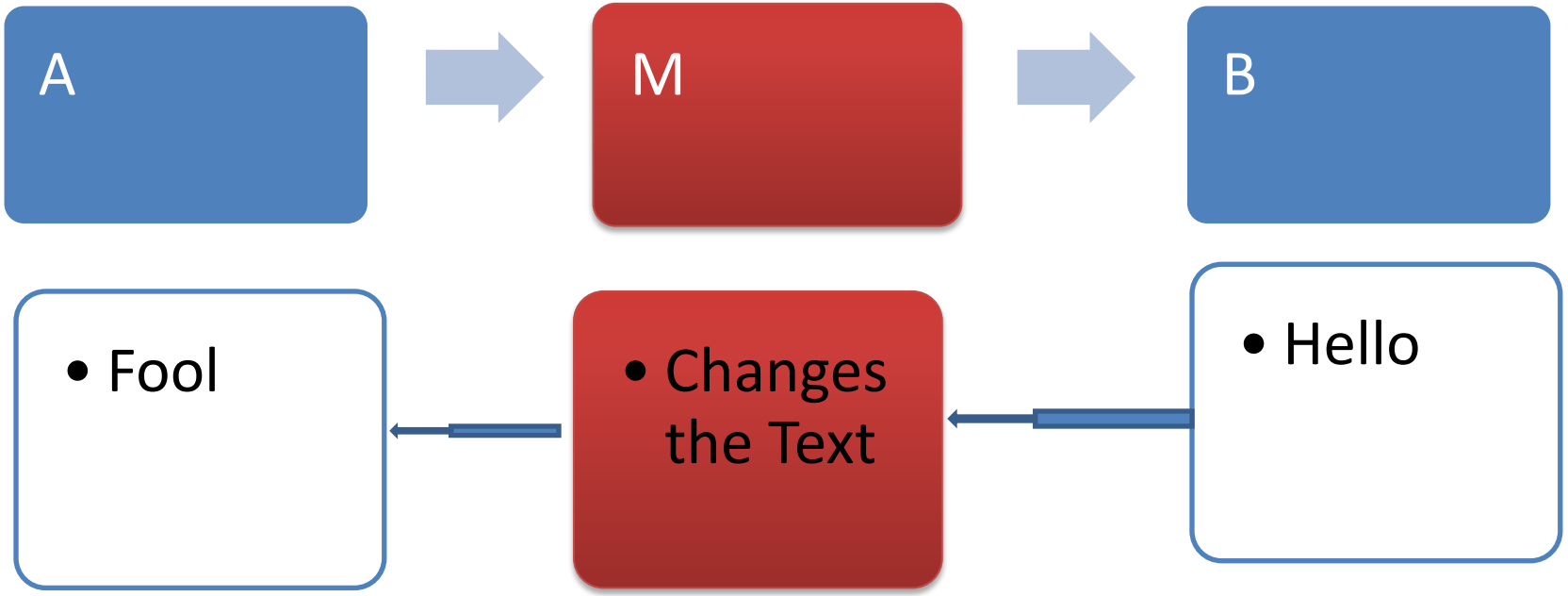
Attacker goals: Outside attackers

- Intrusion
- Network analysis (network security)
- Man in the middle: public key example



Pk_A: public key by A
Pk_B: public key by B
Pk_A',Pk_B': false public keys by M

Man-in-Middle



Man-in-the-Middle

- A Man-in-the-Middle attack is a type of cyber security attack where an attacker intercepts and potentially alters the communication between two parties without their knowledge.

- The attacker inserts themselves between the legitimate communicating parties, allowing them to eavesdrop on the communication, manipulate the data being transmitted, or impersonate one or both parties.

Common scenarios where Man-in-the-Middle attacks

- **Public Wi-Fi Networks:** Attackers may set up rogue Wi-Fi hotspots in public places to intercept communications of unsuspecting users connecting to these networks.

- **Unsecured Websites:** If a website doesn't use encryption (HTTPS), an attacker could intercept and manipulate data between the user and the website.

- **Compromised Routers or Network Devices:** An attacker could compromise routers or other network devices to intercept and manipulate traffic passing through them.

Security In A Traditional Infrastructure

- **Insiders vs. Outsiders**

(a typical organization runs two Wi-Fi network in its buildings: Inside and Guest Network)

- **Perimeter security**

(*firewalls*, *Deep Packet Inspection* (*DPI*) systems, and scanners used to detect viruses and other malware in incoming email and imported files.)

- **Demilitarized zones(DMZs)**

(instead of allowing arbitrary network traffic, restrict access to a specific set of servers.)

- **Standing privileges divided into a few levels**

(one group of IT staff members has privilege to manage database servers, while another group has privilege to manage web servers).

Cloud-Specific Security Problems

- Lack of control and visibility.
- An infrastructure shared with outsiders.
- Many services with interdependencies among them.
- Dynamic execution environment with bursts.
- Remote access for all users
- Extensive use of software from the cloud provider and third parties

Lack of control and visibility

- In a cloud environment, however, a tenant cannot configure or examine the underlying systems, and must trust that the provider's staff has configured security protections correctly.

- When a problem arises, the tenant must rely on the provider's staff to diagnose the cause and affect repairs.

Many services with interdependencies among them.

- Cloud systems encourage a microservices design in which many small services run independently with communication among them.

- However, having many microservices and allowing frequent communication among them increases the attack surface, giving attackers more opportunities to find vulnerabilities.

Dynamic execution environment with bursts

- Orchestration systems achieve elasticity by expanding services as needed, with new instances spread across multiple physical servers.

- Rapid creation of new instances makes it more difficult to distinguish normal execution from a *Denial of Service* (*DoS*) attack.

Remote access for all users

- A tenant's employees, whether working in their organization's offices or at home, must use a remote access mechanism.

- Use of remote access increases the possible attack surface, especially in cases where responsibility for installing and managing security software falls to employees using their own devices.

Extensive use of software from the cloud provider and third parties

- Many cloud users now incorporate pieces of open source software into their systems.
- For example, container software can be downloaded from Docker repositories or GitHub.
- *Vulnerabilities include the extensive use of open source software obtained from public repositories.*

Zero Trust Security Model

- In a Zero Trust model, no entity—whether inside or outside the network—is trusted by default.
- Every user, device, or application attempting to connect to the network is treated as potentially untrusted.
- The model assumes that threats can come from both internal and external sources.
- Implementing a Zero Trust model requires a combination of technology, policies, and cultural changes within an organization.

Zero Trust Security Model

- **Verify Identity:** Instead of relying solely on the traditional perimeter-based security model, Zero Trust emphasizes the need for strong identity verification for all users, devices, and applications. This involves **Multi-Factor authentication (MFA), strong access controls, and continuous monitoring of user behavior.**

- **Least Privilege Access:** Users and devices are granted the minimum level of access necessary to perform their tasks. This principle helps limit the potential damage that can be caused by compromised accounts or devices.

- **User and Device Authentication:** All users and devices attempting to connect to the network must authenticate themselves. This authentication process may involve multiple factors to ensure a higher level of confidence in the legitimacy of the user or device.

Zero Trust Security Model

- **Continuous Monitoring and Analytics:** Zero Trust relies on continuous monitoring of network activities, user behaviors, and security events.

- Advanced analytics and machine learning are often used to detect anomalies and potential security threats in real-time.

- **Encryption:** Zero Trust emphasizes the use of encryption for data in transit and at rest to protect sensitive information from unauthorized access.

Identity and Access Management (IAM)

- Identity management, often referred to as Identity and Access Management (IAM), is a set of processes, policies, and technologies that organizations use to manage and secure digital identities.

- To enable the **right individuals** to access the **right resources** at the **right times** for the right reasons by **authentication** and **authorisation** of identities and access.

- One of the most common ways to control access to computer systems is to identify who is at the keyboard (and prove that identity), and then decide what they are allowed to do.

- **Single Sign-On (SSO):** Allowing users to log in once and gain access to multiple systems or applications without the need to re-authenticate for each one.

Authentication & Authorization

- Authentication is the means of verifying who a **person** (or process) is, while authorization determines what they're **allowed to do**.

- This should always be done in accordance with the principle of least privilege—giving each person only the amount of access they require to be effective in their job function, and no more.

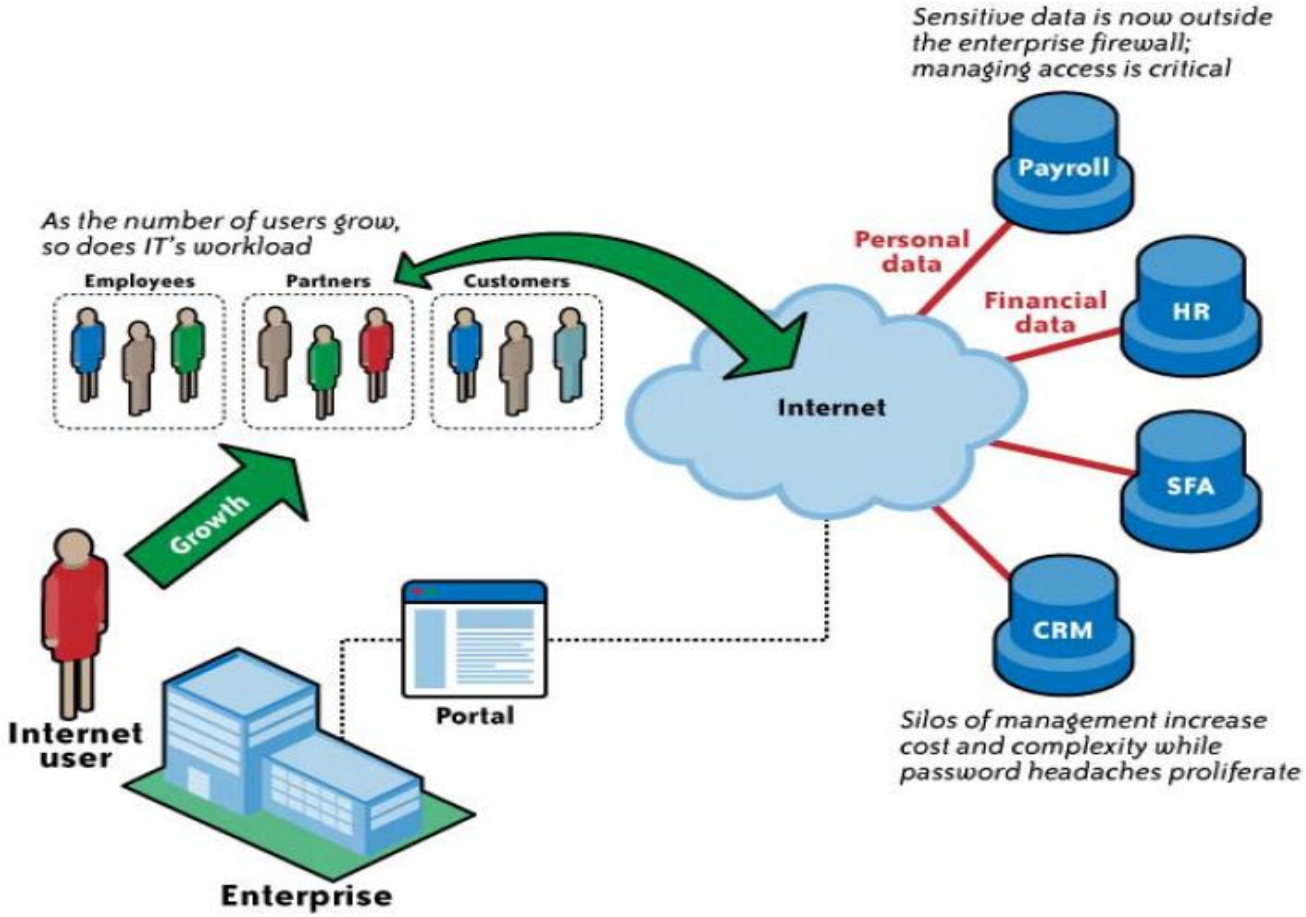
Authentication

- Two parts: a public statement of identity (usually in the form of a *username*)
- Combined with a private response to a challenge (such as a *password*). ***single-factor authentication***
- The secret response to the authentication challenge can be based on **one or more factors**—(***secret word, number, or passphrase, smartcard, ID tag, or code generator, biometric factor like a fingerprint or retinal print***)

Multifactor authentication

- Two or more methods of check-in
- Something you know (a password or PIN code)
- Something you have (such as a card or token)
- Something you are (a unique physical characteristic) identity

Identity Management-As-a-Service (IDMAAS)



Privileged Access Management

- Privileged Access Management (PAM) is a cyber security practice that focuses on securing and managing access to privileged accounts within an organization.

- Privileged accounts are those that have elevated permissions and access rights, allowing users to perform tasks beyond the scope of regular user accounts.

- Examples of privileged accounts include system administrators, database administrators, and other roles with high-level access to critical systems and sensitive data.

Access Control

- **Who should have access to what resource?**

  (Assignment of entitlements to users)

- **Why should the user have access to the resource?**

  (Assignment of entitlements based on the user's job functions and responsibilities)

- **How should the user access the resource?**

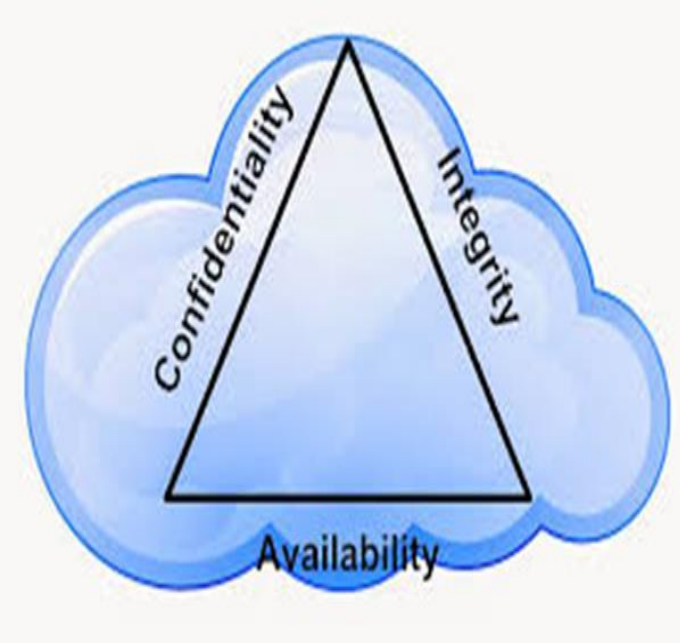
  (What authentication method and strength are required prior to granting access to the resource)

- **Who has access to what resource?**

  (Auditing and reporting to verify entitlement assignments)

Protecting Remote Access

- Multi-Factor Authentication (MFA)
- Virtual Private Network (VPN)
- Identity and Access Management (IAM)
- Network Security Groups (NSGs) and Firewalls
- Encryption
- Audit Logging and Monitoring
- Endpoint Protection
- Regular Software Updates
- Regular Security Assessments
- Compliance and Regulations
- User Education



Privacy in Cloud Environment

- Privacy in a cloud environment is a critical consideration as organizations increasingly rely on cloud services to store, process, and manage sensitive data.

- Protecting the privacy of user information and ensuring compliance with data protection regulations are paramount.

Privacy in Cloud Environment

- Data Encryption
- Data Residency and Jurisdiction
- Privacy Policies and Agreements
- Data Ownership and Control
- User Access Controls
- Auditing and Logging
- Data Portability and Interoperability
- Data Deletion and Retention
- Consent and Transparency

Regularly reassessing and updating privacy strategies

AI Technologies on Security

- Artificial Intelligence (AI) plays a crucial role in enhancing cloud security by providing advanced threat detection, rapid incident response, and improved overall security posture.

Threat Detection and Prevention

- **Anomaly Detection:** AI algorithms can learn the normal patterns of behavior within a cloud environment and identify anomalies that may indicate potential security threats.

- **Behavioral Analysis:** AI tools can analyze user and entity behavior to detect any deviations from normal patterns, helping to identify potential insider threats or compromised accounts.

- **Predictive Analysis:** AI can use historical data and patterns to predict potential future threats, enabling proactive security measures.

Endpoint Security

- **AI-driven Antivirus:** AI algorithms can enhance traditional antivirus solutions by identifying and mitigating new and evolving threats in real-time.

- **Endpoint Detection and Response (EDR):** AI-powered EDR solutions monitor and respond to security incidents on endpoints, providing rapid threat containment and remediation.

Network Security

- **Intrusion Detection and Prevention Systems (IDPS):** AI can analyze network traffic patterns to detect and prevent malicious activities, helping to safeguard the cloud infrastructure.

- **Firewall Optimization:** AI-driven firewalls can dynamically adjust security policies based on real-time threat intelligence, adapting to changing conditions.

Security Automation and Orchestration

- **Automated Threat Remediation:** AI-driven automation can respond to security incidents by taking predefined actions, reducing the response time and minimizing the impact of an incident.

Vulnerabilities in Cloud: Back Doors, Side Channels

- Vulnerabilities refer to weaknesses or gaps in the security architecture that could be exploited by attackers to compromise the confidentiality, integrity, or availability of data and services.

- Back doors and side channels are two types of vulnerabilities that can pose risks to cloud environments

Back Doors

- **Definition:** A back door is a hidden or undocumented method of bypassing normal authentication, encryption, or access controls in a system. It provides unauthorized access to a system or data.

- **In the Cloud:** In cloud environments, back doors may be unintentionally introduced during development, configuration, or maintenance processes. Attackers could exploit these back doors to gain unauthorized access to cloud resources, compromise data, or manipulate system settings.

Side Channels

- **Definition:** Side channels are unintended communication channels that can leak information about the internal state or activity of a system. These channels may exist due to the physical implementation of the system or the way resources are shared.

- **In the Cloud:** Side channels can be relevant in multi-tenant cloud environments where multiple users share the same physical infrastructure. For example, a side channel attack might involve monitoring the usage patterns of shared resources, such as CPU utilization or network traffic, to infer information about the activities of other users on the same system.

Security VPC Management
(Vulnerability, Patch, and Configuration)

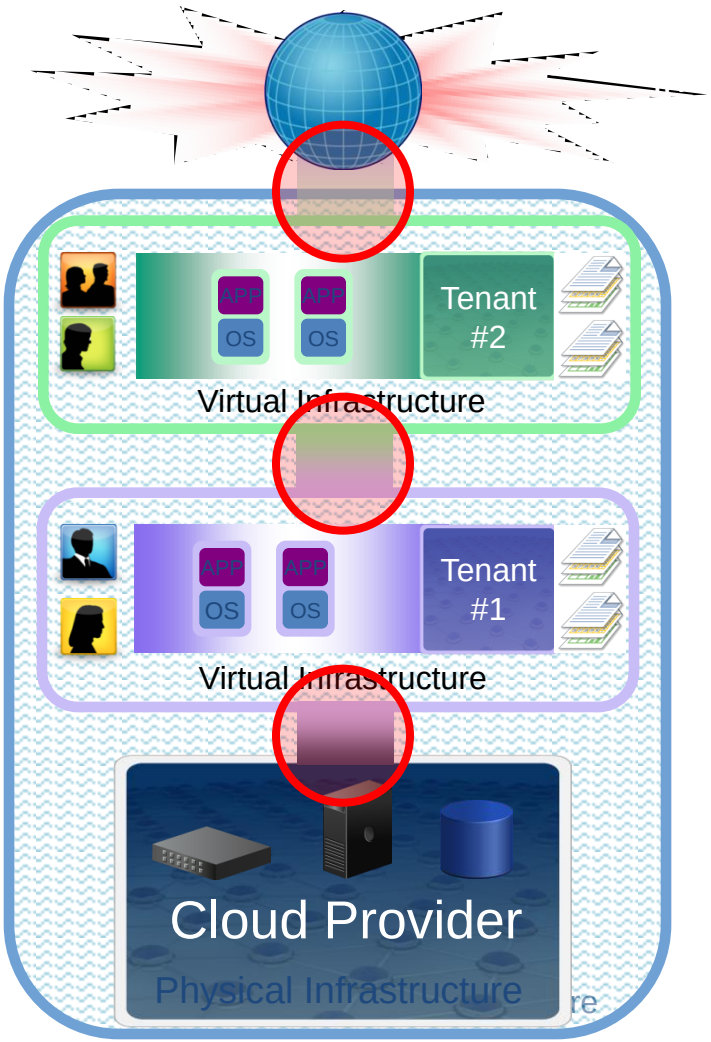
- The ability for malware (or a cracker) to remotely exploit vulnerabilities of infrastructure components, network services, and applications remains a major threat to cloud services.

- CSPs are responsible for the vulnerability, patch, and configuration (VPC) management of the infrastructure. (networks, hosts, applications, and storage)

- Customers are not spared from their VPC duties and should understand the VPC aspects for which they are responsible.

- A VPC management scope should address end-to-end security and should include customer-managed systems and applications that interface with cloud services.

Trusted Zones



Identity federation

Virtual network security

Access Mgmt

Security Info. & Event Mgmt

Anti-malware

Cybercrime intelligence

Strong authentication

Data loss prevention

Encryption & key mgmt

Tokenization

GRC

Managing data in the cloud

- Managing data in the cloud involves storing, organizing, securing, and retrieving data using cloud computing services.

- Cloud storage offers scalability, flexibility, and accessibility, allowing organizations to store and manage their data more efficiently

Storage as a Service (STaaS)

- Storage as a Service (STaaS) in the cloud refers to the delivery of storage infrastructure and services over the internet on a subscription basis.

- This model allows organizations to offload the responsibility of managing physical storage infrastructure, such as servers and disks, to a cloud service provider

Cloud Storage Services

- **Object Storage:** Use cloud object storage services like Amazon S3, Google Cloud Storage, or Microsoft Azure Blob Storage to store unstructured data such as images, videos, and documents.

- **File Storage:** Utilize file storage services (e.g., Amazon EFS, Google Cloud File store) for organized file systems and shared access.

- **Block Storage:** Employ block storage services (e.g., Amazon EBS, Google Cloud Persistent Disks) for applications requiring raw storage volumes.

Security, Identity and Compliance in Amazon Web Services(AWS)

- Amazon Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- AWS WAF (Web Application Firewall)
- Amazon GuardDuty
- Amazon VPC (Virtual Private Cloud)
- Amazon Macie
- AWS CloudTrail

Summary

- Cloud Specific Security Problems
- Security in Traditional Infrastructure
- Zero Trust Security Model
- Identity Management
- Privileged Access Management
- AI Technologies on Security
- Vulnerabilities in Cloud
- Managing Data in the Cloud