UNIT – 5 : SECURING THE CLOUD

Cloud Information Security Fundamentals:

What is Cloud Security?

Cloud security refers to protecting data stored online via cloud computing environments (instead of data centers) from theft, deletion, and leakage. There are many protective methods that help secure the cloud; these measures include access control, firewalls, penetration testing, obfuscation, tokenization, virtual private networks (VPN), and not using public internet connections.

How Secure is the Cloud?

When it comes to network security concerns, the cloud itself is not the issue – rather, the challenge lies within the policies and technologies for security and control of that technology. Put simply? Human error is one of the top reasons for data breaches in the cloud. In fact, Gartner estimates that by 2022, at least 95 percent of cloud security failures will be the customer's fault due to misconfigurations and mismanagement.

Therefore, it is not an issue of whether or not the cloud is secure but if the customer is using the cloud *securely.*

Fundamentals of Cloud Security:

Don't just migrate to the cloud – prevent security threats by following these tips:

1. Understand what you're responsible for – different cloud services require varying levels of responsibility. For instance, while software-as-a-service (SaaS) providers ensure that applications are protected and that data security is guaranteed, IaaS environments may not have the same controls. To ensure security, cloud customers need to double check with their IaaS providers to understand who's in charge of each security control.

2. Control user access – a huge challenge for enterprises has been controlling who has access to their cloud services. Too often, organizations accidently publically expose their cloud storage service despite warnings from cloud providers to avoid allowing storage drive contents to be accessible to anyone with an internet connection. CSO advises that only load balancers and bastion hosts should be exposed to the internet. Further, do not allow Secure Shell (SSH) connections directly from the internet as this will allow anyone who finds the server location to bypass the firewall and directly access the data. Instead, use your cloud provider's identity and access control tools while also knowing who has access to what data and when. Identity and access control

policies should grant the minimum set of privileges needed and only grant other permissions as needed. Configure security groups to have the narrowest focus possible and where possible, use reference security group IDs. Finally, consider tools that let you set access controls based on user activity data.

3. Data protection – data stored on cloud infrastructures should never be unencrypted. Therefore, maintain control of encryption keys where possible. Even though you can hand the keys over to cloud service providers, it is still your responsibility to protect your data. By encrypting your data, you ensure that if a security configuration fails and exposes your data to an unauthorized party, it cannot be used.

4. Secure credentials – AWS access keys can be exposed on public websites, source code repositories, unprotected Kubernetes dashboards, and other such platforms. Therefore, you should create and regularly rotate keys for each external service while also restricting access on the basis of IAM roles. Never use root user accounts – these accounts should only be used for specific account and service management tasks. Further, disable any user accounts that aren't being used to further limit potential paths that hackers can compromise.

5. Implement MFA – your security controls should be so rigorous that if one control fails, other features keep the application, network, and data in the cloud safe. By tying MFA (multi-factor authentication) to usernames and passwords, attackers have an even harder time breaking in. Use MFA to limit access to management consoles, dashboards, and privileged accounts.

6. Increase visibility – to see issues like unauthorized access attempts, turn on security logging and monitoring once your cloud has been set up. Major cloud providers supply some level of logging tools that can be used for change tracking, resource management, security analysis, and compliance audits.

7. Adopt a shift–left approach – with a shift-left approach, security considerations are incorporated early into the development process rather than at the final stage. Before an IaaS platform goes live, enterprises need to check all the code going into the platform while also auditing and catching potential misconfigurations before they happen. One tip – automate the auditing and correction process by choosing security solutions that integrate with Jenkins, Kubernetes, and others. Just remember to check that workloads are compliant before they're put into production. Continuously monitoring your cloud environment is key here.

Types of Cloud Computing Security Controls:

There are 4 types of cloud computing security controls i.e.

1. **Deterrent Controls**: Deterrent controls are designed to block nefarious attacks on a cloud system. These come in handy when there are insider attackers.

2. **Preventive Controls**: Preventive controls make the system resilient to attacks by eliminating vulnerabilities in it.
3. **Detective Controls**: It identifies and reacts to security threats and control. Some examples of detective control software are Intrusion detection software and network security monitoring tools.
4. **Corrective Controls**: In the event of a security attack these controls are activated. They limit the damage caused by the attack.

Importance of cloud security:

For the organizations making their transition to cloud, cloud security is an essential factor while choosing a cloud provider. The attacks are getting stronger day by day and so the security needs to keep up with it. For this purpose, it is essential to pick a cloud provider who offers the best security and is customized with the organization's infrastructure. Cloud security has a lot of benefits –

- **Centralized security:** Centralized security results in centralizing protection. As managing all the devices and endpoints is not an easy task cloud security helps in doing so. This results in enhancing traffic analysis and web filtering which means less policy and software updates.
- **Reduced costs:** Investing in cloud computing and cloud security results in less expenditure in hardware and also less manpower in administration
- **Reduced Administration:** It makes it easier to administer the organization and does not have manual security configuration and constant security updates.
- **Reliability:** These are very reliable and the cloud can be accessed from anywhere with any device with proper authorization.

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

Cloud Security Services:

Cloud security services refer to a range of solutions and tools designed to enhance the security of data, applications, and infrastructure in cloud computing environments. These services are crucial for protecting against various cyber threats, ensuring compliance with regulations, and maintaining the overall integrity of cloud-based systems.

Types of Cloud Security Services:

When we delve into the realm of cloud security, it's crucial to understand that it is not a singular, monolithic entity. Instead, it encompasses a wide range of services, each designed to address specific vulnerabilities and threats. Here's a breakdown of the primary types of cloud security services:

- **Network Security Services**: These services focus on protecting the underlying networking infrastructure from threats, unauthorized access, and disruptions. This is achieved through a combination of methods such as secure gateways, firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS). Network Security Services are designed to safeguard the integrity, usability, reliability, and safety of your network and data.
- **Data Protection Services**: As the name suggests, these services revolve around protecting a company's data stored in the cloud. They ensure data confidentiality, integrity, and availability through encryption, tokenization, and key management practices. This includes safeguarding data at rest, in transit, and in use. Additionally, data loss prevention (DLP) measures are put in place to prevent data leakage or loss.
- **Identity and Access Management Services (IAM)**: IAM services are critical to cloud security, ensuring that only authorized individuals can access specific resources. This is achieved by using tools like multi-factor authentication (MFA), single sign-on (SSO), and identity federation. IAM services help manage user identities and their permissions, reducing the risk of internal data breaches.
- **Threat Intelligence and Secure DevOps Services**: These services focus on predicting, identifying, and mitigating potential threats to cloud security. Threat intelligence services use data analysis to understand and anticipate potential threats, providing actionable insights. On the other hand, Secure DevOps services integrate security practices into the DevOps process, ensuring that security is embedded in applications right from the development stage.
- **Data Encryption Services:** Encryption services provide mechanisms to encrypt data both in transit and at rest. This protects sensitive information from unauthorized access even if a security breach occurs.

- **Security Information and Event Management (SIEM):** SIEM services collect and analyze log data from various cloud resources to identify and respond to security incidents. They help in real-time monitoring, threat detection, and incident response.
- **Endpoint Security Services:** Endpoint security services protect devices (endpoints) connected to the cloud, such as laptops, desktops, and mobile devices. They include antivirus, anti-malware, and device management solutions.
- **Cloud Access Security Broker (CASB):** CASB services provide visibility and control over data and applications as they move between an organization's on-premises environment and cloud service providers. They help enforce security policies and ensure compliance.

Each of these cloud security services plays a vital role in creating a comprehensive and robust cloud security strategy. They work together to provide an in-depth defense strategy, mitigating risks, and ensuring that businesses can confidently and securely utilize the power of the cloud.

Features of Cloud Security Services:

- **High-Level Data Encryption**: Encryption is one of the fundamental features of Cloud Security Services. It involves converting readable data into a coded form, so it can't be understood if intercepted. It is used both for data at rest (stored data) and data in transit (data being sent or received). Only authorized parties with the decryption key can decode and read the data, offering a high level of data protection.
- **Regular Security Audits**: Regular security audits are essential to maintaining a strong security posture. These audits can identify potential vulnerabilities and ensure all security controls are functioning as intended. Cloud Security Services often include tools for continuous monitoring and regular auditing of security measures, helping to maintain regulatory compliance and secure operations.
- **Disaster Recovery Planning**: Another feature of Cloud Security Services is disaster recovery planning. These services often include backup and recovery solutions that ensure business continuity in the event of a disaster, whether natural or man-made. Cloud backups are stored in geographically distributed locations, so data can be recovered even if one location is compromised.
- **Multi-Factor Authentication (MFA)**: MFA is an authentication method that requires users to verify their identities through multiple methods before they can access certain data or systems. It is an essential feature of Identity and Access Management Services, adding an additional layer of security that makes it harder for unauthorized users to gain access.

- **Intrusion Detection and Prevention**: These features are designed to detect and prevent cyber threats in real-time. Intrusion detection systems (IDS) monitor network traffic for suspicious activity, while intrusion prevention systems (IPS) proactively deny network traffic based on a security profile.

These features, when combined, create a robust cloud security framework, ensuring comprehensive protection for businesses operating in the cloud environment. Each feature addresses different areas of security, contributing to a layered and effective defense mechanism against cyber threats.

Best Practices for Cloud Security Services:

Making the most of Cloud Security Services involves implementing best practices that enhance your security posture and mitigate potential risks. These practices cover various aspects of cloud security and ensure that businesses can safely navigate the digital landscape. Here are a few essential best practices:

- **Clear Understanding of Shared Responsibility Model**: In the realm of cloud computing, security is often a shared responsibility between the cloud service provider and the customer. This model varies depending on the cloud service type: IaaS, PaaS, or SaaS. The cloud service provider typically secures the underlying infrastructure that runs cloud services. At the same time, the customer is often responsible for securing the data they process and store in the cloud. Clear comprehension of this model ensures all parties understand their security roles and responsibilities, and nothing slips through the cracks.
- **Comprehensive Access Control Implementation**: To prevent unauthorized access to your cloud resources, comprehensive access control measures should be in place. This practice includes implementing Identity and Access Management Services (IAM) that manage user identities and permissions. Techniques like multi-factor authentication (MFA) add an extra layer of security, ensuring that users prove their identity by presenting two or more pieces of evidence before gaining access. This strategy significantly reduces the chances of unauthorized access, even if a hacker manages to obtain a user's password.
- **Consistent Data Encryption**: Protecting your data is paramount, and encryption is one of the most reliable ways to do it. Encryption involves converting your data into an unreadable format that can only be deciphered with a specific key. It's advisable to encrypt all data, whether at rest or in transit, to prevent unauthorized access. This step adds a formidable barrier to potential cybercriminals who may try to compromise your data.

Design Principles:

- **Implement a strong identity foundation:** Implement the principle of least privilege and enforce separation of duties with appropriate authorization for each interaction with your AWS resources. Centralize identity management and aim to eliminate reliance on long-term static credentials.
- **Enable traceability:** Monitor, alert, and audit actions and changes to your environment in real time. Integrate log and metric collection with systems to automatically investigate and take action.
- **Apply security at all layers:** Apply a defense in depth approach with multiple security controls. Apply to all layers (for example, edge of network, VPC, load balancing, every instance and compute service, operating system, application, and code).
- **Automate security best practices:** Automated software-based security mechanisms improve your ability to securely scale more rapidly and cost-effectively. Create secure architectures, including the implementation of controls that are defined and managed as code in version-controlled templates.
- **Protect data in transit and at rest**: Classify your data into sensitivity levels and use mechanisms, such as encryption, tokenization, and access control where appropriate.
- **Keep people away from data:** Use mechanisms and tools to reduce or eliminate the need for direct access or manual processing of data. This reduces the risk of mishandling or modification and human error when handling sensitive data.
- **Prepare for security events:** Prepare for an incident by having incident management and investigation policy and processes that align to your organizational requirements. Run incident response simulations and use tools with automation to increase your speed for detection, investigation, and recovery.

The above mentioned 7 principles should be applied to all 6 areas of security in the cloud:

- Foundations
- Identity and Access Management
- Detection
- Infrastructure protection
- Data Protection
- Incident Response

Policy Implementation:

Implementing effective security policies is crucial for securing the cloud environment. Security policies define the rules, guidelines, and procedures that organizations follow to safeguard their data, applications, and infrastructure in the cloud.

The specific types of policies to be implemented may vary based on the organization's industry, regulatory requirements, and the nature of its cloud deployment. Here are some common types of policies that organizations typically implement to secure their cloud environments:

1. **Access Control Policy:** Defines rules and procedures for controlling access to cloud resources. It includes user authentication, authorization, and the principle of least privilege to ensure that users have the minimum access necessary to perform their tasks.
2. **Data Classification and Handling Policy:** Establishes guidelines for classifying data based on sensitivity and importance. It outlines how different types of data should be handled, stored, transmitted, and protected, including encryption requirements.
3. **Network Security Policy:** Defines rules and configurations for securing the network infrastructure in the cloud. This policy addresses firewall settings, network segmentation, secure communication channels, and other measures to protect against unauthorized access and network-based attacks.
4. **Encryption Policy:** Specifies the use of encryption for data both in transit and at rest. It outlines the encryption algorithms, key management practices, and the circumstances under which encryption should be applied.
5. **Incident Response Policy:** Outlines the procedures to be followed in the event of a security incident. It includes steps for reporting incidents, incident analysis, containment, eradication, recovery, and post-incident review.
6. **Backup and Recovery Policy:** Establishes guidelines for regular data backups and defines procedures for data recovery in case of data loss or a security incident. It includes the frequency of backups, storage locations, and verification processes.
7. **Third-Party Security Policy:** Provides guidelines for assessing and managing the security risks associated with third-party services or vendors. This policy outlines expectations regarding security controls, auditing, and compliance for third-party relationships.
8. **Cloud Usage Policy:** Outlines the acceptable use of cloud services within the organization. It may cover aspects such as approved cloud service providers, data residency, and guidelines for deploying and configuring cloud resources.

9. **Mobile Device Security Policy:** Addresses security considerations for mobile devices accessing cloud resources. It includes rules for device management, secure configurations, and measures to protect against the loss or theft of mobile devices.
10. **User Training and Awareness Policy:** Establishes guidelines for ongoing user training and awareness programs. It ensures that employees are educated about security best practices, social engineering threats, and the importance of adhering to security policies.
11. **Compliance Monitoring Policy:** Defines procedures for monitoring and ensuring compliance with security policies. This includes regular audits, assessments, and reporting mechanisms to verify adherence to security controls and regulatory requirements.
12. **Physical Security Policy:** Outlines measures to secure physical access to data centers or server rooms hosting cloud infrastructure. It includes guidelines for access controls, surveillance, and environmental controls.
13. **Vendor Management Policy:** Specifies the procedures for selecting, onboarding, and managing relationships with cloud service providers and other vendors. It includes security expectations, contractual obligations, and ongoing monitoring.
14. **Configuration Management Policy:** Defines rules for managing configurations of cloud resources. It ensures that systems are configured securely, and changes are documented and tested to prevent misconfigurations that could introduce security vulnerabilities.
15. **Social Media and Online Presence Policy:** Provides guidelines for employees regarding the use of social media and online platforms, especially when representing the organization. It addresses security considerations and the protection of sensitive information.

Implementation Strategies:

- **Communication and Awareness:** Clearly communicate the policies to all stakeholders, including employees, contractors, and third-party vendors. Ensure they understand their roles and responsibilities in maintaining cloud security.
- **Training and Education:** Provide training programs to educate employees on security best practices, phishing awareness, and proper cloud usage.
- **Technology Integration:** Leverage security tools and technologies to automate policy enforcement, such as identity and access management (IAM) systems, security information and event management (SIEM) solutions, and cloud security posture management (CSPM) tools.

- **Monitoring and Auditing:** Regularly monitor compliance with policies through audits and assessments. Identify and address any gaps or vulnerabilities.
- **Continuous Improvement:** Review and update policies regularly to adapt to evolving threats and cloud technologies. Foster a culture of continuous security improvement within your organization.

Challenges and Considerations:

- **Complexity of the Cloud:** The intricate nature of cloud ecosystems and shared responsibility models can complicate policy implementation.
- **Employee Behavior:** Human error and non-compliance with policies can pose significant security risks.
- **Technology Integration:** Integrating various security tools and technologies can be challenging and require ongoing maintenance.
- **Change Management:** Implementing new policies may encounter resistance from stakeholders. Effective communication and training are crucial.

Benefits of Effective Policy Implementation:

- **Reduced Risk of Security Breaches:** Proactive policies minimize vulnerabilities and make it harder for attackers to exploit your cloud environment.
- **Improved Data Security:** Strong data protection policies and practices safeguard sensitive information in the cloud.
- **Compliance with Regulations:** Implementing policies aligned with relevant data privacy and security regulations can avoid penalties and legal issues.
- **Increased Organizational Resilience:** Robust cloud security policies ensure your organization is prepared to handle security incidents and maintain business continuity.

By effectively implementing and continually adapting your cloud security policies, you can significantly enhance your cloud environment's security posture and protect your valuable data and systems. Remember, strong policies are the foundation of a secure cloud, but effective implementation is crucial for realizing their full potential.

Cloud Computing Security Challenges:

Cloud computing offers numerous benefits, including scalability, cost efficiency, and accessibility. However, it also introduces unique security challenges that organizations need to address to ensure the confidentiality, integrity, and availability of their data and applications. Some common cloud computing security challenges include:

1. **Data Breaches:** Unauthorized access to sensitive data is a significant concern. Whether due to misconfigurations, inadequate access controls, or sophisticated cyberattacks, data breaches can lead to the exposure of sensitive information.
2. **Inadequate Identity and Access Management (IAM):** Poorly implemented IAM practices can result in unauthorized access to cloud resources. Weak authentication, improper authorization, and insufficient monitoring of user activities contribute to this challenge.
3. **Insufficient Data Encryption:** Inadequate or improperly implemented data encryption can lead to data exposure, especially during data transfers or when data is stored in the cloud. Encryption should be applied both in transit and at rest to protect sensitive information.
4. **Shared Technology Vulnerabilities:** Cloud environments often share underlying infrastructure and services among multiple users. Vulnerabilities in shared components, such as hypervisors or underlying software stacks, can potentially lead to security risks for all users on the shared infrastructure.
5. **Lack of Visibility and Control:** Organizations may face challenges in maintaining visibility and control over their data and applications in the cloud. This is especially true in multi-cloud or hybrid cloud environments, where resources are distributed across various platforms.
6. **Insufficient Security due to Misconfigurations:** Misconfigurations of cloud resources, such as storage buckets, databases, or network settings, can result in security vulnerabilities. Human error in configuring cloud services is a common factor contributing to misconfigurations.
7. **Compliance and Legal Concerns:** Ensuring compliance with industry regulations and legal requirements can be challenging in the cloud. Different regions and industries have varied data protection and privacy laws, and navigating these complexities is crucial for compliance.
8. **Insecure APIs:** Application Programming Interfaces (APIs) facilitate communication and data exchange between cloud services. Insecure APIs can be exploited by attackers to gain unauthorized access or execute malicious activities.
9. **Denial of Service (DoS) Attacks:** Cloud services can be targeted by DoS attacks, affecting the availability of resources and disrupting service for legitimate users. This can lead to downtime and financial losses for organizations.

10. **Data Loss and Leakage:** Data loss or leakage can occur due to accidental deletion, unauthorized access, or vulnerabilities in cloud services. Organizations need robust backup and recovery mechanisms to mitigate the impact of data loss incidents.
11. **Inadequate Incident Response and Forensics:** Cloud environments require effective incident response plans and forensic capabilities to investigate and respond to security incidents. Limited visibility and control can complicate the detection and mitigation of security breaches.
12. **Supply Chain Risks:** Dependencies on third-party providers, including cloud service providers and other vendors, introduce supply chain risks. Organizations need to assess and manage the security posture of their providers and ensure they meet security standards.
13. **Shadow IT:** Employees may use unauthorized cloud services without the knowledge or approval of the IT department (shadow IT). This can lead to uncontrolled data exposure and potential security risks.
14. **Emerging Threat Landscape:** The rapid evolution of cyber threats poses a continuous challenge for cloud security. New attack vectors and sophisticated techniques require organizations to stay vigilant and update their security measures accordingly.

Cloud Security Solutions:

Cloud security solutions are used depending on each cloud environment's specific needs and requirements, and since it's a complex and evolving field, you must adapt to new technologies to keep up with the changing threats and challenges.

Here are some solutions you should put to use:

1. Security Information and Event Management (SIEM): SIEM collects, analyzes, and correlates data from sources, such as logs, alerts, and events, to show you a view of cloud environments' security posture and activity.

It's a cybersecurity technology that provides a single, streamlined view of your data, insight into security activities, and operational capabilities so you can effectively detect, investigate and respond to security threats.

2. Identity and Access Management (IAM): The IAM framework manages the identities and access rights of users and entities in cloud environments.

It's a set of technologies, rules, and practices that IT departments employ to manage control and give network access permissions. With IAM, your assets are protected by ensuring that particular users can access the essential assets in the proper context.

3. Data Loss Prevention (DLP): DLP monitors and controls the movement and usage of sensitive or confidential data in cloud environments. It prevents data leakage, exposure, or theft, by applying rules and actions based on data classification, content, context, and destination.

4. Public Key Infrastructure (PKI): PKI is a solution that uses cryptography to secure the communication and transactions between users and entities in cloud environments. It can help you encrypt, decrypt, sign, and verify data using public and private keys, certificates, and certificate authorities.

5. Cloud-Native Application Protection Platform (CNAPP): CNAPP provides end-to-end security for cloud-native applications that run on containers, serverless platforms, or microservices architectures. Here's how it secures the application lifecycle, from development to deployment to runtime:

- Scanning for vulnerabilities and misconfigurations
- Integrating with DevOps tools and processes
- Enforcing policies and compliance
- Detecting and preventing attacks

6. Disaster Recovery and Business Continuity (DRBC): DR and BC help restore and continue cloud operations in case of a disaster or an attack. They can help you ensure data availability, integrity, and resilience by:

- Providing backup
- Replication
- Failover
- Recovery
- Testing capabilities

7. Cloud Security Posture Management (CSPM): CSPM monitors and assesses cloud environments' security configuration and compliance. It identifies security gaps, misconfigurations, and violations by providing:

- Visibility
- Automation
- Reporting
- Remediation

8. Secure Access Service Edge (SASE): SASE converges network and security services into a unified cloud-based platform. It delivers secure and reliable access to cloud resources from any device or location by providing the following capabilities:

- Firewall-as-a-service (FWaaS)
- Zero-trust network access (ZTNA)
- Software-defined wide area network (SD-WAN)
- Secure web gateway (SWG)
- Cloud access security broker (CASB)

Cloud Computing Security Architecture:

Security Planning:

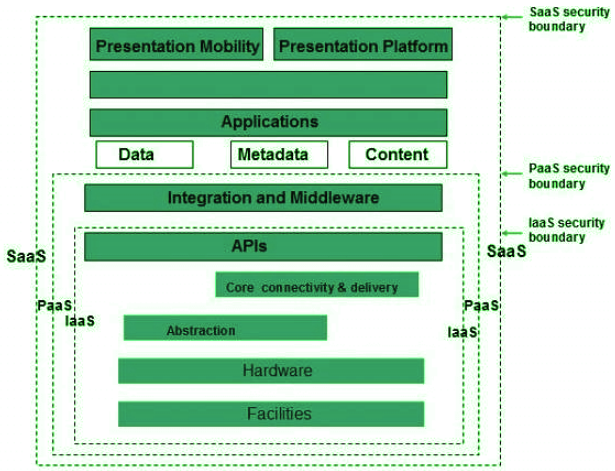
Before deploying a particular resource to the cloud, one should need to analyze several aspects of the resource, such as:

- 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:**



Key Points to CSA Model:

- IaaS is the most basic level of service, with PaaS and SaaS next two above levels of services.
- Moving upwar++ds, 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.

Although each service model has a security mechanism, security requirements also depend on where these services are located, private, public, hybrid, or community cloud.

Understanding data security:

Since all data is transferred using the Internet, data security in the cloud is a major concern. Here are the key mechanisms to protect the data.

- access control
- audit trail
- certification
- authority

The service model should include security mechanisms working in all of the above areas.

Separate access to data:

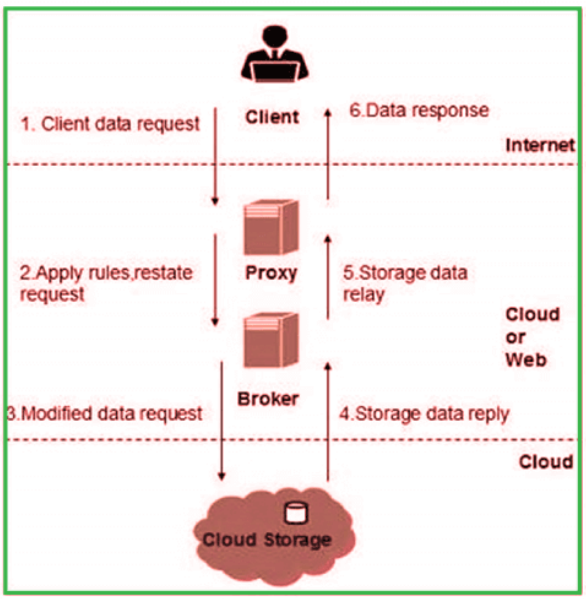
Since the data stored in the cloud can be accessed from anywhere, we need to have a mechanism to isolate the data and protect it from the client's direct access.

Broker cloud storage is a way of separating storage in the Access Cloud. In this approach, two services are created:

1. A broker has full access to the storage but does not have access to the client.

2. A proxy does not have access to storage but has access to both the client and the broker.
3. Working on a Brocade cloud storage access system
4. When the client issues a request to access data:
5. The client data request goes to the external service interface of the proxy.
6. The proxy forwards the request to the broker.
7. The broker requests the data from the cloud storage system.
8. The cloud storage system returns the data to the broker.
9. The broker returns the data to the proxy.
10. Finally, the proxy sends the data to the client.

All the above steps are shown in the following diagram:



Encoding:

Encryption helps to protect the data from being hacked. It protects the data being transferred and the data stored in the cloud. Although encryption helps protect data from unauthorized access, it does not prevent data loss.

Why is cloud security architecture important?

The difference between "cloud security" and "cloud security architecture" is that the former is built from problem-specific measures while the latter is built from threats. A cloud security architecture can reduce or eliminate the holes in Security that point-of-solution approaches are almost certainly about to leave.

It does this by building down - defining threats starting with the users, moving to the cloud environment and service provider, and then to the applications. Cloud security architectures can also reduce redundancy in security measures, which will contribute to threat mitigation and increase both capital and operating costs.

The cloud security architecture also organizes security measures, making them more consistent and easier to implement, particularly during cloud deployments and redeployments. Security is often destroyed because it is illogical or complex, and these flaws can be identified with the proper cloud security architecture.

Elements of cloud security architecture:

The best way to approach cloud security architecture is to start with a description of the goals. The architecture has to address three things: an attack surface represented by external access interfaces, a protected asset set that represents the information being protected, and vectors designed to perform indirect attacks anywhere, including in the cloud and attacks the system.

The goal of the cloud security architecture is accomplished through a series of functional elements. These elements are often considered separately rather than part of a coordinated architectural plan. It includes access security or access control, network security, application security, contractual Security, and monitoring, sometimes called service security. Finally, there is data protection, which are measures implemented at the protected-asset level.

A complete cloud security architecture addresses the goals by unifying the functional elements.

Cloud security architecture and shared responsibility model:

The security and security architectures for the cloud are not single-player processes. Most enterprises will keep a large portion of their IT workflow within their data centers, local networks, and VPNs. The cloud adds additional players, so the cloud security architecture should be part of a broader shared responsibility model.

A shared responsibility model is an architecture diagram and a contract form. It exists formally between a cloud user and each cloud provider and network service provider if they are contracted separately.

Each will divide the components of a cloud application into layers, with the top layer being the responsibility of the customer and the lower layer being the responsibility of the cloud provider. Each separate function or component of the application is mapped to the appropriate layer depending on who provides it. The contract form then describes how each party responds.

Legal Issues in Cloud Computing:

Legal issues in cloud computing involve a range of concerns related to privacy, compliance, intellectual property, data protection, and contractual agreements. Here are some of the key legal issues that organizations may encounter when using cloud computing services:

1. **Data Privacy and Protection:**
   - **GDPR Compliance:** The General Data Protection Regulation (GDPR) in the European Union imposes strict rules on the processing and storage of personal data. Organizations using cloud services must ensure compliance with GDPR requirements.
   - **Data Ownership and Control:** Clarifying data ownership and control is crucial. Cloud customers need to understand where their data is stored, who has access to it, and how it can be transferred or deleted.
2. **Data Security:**
   - **Security Breaches and Notifications:** In the event of a security breach, cloud service providers and their customers may have legal obligations to notify affected parties, regulators, or law enforcement agencies.
   - **Security Standards and Certifications:** Ensure that cloud providers adhere to industry-standard security certifications (e.g., ISO 27001) to meet legal and regulatory requirements.
3. **Compliance with Industry Regulations:** Different industries may have specific regulations governing the handling of data. For example, healthcare organizations must comply with the Health Insurance Portability and Accountability Act (HIPAA), while financial institutions adhere to regulations like the Payment Card Industry Data Security Standard (PCI DSS).
4. **Intellectual Property Rights:** Clarify the terms of software licensing and ownership of intellectual property in the cloud. Organizations should understand how their data and applications are treated in terms of licensing and ownership rights.
5. **Contractual Agreements:**
   - **Service Level Agreements (SLAs):** Cloud customers should carefully review SLAs to understand service guarantees, performance levels, and the responsibilities of the cloud provider. SLAs may also outline dispute resolution mechanisms.
   - **Terms and Conditions:** Clearly define the terms and conditions of the contractual relationship between the cloud customer and provider. This includes liability, indemnification, and termination clauses.

6. **Cross-Border Data Transfers:** Transferring data across borders may be subject to restrictions and regulations. Organizations must ensure that they comply with data protection laws and regulations in the countries where they operate.
7. **E-Discovery and Legal Hold:** In legal proceedings, organizations may need to produce electronically stored information (ESI). Cloud customers should understand how to meet e-discovery obligations, including data preservation and retrieval from the cloud.
8. **Government Surveillance Laws:** Different countries have laws that allow government authorities to access data for national security or law enforcement purposes. Cloud customers should be aware of these laws and their implications.
9. **Audit and Compliance Verification:** Cloud customers may need the ability to audit the cloud provider's security practices and data handling procedures to ensure compliance with legal and regulatory requirements.
10. **Exit Strategy:** Develop an exit strategy that ensures data portability and the ability to transition to another cloud provider or back to an on-premises environment without encountering legal and technical obstacles.
11. **Subcontractor Agreements:** Understand the cloud provider's use of subcontractors or third-party services and ensure that these arrangements comply with legal and regulatory requirements.
12. **Liability and Indemnification:** Review and negotiate liability limits in contracts to ensure they are reasonable and proportional to the risks involved. Clarify indemnification clauses to allocate responsibility for legal liabilities.