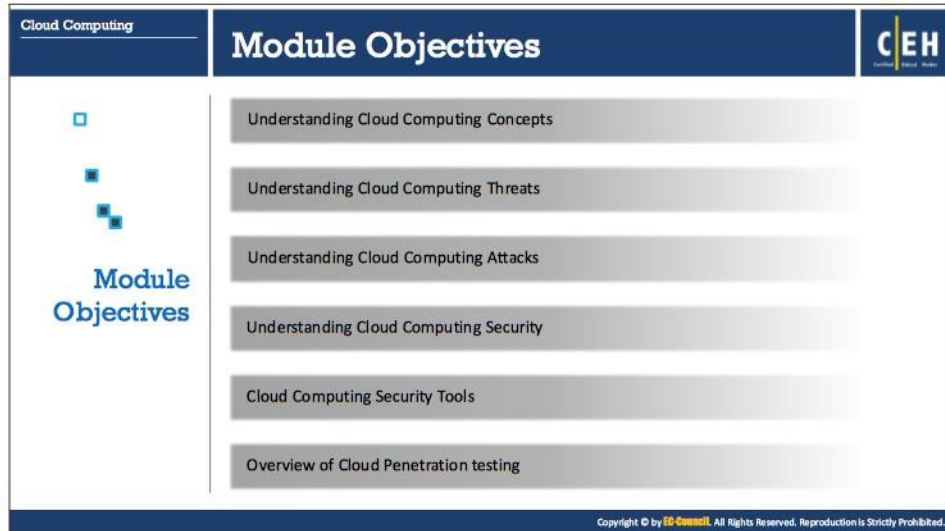




Module 19

## Cloud Computing



Cloud Computing

## Module Objectives

CEH

- Understanding Cloud Computing Concepts
- Understanding Cloud Computing Threats
- Understanding Cloud Computing Attacks
- Understanding Cloud Computing Security
- Cloud Computing Security Tools
- Overview of Cloud Penetration testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

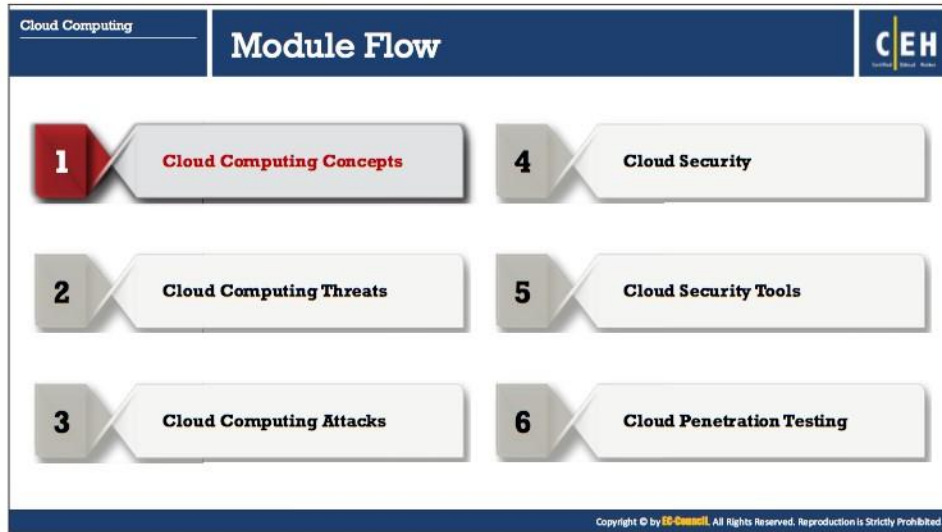
## Module Objectives

Cloud computing is an emerging technology that delivers computing services such as online business applications, online data storage, and webmail over the Internet. Cloud implementation enables a distributed workforce, reduces organization expenses, and provides data security, and so on. As many enterprises are adopting the cloud, attackers make cloud as their target of an exploit to gain unauthorized access to the valuable data stored in it. Therefore, one should perform cloud pen testing regularly to monitor its security posture.

This module starts with an overview of cloud computing concepts. It provides an insight into cloud computing threats and cloud computing attacks. Later, it discusses cloud computing security and the necessary tools. The module ends with an overview of pen-testing steps which an ethical hacker should follow to perform a security assessment of the cloud environment.

At the end of this module, you will be able to:

- Describe cloud computing concepts
- Understand cloud computing threats
- Explain cloud computing attacks
- Apply cloud computing security measures
- Use various cloud computing security tools
- Perform cloud penetration testing



## Cloud Computing Concepts

Cloud computing delivers various types of services and applications over the Internet. These services enable users to utilize software and hardware managed by third parties at remote locations. Some of the cloud service providers include Google, Amazon, and Microsoft.

This section introduces cloud computing, types of cloud computing services, separation of responsibilities, cloud deployment models, the NIST reference architecture, benefits, and the general benefits of cloud virtualization.



The slide is titled "Introduction to Cloud Computing" and is part of a presentation on "Cloud Computing Concepts". It features the CEH logo in the top right corner. The main content is organized into several sections:

- Definition:** Cloud computing is an on-demand delivery of IT capabilities where IT infrastructure and applications are provided to subscribers as a metered service over a network.
- Characteristics of Cloud Computing:** A grid of eight boxes listing: On-demand self service, Broad network access, Distributed storage, Resource pooling, Rapid elasticity, Measured service, Automated management, and Virtualization technology.
- Types of Cloud Computing Services:** A vertical list of three service models, each associated with a user role:
  - Infrastructure-as-a-Service (IaaS):** Associated with "SYS ADMINS". Provides virtual machines and other abstracted hardware and operating systems which may be controlled through a service API. Examples: Amazon EC2, Go grid, Sungrid, Windows SkyDrive, Rackspace.com, etc.
  - Platform-as-a-Service (PaaS):** Associated with "DEVELOPERS". Offers development tools, configuration management, and deployment platforms on-demand that can be used by subscribers to develop custom applications. Examples: Intel MashMaker, Google App Engine, Force.com, Microsoft Azure, etc.
  - Software-as-a-Service (SaaS):** Associated with "END CUSTOMERS". Offers software to subscribers on-demand over the Internet. Examples: web-based office applications like Google Docs or Calendar, Salesforce CRM, Freshbooks, basecamp, etc.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Introduction to Cloud Computing

Cloud computing is an on-demand delivery of IT capabilities in which IT infrastructure and applications are provided to subscribers as metered services over networks. Examples of cloud solutions include Gmail, Facebook, Dropbox, and Salesforce.com.

### Characteristics of Cloud Computing

Discussed below are the characteristics of cloud computing that attract many businesses today to adopt cloud technology.

- **On-demand self-service:** A type of service rendered by cloud service providers that allow provisions for cloud resources such as computing power, storage, network, etc., always on demand, without the need for human interaction with service providers.
- **Distributed storage:** Distributed storage in the cloud offers better scalability, availability, and reliability of data. However, cloud distributed storage does have the potential for security and compliance concerns.
- **Rapid elasticity:** The cloud offers instant provisioning of capabilities, to rapidly scale up or down, according to demand. To the consumers, the resources available for provisioning seem to be unlimited, and they can purchase in any quantity at any point of time.
- **Automated management:** By minimizing the user involvement, cloud automation speeds up the process, reduces labor costs, and reduces the possibility of human error.
- **Broad network access:** Cloud resources are available over the network and accessed through standard procedures, via a wide-variety of platforms, including laptops, mobile phones, and PDAs.



- **Resource pooling:** The cloud service provider pools all the resources together to serve multiple customers in the multi-tenant environment, with physical and virtual resources dynamically assigned and reassigned on demand by the consumer of cloud.
- **Measured service:** Cloud systems employ “pay-per-use” metering method. Subscribers pay for cloud services by monthly subscription or according to the usage of resources such as storage levels, processing power, bandwidth, and so on. Cloud service providers monitor, control, report, and charge consumption of resources by customers with complete transparency.
- **Virtualization technology:** Virtualization technology in the cloud enables rapid scaling of resources in a way that non-virtualized environments could not achieve.

#### **Limitations of Cloud Computing**

- Organizations have limited control and flexibility
- Prone to outages and other technical issues
- Security, privacy, and compliance issues
- Contracts and lock-ins
- Depends on network connections

#### **Types of Cloud Computing Services**

Cloud services are divided broadly into three categories:

- **Infrastructure-as-a-Service (IaaS)**

This cloud computing service enables subscribers to use on demand fundamental IT resources such as computing power, virtualization, data storage, network, and so on. This service provides virtual machines and other abstracted hardware and operating systems (OSs) which may be controlled through a service API. As cloud service providers are responsible for managing the underlying cloud-computing infrastructure, subscribers can avoid costs of human capital, hardware, and others (e.g., Amazon EC2, Go grid, Sungrid, Windows SkyDrive, Rackspace.com, etc.).

##### **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

▪ **Platform-as-a-Service (PaaS)**

This type of cloud computing service offers the platform for the development of applications and services. Subscribers need not to buy and manage the software and infrastructure underneath it but have authority over deployed applications and perhaps application hosting environment configurations. This offers development tools, configuration management, and deployment platforms on-demand that can be used by subscribers to develop custom applications (E.g., Intel MashMaker, Google App Engine, Force.com, Microsoft Azure, etc.). Advantages of writing applications in the PaaS environment includes dynamic scalability, automated backups, and other platform services, without the need to explicitly code for it.

**Advantages:**

- Simplified deployment
- Prebuilt business functionality
- Lower risk
- Instant community
- Pay-per-use model
- Scalability

**Disadvantages:**

- Vendor lock-in
- Data privacy
- Integration with the rest of the system applications

▪ **Software-as-a-Service (SaaS)**

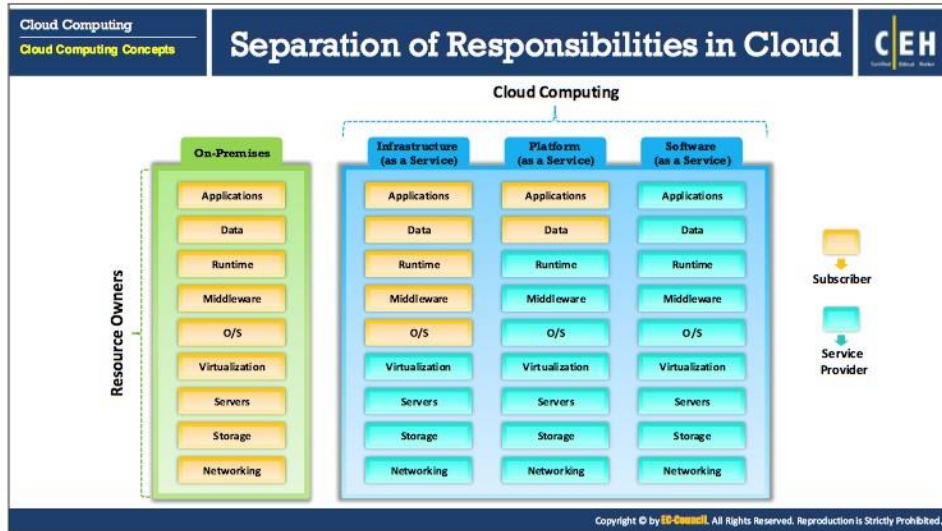
This cloud computing service offers application software to subscribers on demand over the Internet; the provider charges for it on a pay-per-use basis, by subscription, by advertising, or by sharing among multiple users (E.g. web-based office applications like Google Docs or Calendar, Salesforce CRM, Freshbooks, Basecamp, etc.).

**Advantages:**

- Low cost
- Easier administration
- Global accessibility
- Compatible (no specialized hardware or software is required)

**Disadvantages:**

- Security and latency issues
- Total dependency on the Internet
- Switching between SaaS vendors is difficult



### Separation of Responsibilities in Cloud

In cloud computing, separation of responsibilities of subscriber and service provider is essential. Separation of duties prevents conflict of interest, illegal acts, fraud, abuse, and error, and helps in identifying security control failures, including information theft, security breaches, and evasion of security controls. It also helps in restricting the amount of influence held by any individual and ensures that there are no conflicting responsibilities.

Three types of cloud services exist (IaaS), PaaS, and SaaS. It is essential to know the limitations of each cloud service delivery model when accessing specific clouds and their models. The diagram above illustrates the separation of cloud responsibilities specific to service delivery models:





Cloud Computing  
Cloud Computing Concepts

## Cloud Deployment Models

CEH  
Certified Ethical Hacker

Cloud deployment model selection is based on the **enterprise requirements**

<h3>Public Cloud</h3> <p>Services are rendered over a <b>network that is open for public use</b></p> 	<h3>Private Cloud</h3> <p>Cloud infrastructure operated solely for a <b>single organization</b></p> 
<h3>Community Cloud</h3> <p>Shared infrastructure between <b>several organizations from a specific community</b> with common concerns (security, compliance, jurisdiction, etc.)</p>	<h3>Hybrid Cloud</h3> <p><b>Composition of two or more clouds</b> (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models</p>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Cloud Deployment Models

Cloud deployment model selection is based on the enterprise requirements. One can deploy cloud services in different ways, according to the factors given below:

- Where cloud computing services are hosted
- Security requirements
- Sharing cloud services
- Ability to manage some or all of the cloud services
- Customization capabilities

The four standard cloud deployment models are:

- **Public Cloud**

In this model, the provider makes services such as applications, servers, and data storage available to the public over the Internet. In this model, the cloud provider is liable for the creation and constant maintenance of the public cloud and its IT resources. Public cloud services may be free or based on a pay-per-usage model (e.g., Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Google App Engine, Windows Azure Services Platform).

- **Advantages:**

- Simplicity and efficiency
- Low cost
- Reduced time (when server crashes, needs to restart or reconfigure cloud)

- No maintenance (public cloud service is hosted off-site)
- No contracts (no long-term commitments)
- **Disadvantages:**
  - Security is not guaranteed
  - Lack of control (third-party providers are in charge)
  - Slow speed (relies on Internet connections, data transfer rate is limited)

▪ **Private Cloud**

A private cloud, also known as internal or corporate cloud, is a cloud infrastructure that a single organization operates solely. The organization can implement the private cloud within a corporate firewall. Organizations deploy private cloud infrastructures to retain full control over corporate data.

- **Advantages:**
  - Enhance security (services are dedicated to a single organization)
  - More control over resources (organization is in charge)
  - Greater performance (deployed within the firewall, therefore data transfer rates are high)
  - Customizable hardware, network, and storage performances (as the organization owns private cloud)
  - Sarbanes Oxley, PCI DSS, and HIPAA compliance data is much easier to attain
- **Disadvantages:**
  - Expensive
  - On-site maintenance

▪ **Community Cloud**

It is a multi-tenant infrastructure shared among organizations from a specific community with common computing concerns such as security, regulatory compliance, performance requirements, and jurisdiction. The community cloud can be either on-premises or off-premises and governed by the participated organizations or by a third-party managed service provider.

- **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 and from anywhere via Internet

○ **Disadvantages:**

- Competition between consumers in usage of resources
- No accurate prediction of required resources
- Who is the legal entity in case of liability
- Moderate security (other tenants may be able to access data)
- Trust and security concerns between the tenants

▪ **Hybrid Cloud**

It is a cloud environment comprised of two or more clouds (private, public, or community) that remain unique entities but bound together for offering the benefits of multiple deployment models. In this model, the organization makes available, manages some resources in-house, and provides other resources externally.

**Example:** An organization performs its critical activities on the private cloud (such as operational customer data) and non-critical activities on the public cloud.

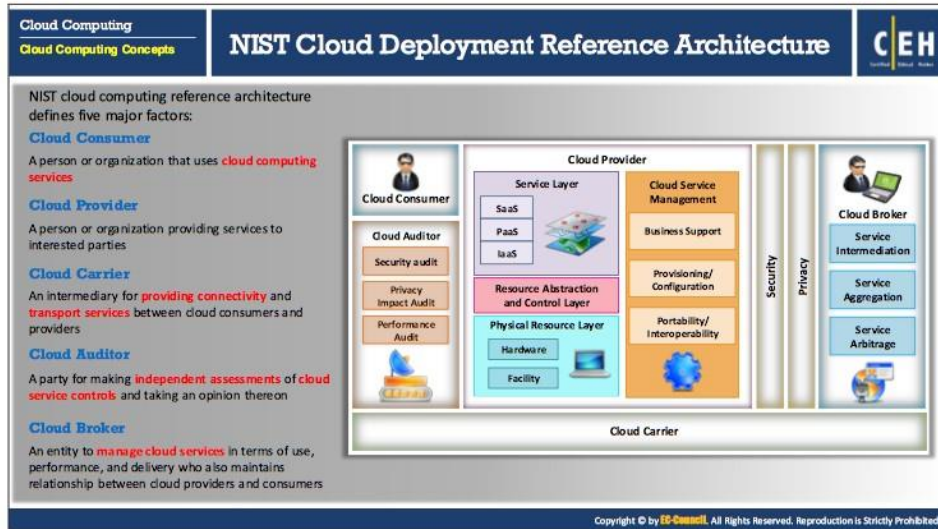
○ **Advantages:**

- More scalable (contains both public and private clouds)
- Offers both secure resources and scalable public resources
- High level of security (comprises private cloud)
- Allows to reduce and manage the cost as per the requirement

○ **Disadvantages:**

- Communication at the network level may be conflicted as it uses both public and private clouds
- Difficult to achieve data compliance
- Organization has to rely on the internal IT infrastructure for support to handle any outages (maintain redundancy across data centers to overcome)
- Complex Service Level Agreements (SLAs)





### NIST Cloud Deployment Reference Architecture

The slide provides an overview of the NIST cloud computing reference architecture, displaying the primary actors, their activities, and functions in cloud computing. The diagram above is a generic high-level architecture, intended for better understanding of uses, requirements, characteristics, and standards of cloud computing.

The five significant actors are:

- **Cloud consumer**

A cloud consumer is a person or organization that maintains a business relationship with cloud service providers and uses cloud computing services. The cloud consumer browses the CSP's service catalog requests for the desired services, sets up service contracts with the CSP (either directly or via cloud broker) and uses the service. The CSP will bill the consumer based on the services provided. The CSP should fulfill Service Level Agreement (SLA) in which the cloud consumer specifies the technical performance requirements such as quality of service, security, remedies for performance failure, etc. The CSP may also define limitations and obligations, if any that cloud consumer must accept. Services available to a cloud consumer in, **PaaS, IaaS, and SaaS** models:

- **PaaS** – database, business intelligence, application deployment, development and testing, and integration
- **IaaS** – storage, services management, CDN (content delivery network), platform hosting, backup and recovery, and compute
- **SaaS** – human resources, ERP (Enterprise Resource Planning), sales, CRM (Customer Relationship Management), collaboration, document management, email and office productivity, content management, financials, and social networks.

- **Cloud Provider**

A cloud provider is a person or organization who acquires and manages the computing infrastructure intended for providing services (directly or via a cloud broker) to interested parties via network access.

- **Cloud Carrier**

A cloud carrier acts as an intermediary that provides connectivity and transport services between CSPs and cloud consumers. The cloud carrier provides access to consumers via a network, telecommunication, and other access devices.

- **Cloud Auditor**

A cloud auditor is a party that performs an independent examination of cloud service controls with the intent of expressing an opinion thereon. Audits verify adherence to standards through a review of the objective evidence. A cloud auditor can evaluate the services provided by a cloud provider regarding security controls (management, operational, and technical safeguards intended to protect the confidentiality, integrity, and availability of the system and its information), privacy impact (comply with applicable privacy laws and regulations governing an individual's privacy), performance, and so on.

- **Cloud Broker**

Integration of cloud services is becoming too complicated for cloud consumers to manage. Thus, a cloud consumer may request cloud services from a cloud broker, rather than directly contacting a CSP. The cloud broker is an entity that manages cloud services regarding use, performance, and delivery, and maintains the relationship between CSPs and cloud consumers.

Cloud brokers provide services in three categories:

- **Service Intermediation**

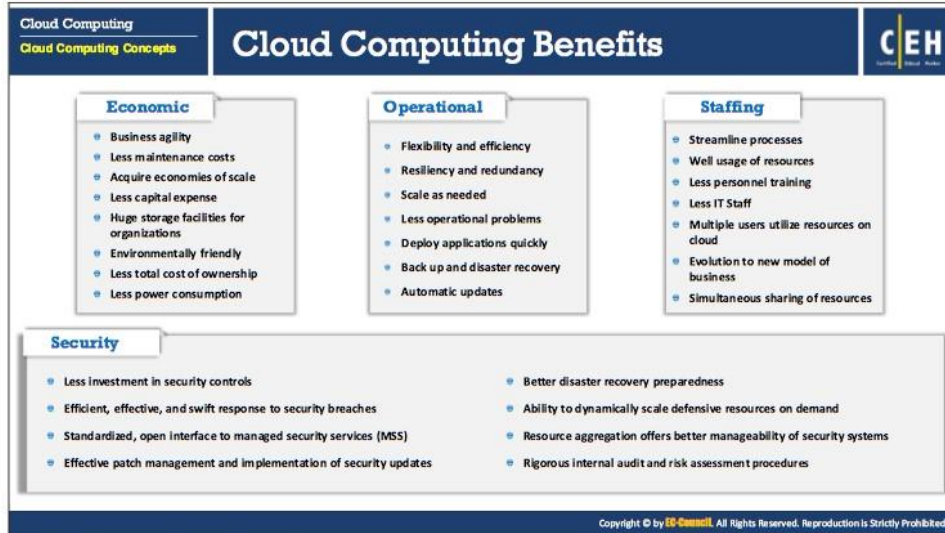
Improves a given function by a specific capability and provides value-added services to cloud consumers.

- **Service Aggregation**

Combines and integrates multiple services into one or more new services.

- **Service Arbitrage**

Similar to service aggregation, but here the services being aggregated are not fixed (cloud broker has the flexibility to choose services from multiple agencies).



### Cloud Computing Benefits

- **Economic**
  - Business agility
  - Less maintenance costs
  - Acquire economies of scale
  - Less capital expense
  - Huge storage facilities for organizations
  - Environmentally friendly
  - Less total cost of ownership
  - Less power consumption
- **Operational**
  - Flexibility and efficiency
  - Resiliency and redundancy
  - Scale as needed
  - Less operational problems
  - Deploy applications quickly
  - Back up and disaster recovery
  - Automatic updates

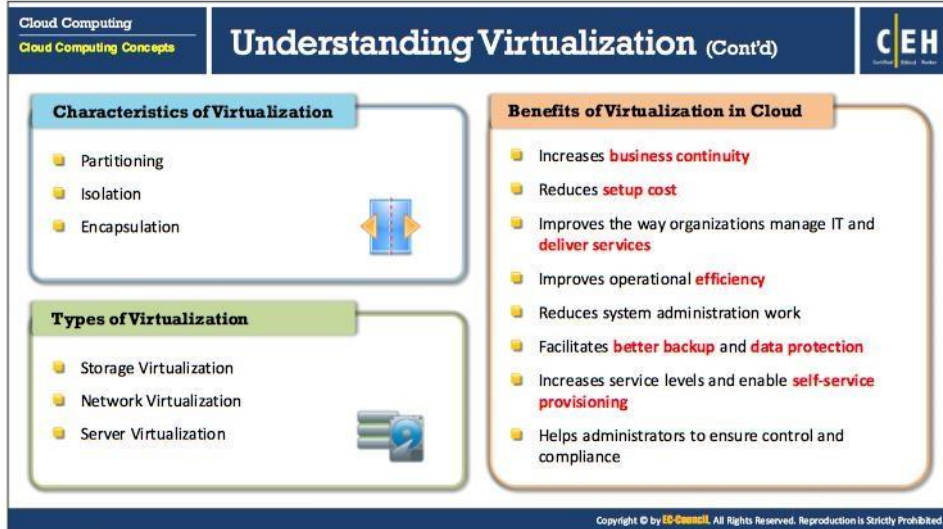
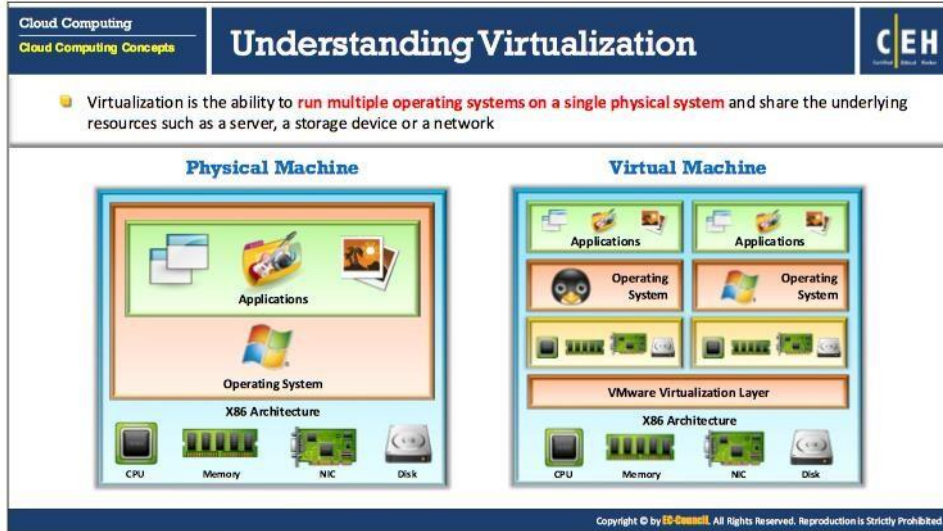


▪ **Staffing**

- Streamline processes
- Well usage of resources
- Less personnel training
- Less IT Staff
- Multiple users utilize resources on cloud
- Evolution of new model of business
- Simultaneous sharing of resources

▪ **Security**

- Less investment in security controls
- Efficient, effective, and swift response to security breaches
- Standardized, open interface to managed security services (MSS)
- Effective patch management and implementation of security updates
- Better disaster recovery preparedness
- Ability to dynamically scale defensive resources on demand
- Resource aggregation offers better manageability of security systems
- Rigorous internal audit and risk assessment procedures



### Understanding Virtualization

Virtualization is the ability to run multiple OSs on a single physical system and share the underlying resources such as a server, a storage device, or network. It is the essential technology that powers cloud computing. Virtualization allows organizations to cut IT costs while enhancing the productivity, utilization, and flexibility of their existing computer hardware. Some of the virtualization vendors include VMware vCloud Suite, VMware vSphere, VirtualBox, Microsoft Virtual PC, etc.

- **Types of Machines**

- **Physical Machine**

- The architecture of a physical machine consists of CPU, memory, NIC, disk, OS, etc. It consumes the complete existing physical resources.

- **Virtual Machine**

- A virtual machine is a machine that sits on the standard physical resources. These machines have an advantage over physical machines since many OSs, memory allocation, etc. is possible over the existing physical resource. Virtual machines are used effectively in cloud computing environments.

- **Characteristics of virtualization in cloud computing technology**

- **Partitioning**

- The cloud supports many applications and multiple OSs in a single physical system by segregating the available resources.

- **Isolation**

- Cloud isolates each virtual machine from its host physical system and other virtual machines, so that if one virtual machine fails it does not have any impact on the others as well as on the data sharing.

- **Encapsulation**

- A virtual machine can be stored as a single file, and thus can be identified based on its service. Encapsulation protects each application from interfering with other applications.

- **Types of virtualization**

- **Storage Virtualization**

- It combines storage devices from multiple networks into a single storage device and helps in:

- Expanding the storage capacity
    - Making changes to store configuration easy

- **Network Virtualization**

- It combines all network resources, both hardware, and software into a single virtual network and is used to:

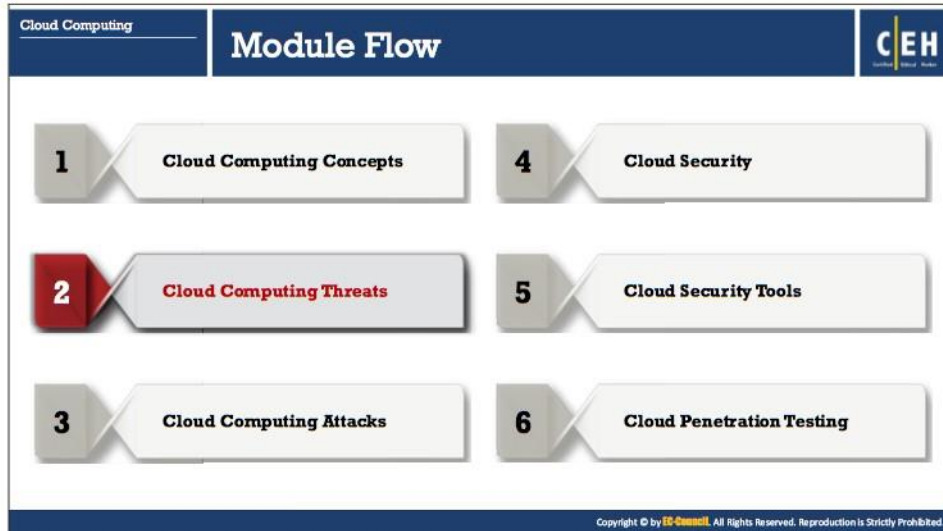
- Optimize reliability and security
    - Improves network resource usage



- **Server Virtualization**

It splits a physical server into multiple smaller virtual servers. Storage utilization is used to:

  - Increase the space utilization
  - Reduces the hardware maintenance cost
- **Benefits of Virtualization in Cloud**
  - Increases business continuity through efficient disaster recovery
  - Reduces cost of setting cloud infrastructure (cost on hardware, servers, etc.)
  - Improves the way organizations manage IT and deliver services
  - Improves operational efficiency
  - Reduces system administration work
  - Facilitates better backup and data protection
  - Increases service levels and enable self-service provisioning
  - Helps administrators to ensure control and compliance



## Cloud Computing Threats

Most organizations adopt the cloud technology, as it reduces the cost via optimized and efficient computing. Robust cloud technology offers different types of services to end users; many people are concerned about critical cloud security risks and threats, which an attacker may take as an advantage to compromise data security, gain illegal access of the network, and so on. This section deals with significant security threats and vulnerabilities affecting cloud systems.

Cloud Computing  
Cloud Computing Threats

## Cloud Computing Threats

CEH

1. Data breach/loss
2. Abuse and Nefarious Use of Cloud services
3. Insecure interfaces and APIs
4. Insufficient due diligence
5. Shared technology issues
6. Unknown risk profile
7. Unsynchronized system clocks
8. Inadequate infrastructure design and planning
9. Conflicts between client hardening procedures and cloud environment
10. Loss of operational and security logs
11. Malicious insiders
12. Illegal access to cloud systems
13. Loss of business reputation due to co-tenant activities
14. Privilege escalation
15. Natural disasters
16. Hardware failure
17. Supply chain failure
18. Modifying network traffic
19. Isolation failure
20. Cloud provider acquisition
21. Management interface compromise
22. Network management failure
23. Authentication attacks
24. VM-level attacks
25. Lock-in
26. Licensing risks
27. Loss of governance
28. Loss of encryption keys
29. Risks from changes of Jurisdiction
30. Undertaking malicious probes or scans
31. Theft of computer equipment
32. Cloud service termination or failure
33. Subpoena and e-discovery
34. Improper data handling and disposal
35. Loss or modification of backup data
36. Compliance risks
37. Economic Denial of Sustainability (EDoS)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing  
Cloud Computing Threats

## Cloud Computing Threats

CEH

### Data Breach/Loss

Data loss issues include:

- Data is **erased**, modified or decoupled (lost)
- **Encryption keys are lost**, misplaced or stolen
- **Illegal access to the data** in cloud due to improper authentication, authorization, and access controls
- **Misuse of data** by CSP

### Abuse and Nefarious Use of Cloud services

Attackers **create anonymous access to cloud services** and perpetrate various attacks such as:

- **Password and key** cracking
- Building rainbow tables
- **CAPTCHA-solving** farms
- Launching **dynamic attack points**
- Hosting **exploits** on cloud platforms
- Hosting **malicious data**
- **Botnet** command or control
- **DDoS**

### Insecure Interfaces and APIs

Insecure interfaces and APIs related risks:

- Circumvents **user defined policies**
- Is not credential leak proof
- Breach in **logging and monitoring facilities**
- Unknown API dependencies
- Reusable **passwords/tokens**
- Insufficient input-data validation

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing		Cloud Computing Threats (Cont'd)		CEH	
Cloud Computing Threats					
<b>Insufficient Due Diligence</b>		Ignorance of CSP's cloud environment pose risks in <b>operational responsibilities</b> such as security, encryption, incident response, and more issues such as contractual issues, design and architectural issues, etc.			
<b>Shared Technology Issues</b>		Most underlying components that make up the cloud infrastructure (ex: GPU, CPU caches, etc.) <b>does not offer strong isolation properties</b> in a multi-tenant environment which enables attackers to attack other machines if they can exploit vulnerabilities in one client's applications			
<b>Unknown Risk Profile</b>		Client organizations are unable to get a clear picture of internal security procedures, security compliance, configuration hardening, patching, auditing, and logging, etc. as they are less involved with <b>hardware and software ownership</b> and maintenance in the cloud			
<b>Unsynchronized System Clocks</b>		<ul style="list-style-type: none"><li>Unsynchronized clocks can <b>affect the working of automated tasks</b></li><li>Network administrator would be unable to accurately analyze the log files for any malicious activity, if the time stamps are mismatched</li></ul>			

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing		Cloud Computing Threats (Cont'd)		CEH	
Cloud Computing Threats					
<b>Inadequate Infrastructure Design and Planning</b>		<b>Conflicts between Client Hardening Procedures and Cloud Environment</b>			
<ul style="list-style-type: none"><li>Shortage of computing resources and/or poor network design gives rise to unacceptable <b>network latency or inability to meet agreed service levels</b></li></ul>		<ul style="list-style-type: none"><li>Certain client hardening procedures may conflict with a <b>cloud provider's environment</b>, making their implementation by the client impossible</li></ul>			
<b>Loss of Operational and Security Logs</b>		<b>Malicious Insiders</b>			
<ul style="list-style-type: none"><li>The loss of security logs poses a <b>risk for managing the implementation of the information security management program</b></li><li>Loss of security logs may occur in case of under-provisioning of storage</li></ul>		<ul style="list-style-type: none"><li>Disgruntled current or former employees, contractors, or other business partners who have authorized access to cloud resources can misuse their access to compromise the <b>information available in the cloud</b></li></ul>			

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Computing Cloud Computing Threats	<h2>Cloud Computing Threats (Cont'd)</h2>	CEH
<b>Illegal Access to the Cloud</b> Weak authentication and authorization controls could lead to illegal access thereby compromising confidential and critical data stored in the cloud		
<b>Loss of Business Reputation due to Co-tenant Activities</b> Resources are shared in the cloud, thus malicious activity of one co-tenant might affect the reputation of the other, resulting in poor service delivery, data loss, etc. that bring down organization's reputation		
<b>Privilege Escalation</b> A mistake in the access allocation system causes a customer, third party, or employee to get more access rights than needed		
<b>Natural Disasters</b> Based on geographic location and climate, data centers may be exposed to natural disasters such as floods, lightning, earthquakes, etc. that can affect the cloud services		
<b>Hardware Failure</b> Hardware failure such as switches, servers, etc. in data centers can make the cloud data inaccessible		
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.		

Cloud Computing Cloud Computing Threats	<h2>Cloud Computing Threats (Cont'd)</h2>	CEH
<b>Supply Chain Failure</b> <ul style="list-style-type: none"><li>Cloud providers outsource certain tasks to third parties. Thus the security of the cloud is directly proportional to security of each link and the extent of dependency on third parties</li><li>A disruption in the chain may lead to loss of data privacy and integrity, services unavailability, violation of SLA, economic and reputational losses resulting in failure to meet customer demand, and cascading failure</li></ul> 		
<b>Modifying Network Traffic</b> <ul style="list-style-type: none"><li>In cloud, the network traffic may be modified due to flaws while provisioning or de-provisioning network, or vulnerabilities in communication encryption</li><li>Modification of network traffic may cause loss, alteration, or theft of confidential data and communications</li></ul> 		
<b>Isolation Failure</b> <ul style="list-style-type: none"><li>Due to the isolation failure, attackers try to control operations of other cloud customers to gain illegal access to the data</li></ul> 		
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.		

Cloud Computing  
Cloud Computing Threats

## Cloud Computing Threats (Cont'd)

CEH  
Certified Ethical Hacker

<h3>Cloud Provider Acquisition</h3> <p>Acquisition of the cloud provider may <b>increase the probability of tactical shift</b> and may affect non-binding agreements at risk. This could make it difficult to cope up with the security requirements</p>	<h3>Management Interface Compromise</h3> <p>Customer management interfaces of cloud provider are accessible via the Internet and facilitate <b>access to a large number of resources</b>. This enhances the risk, particularly when combined with <b>remote access</b> and <b>web browser vulnerabilities</b></p>
<h3>Network Management Failure</h3> <p>Poor network management leads to <b>network congestion, misconnection, misconfiguration</b>, lack of resource isolation, etc., which affects services and security</p>	<h3>Authentication Attacks</h3> <p>Weak authentication mechanisms (weak passwords, re-use passwords, etc.) and inherent limitations of <b>one-factor authentication mechanisms</b> allows attacker to gain unauthorized access to cloud computing systems</p>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing  
Cloud Computing Threats

## Cloud Computing Threats (Cont'd)

CEH  
Certified Ethical Hacker

<h3>VM-Level Attacks</h3>	Cloud extensively use <b>virtualization technology</b> . This threat arises due to the <b>existence of vulnerabilities in the hypervisors</b>
<h3>Lock-in</h3>	Inability of the client to <b>migrate from one cloud service provider to another</b> or in-house systems due to the lack of tools, procedures or standards data formats for data, application, and service portability
<h3>Licensing Risks</h3>	The organization may <b>incur huge licensing fee</b> if the software deployed in the cloud is charged on a per instance basis
<h3>Loss of Governance</h3>	In using cloud infrastructures, <b>customer gives up control to the cloud service provider</b> regarding issues that may affect security
<h3>Loss of Encryption Keys</h3>	The loss of encryption keys required for <b>secure communication</b> or systems access provide a potential attacker with the possibility to get <b>unauthorized assets</b>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing		Cloud Computing Threats (Cont'd)		CEH	
<b>VM-Level Attacks</b>		Cloud extensively use <b>virtualization technology</b> . This threat arises due to the <b>existence of vulnerabilities in the hypervisors</b>			
<b>Lock-in</b>		Inability of the client to <b>migrate from one cloud service provider to another</b> or in-house systems due to the lack of tools, procedures or standards data formats for data, application, and service portability			
<b>Licensing Risks</b>		The organization may <b>incur huge licensing fee</b> if the software deployed in the cloud is charged on a per instance basis			
<b>Loss of Governance</b>		In using cloud infrastructures, <b>customer gives up control to the cloud service provider</b> regarding issues that may affect security			
<b>Loss of Encryption Keys</b>		The loss of encryption keys required for <b>secure communication</b> or systems access provide a potential attacker with the possibility to get <b>unauthorized assets</b>			

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing		Cloud Computing Threats (Cont'd)		CEH	
<b>Improper Data Handling and Disposal</b>	01	It is difficult to ascertain data handling and disposal procedures followed by CSPs due to <b>limited access to cloud infrastructure</b>			
<b>Loss/Modification of Backup Data</b>	02	Attackers might exploit vulnerabilities such as <b>SQL injection</b> , insecure user behavior like <b>storing passwords, reusing passwords</b> etc. to gain illegal access to the data backups in the cloud			
<b>Compliance Risks</b>	03	Organizations that seek to obtain compliance to standards and laws may be put at risk if the CSP <b>cannot provide evidence of their own compliance</b> with the necessary requirements, outsource cloud management to third parties and/or <b>does not permit audit</b> by the client			
<b>Economic Denial of Sustainability (EDOS)</b>	04	If an attacker engages the cloud with a malicious service or executes malicious code that <b>consumes a lot of computational power and storage from the cloud server</b> , then the legitimate account holder is charged for this kind of computation until the primary cause of CPU usage is detected			

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Cloud Computing Threats

Discussed below are some threats to cloud computing:

### ▪ Data Breach/Loss

An improperly designed cloud environment with multiple clients is at higher risk to a data breach as a flaw in one client's application could allow attackers to access other client's data. The risk of data leakage varies based on cloud architecture and operations. Data loss issues include:

- Data is erased, modified or decoupled (lost)
- Encryption keys are lost, misplaced or stolen
- Illegal access to the data due to improper authentication, authorization, and access controls
- Misuse of data by CSP

#### Countermeasures:

- Encrypt the data stored in cloud and data in transit to protect its integrity
- Implement strong key generation, storage, and management
- Check for data protection at both design and runtime

### ▪ Abuse and Nefarious Use of Cloud services

Presence of weak registration systems in the cloud-computing environment gives rise to this threat. Attackers create anonymous access to cloud services and perpetrate various attacks such as password and critical cracking, building rainbow tables, CAPTCHA-solving farms, launching dynamic attack points, hosting exploits on cloud platforms, hosting malicious data, Botnet command or control, DDoS, etc.

#### Countermeasures:

- Implement robust registration and validation process
- Monitor the client's traffic for any malicious activities

### ▪ Insecure Interfaces and APIs

Interfaces or APIs enable customers to manage and interact with cloud services. Cloud service models must be security integrated, and users must be aware of security risks in the use, implementation, and monitoring of such services. Following are some of the insecure interfaces and APIs risks:

- Circumvents user-defined policies
- Is not credential leak proof
- Breach in logging and monitoring facilities
- Unknown API dependencies
- Reusable passwords/tokens
- Insufficient input-data validation



**Countermeasures:**

- Analyze the security model of cloud provider interfaces
- Implement secure authentication and access controls
- Encrypt the data in transit and understand the dependency chain associated with the API

▪ **Insufficient Due Diligence**

Ignorance of CSP's cloud environment pose risks in operational responsibilities such as security, encryption, incident response, and more such problems as contractual issues, design, and architectural issues, etc.

**Countermeasure:**

- Organizations that intend to move to a cloud must extensively research the risks, CSP due diligence, and possess capable resources

▪ **Shared Technology Issues**

IaaS vendors share the infrastructure to deliver the services in a scalable way. Most underlying components that make up this infrastructure (e.g., GPU, CPU caches) do not offer substantial isolation properties in a multi-tenant environment, which enables attackers to attack other machines if they can exploit vulnerabilities in one client's applications. To address this gap, virtualization hypervisors mediate access between guest OSs and the physical resources that might contain loopholes that allow hackers to gain unauthorized control over the underlying platforms. Issues include Rutkowska's Red and Blue Pill exploits and Kortchinsky's CloudBurst presentations.

**Countermeasures:**

- Implement security best practices for installation/configuration
- Monitor environment for unauthorized changes/activity
- Promote secure authentication and access control for administrative access and operations
- Enforce service level agreements for patching and vulnerability remediation
- Conduct vulnerability scanning and configuration audits

▪ **Unknown Risk Profile**

Software updates, threat analysis, intrusion detection, security practices, and various other components determine security posture of an organization. Client organizations are unable to get a clear picture of internal security procedures, security compliance, configuration hardening, patching, auditing, and logging, etc. as they are less involved with hardware and software ownership and maintenance in the cloud. However, organizations must be aware of issues such as internal security procedures, security compliance, configuration hardening, patching, and auditing and logging.

**Countermeasures:**

- Disclosure of applicable logs and data to customers
- Partial/full disclosure of infrastructure details (e.g., patch levels, firewalls)
- Monitoring and alerting on necessary information

▪ **Unsynchronized System Clocks**

This threat arises due to the failure of synchronizing clocks at the end systems. Unsynchronized clocks can affect the working of automated tasks. For example, if the cloud computing devices do not have synchronized time, then due to the inaccuracy of the time stamps the network administrator would be unable to analyze the log files for any malicious activity accurately. Unsynchronized clocks can cause various other problems, for example, in case of money transactions or database backups, the mismatched timestamp may result in creating a significant problem or discrepancies.

**Countermeasures:**

- Use clock synchronization solution such as NTP (Network Time Protocol)
- Install a time server within an organization's firewall which results in minimizing the threats from the outside and maximizing the time accuracy on the network
- Network Time System can also be used to synchronize clocks with an enterprise network server

▪ **Inadequate Infrastructure Design and Planning**

An agreement between the Cloud Service Provider (CSP) and customer states the quality of service that the CSP offers such as downtime, physical and network-based redundancies, standard data backup, and restore processes, and availability periods.

At times, cloud service providers may not satisfy the rapid rise in demand due to a shortage of computing resources and/or poor network design (e.g., traffic flows through a single point, even though the necessary hardware is available) giving rise to unacceptable network latency or inability to meet agreed service levels.

**Countermeasure:**

- Forecast the demand and accordingly be prepared with the sufficient infrastructure

▪ **Conflicts between Client Hardening Procedures and Cloud Environment**

Certain client hardening procedures may conflict with a cloud provider's environment, making their implementation impossible by the client. The reason for this is that, because a cloud is a multi-tenant environment, the colocation of many customers indeed causes conflict for the cloud providers, as customers' communication security requirements are likely to diverge from one another.

**Countermeasure:**

- Set clear segregation of responsibilities that expresses the minimum actions customers must undertake



▪ **Loss of Operational and Security Logs**

The loss of operational logs makes it challenging to evaluate operational variables. The options for solving issues are limited when no data is available for analysis. The loss of security logs poses a risk for managing the implementation of the information security management program. Loss of security logs may occur in case of under-provisioning of storage.

**Countermeasures:**

- Implement effective policies and procedures
- Monitor operational and security logs on the regular basis

▪ **Malicious Insiders**

Malicious insiders are disgruntled current/former employees, contractors, or other business partners who have/had authorized access to cloud resources and could intentionally exceed or misuse that access to compromise the confidentiality, integrity, or availability of the organization's information. Malicious insiders who have authorized access to cloud resources can abuse their access to compromise the information available in the cloud. Threats include loss of reputation, productivity, and financial theft.

**Countermeasures:**

- Enforce strict supply chain management and conduct a comprehensive supplier assessment
- Specify human resource requirements as part of legal contracts
- Require transparency in overall information security and management practices, as well as compliance reporting
- Determine security breach notification processes

▪ **Illegal Access to the Cloud**

Weak authentication and authorization controls could lead to unlawful access thereby compromising confidential and critical data stored in the cloud.

**Countermeasures:**

- Enforce robust Information Security (IS) Policy and adhere to it
- Clients should be permitted to audit/review cloud providers IS policy and procedures

▪ **Loss of Business Reputation due to Co-tenant Activities**

This threat arises because of lack of resource isolation, lack of reputational isolation, vulnerabilities in the hypervisors, and others. Resources are shared in the cloud, thus the malicious activity of one co-tenant might affect the reputation of the other, resulting in poor service delivery, data loss, etc. that bring down organization's reputation.

**Countermeasure:**

- Choose a well-known and efficient cloud service provider to reduce the risk, and ensure isolation of resources

▪ **Privilege Escalation**

A mistake in the access allocation system such as coding errors, design flaws, and others can result in a customer, third party, or employee obtaining more access rights than required. This threat arises because of AAA (authentication, authorization, and accountability) vulnerabilities, user-provisioning and de-provisioning vulnerabilities, hypervisor vulnerabilities, unclear roles and responsibilities, misconfiguration, and others.

**Countermeasures:**

- Employ a good privilege separation scheme
- Update software programs on regular basis to fix the newly discovered privilege escalation vulnerabilities, if any

▪ **Natural Disasters**

Based on geographic location and climate, data centers may be exposed to natural disasters such as floods, lightning, earthquakes, etc. that can affect the cloud services

**Countermeasures:**

- Ensure that the organization is located in safe area
- Maintain data backups at different locations
- Implement mitigation measures that help reduce or eliminate your long-term risk from natural disasters
- Prepare an effective business continuity and disaster recovery plan

▪ **Hardware Failure**

Hardware failure such as switches, servers, routers, access points, hard disks, network cards, and processors in data centers can make cloud data inaccessible. The majority of hardware failures happen because of hard disk problems. Hard disk failures take a lot of time to track and fix because of their low-level complexities. Hardware failure can lead to the poor performance delivery to end users and can damage the business.

**Countermeasures:**

- Implement and maintain physical security programs
- Pre-installed standby hardware devices are a must

▪ **Supply Chain Failure**

This threat arises because of incomplete and non-transparent terms of use, hidden dependency created by cross-cloud applications, inappropriate CSP selection, lack of supplier redundancy, and others. Cloud providers outsource certain tasks to third



parties. Thus, the security of the cloud is directly proportional to the security of each link and the extent of dependency on third parties. A disruption in the chain may lead to loss of data privacy and integrity, services unavailability, violation of SLA, economic and reputational losses failing to meet customer demand, and cascading failure.

**Countermeasures:**

- Define a set of controls to mitigate supply-chain risks
- Develop a containment plan to restrict the damage caused by a counterparty that is trusted to fail
- Create visibility mechanisms to find when elements of a supply chain are compromised
- Consider procuring third parties which offer information on the security posture of counterparties

▪ **Modifying Network Traffic**

In the cloud, the network traffic may be altered due to flaws during provisioning or de-provisioning network, or vulnerabilities in communication encryption. Modification of network traffic may cause loss, alteration, or theft of confidential data and communications. This threat arises because of user-provisioning and de-provisioning vulnerabilities, communication encryption vulnerabilities, and so on.

**Countermeasure:**

- Perform network traffic analysis using tools to find abnormalities, if any

▪ **Isolation Failure**

Multi-tenancy and shared resources are the characteristics of cloud computing. Strong isolation or compartmentalization of storage, memory, routing, and reputation among different tenants is lacking. Because of isolation failure, attackers try to control operations of other cloud customers to gain illegal access to the data.

**Countermeasure:**

- It is essential to keep memory, storage, and network access isolated

▪ **Cloud Provider Acquisition**

Acquisition of the cloud provider may increase the probability of tactical shift and may affect non-binding agreements at risk. This could make it difficult to cope up with the security requirements.

**Countermeasure:**

- Be tactful while choosing a cloud provider; prefer a reputed and popular cloud service provider to avoid the risk

▪ **Management Interface Compromise**

Customer management interfaces of cloud provider are accessible via the Internet and facilitate access to a large number of resources. This enhances the risk, particularly when combined with remote access and web browser vulnerabilities. This threat arises due to the improper configuration, system and application vulnerabilities, remote access to the management interface, and so on.

**Countermeasure:**

- It is essential to keep memory, storage, and network access isolated
- Use secure protocol to provide access to mitigate threats arising because of remote access
- Regularly update the patches for web browser vulnerabilities

▪ **Network Management Failure**

Poor network management leads to network congestion, misconnection, misconfiguration, lack of resource isolation, etc., which affects services and security.

**Countermeasure:**

- Ensure that an adequate security policy is implemented
- Use proactive network management techniques
- Keep updating new technologies and analyze what might work better for your organization

▪ **Authentication Attacks**

Weak authentication mechanisms (weak passwords, re-use passwords, etc.) and inherent limitations of one-factor authentication mechanisms allow attacker to gain unauthorized access to cloud computing systems.

**Countermeasure:**

- Implement strong password policies and keep the passwords secure
- Enforce two-factor authentication where required

▪ **VM-Level Attacks**

Cloud computing extensively uses virtualization technologies offered by several vendors including VMware, Xen, Virtual box, and vSphere. Threats to these technologies arise because of vulnerabilities in the hypervisors.

**Countermeasure:**

- Employ IDS/IPS and implement firewall to mitigate known VM-level attacks

▪ **Lock-in**

The inability of the client to migrate from one cloud service provider to another or in-house systems due to the lack of tools, procedures or standards data formats for data, application, and service portability. This threat is due to the inappropriate selection of

CSP, incomplete and non-transparent terms of use, lack of standard mechanisms, and so on.

**Countermeasure:**

- Using standardized cloud API cloud be beneficial

▪ **Licensing Risks**

The organization may incur substantial licensing fee if the CSP charges the software deployed in the cloud on a per-instance basis. Therefore, the organization should always retain ownership over its software assets located in the cloud provider environment. Risks to licensing occur because of incomplete and non-transparent terms of use.

▪ **Loss of Governance**

In using cloud infrastructures, customers give up control to cloud service providers regarding issues that could affect security. Also, SLAs may not offer a commitment on the part of the cloud provider to provide such services, thus leaving a gap in security defenses. This threat results from unclearness of roles and responsibilities, lack of vulnerability assessment process, conflicting promises in SLAs, no certification schemes, lack of jurisdiction, unavailability of the audit, and others.

Loss of governance results in noncompliance with security requirements, lack of confidentiality, integrity, and availability of data, poor performance and quality of service, and so on.

**Countermeasure:**

- Workout persistent and careful efforts for execution of service-level agreements (SLA)

▪ **Loss of Encryption Keys**

The loss of encryption keys required for secure communication or systems access provides a potential attacker with the possibility to get unauthorized assets. This threat arises due to the poor management of keys and poor key generation techniques.

**Countermeasures:**

- Do not store the encryption keys alongside the encrypted data
- Use strong algorithms such as AES and RSA to generate keys

▪ **Risks from Changes of Jurisdiction**

Clouds may store the customer data in multiple jurisdictions, of which some may be high risk. Local authorities in high-risk countries (e.g., those without the rule of law, with an unpredictable legal framework and enforcement, with autocratic police states) could raid data centers; the data or information system could subject to enforced disclosure or seizure. Change in jurisdiction of the data leads to the risk, the data or information system is blocked or impounded by the government or other organization. Customers



should consider jurisdictional ambiguities before adopting a cloud, as local laws of a particular country for data storage could provide government access to private data.

**Countermeasure:**

- Gain insight about the jurisdictions in which data may be stored and processed, and assess the risks, if any, in those jurisdictions

▪ **Undertaking Malicious Probes or Scans**

Malicious probes or scanning allows an attacker to collect sensitive information that may lead to loss of confidentiality, integrity, and availability of services and data.

**Countermeasure:**

- Deploy various security mechanisms such as firewalls, intrusion detection systems, and others

▪ **Theft of Computer Equipment**

Theft of equipment may occur due to inadequate controls on physical parameters such as smart card access at the entry etc. which may lead to loss of physical equipment and sensitive data.

**Countermeasure:**

- Enforce physical security measures such as hiring security guards, CCTV coverage, alarms, identity cards, and proper fencing

▪ **Cloud Service Termination or Failure**

Termination of cloud service because of non-profitability or disputes might lead to data loss unless end-users protect themselves legally. Many factors, such as competitive pressure, lack of financial support, and inadequate business strategy, could lead to termination or failure of the cloud service.

This threat results in poor service delivery, loss of investment, and quality of service. Furthermore, failures in the services outsourced to the CSP may affect cloud customers' ability to meet its duties and commitments to its customers.

**Countermeasure:**

- Ensure that the cloud providers define clear and auditable procedures for termination of the service. This service includes how the cloud provider will transfer data back to the customer and guarantee that all data is disposed of securely, according to the terms of agreement

▪ **Subpoena and E-Discovery**

Customer data and services are subjected to a cease request from authorities or third parties. This threat occurs due to the improper resource isolation, data storage in multiple jurisdictions, and lack of insight on jurisdictions.



**Countermeasures:**

- Carefully select the cloud service provider and ensure proper security is provided
- Thoroughly review the service agreement. It should address records management, accessibility, customer support, legal policies, accountability, confidentiality, length of agreement, termination, and others
- Execute a coordinated eDiscovery plan
- Contemplate an exit strategy

▪ **Improper Data Handling and Disposal**

It is difficult to ascertain data handling and disposal procedures followed by CSPs due to limited access to cloud infrastructure. When clients request data deletion, data may not be truly wiped since:

- Multiple copies of data are stored but not available
- The disk to be destroyed might also contain the data of other clients
- Multi-tenancy and reuse of hardware resources in cloud keeps clients' data at risk

**Countermeasure:**

- Use VPNs to secure the client's data and ensure that data is completely removed from the primary servers along with its replicas

▪ **Loss/Modification of Backup Data**

Attackers might exploit vulnerabilities such as SQL injection and insecure user behavior (e.g., storing or reusing passwords) to gain illegal access to the data backups in the cloud. After gaining access, attackers might delete or modify the data stored in the databases. Lack of data restoration procedures in case of backup data loss keeps the service levels at risk.

**Countermeasure:**

- Use appropriate data restoration procedures or tools to retrieve lost data

▪ **Compliance Risks**

Organizations that seek to obtain compliance to standards and laws may be at the risk if CSP cannot provide evidence of their compliance with the requirements, outsource cloud management to third parties and/or does not permit audit by the client. This threat is due to the lack of governance over audits and industry standard assessments. Thus, clients are not aware of the processes, procedures, and practices of providers in the areas of access, identity management, and segregation of duties.

**Countermeasures:**

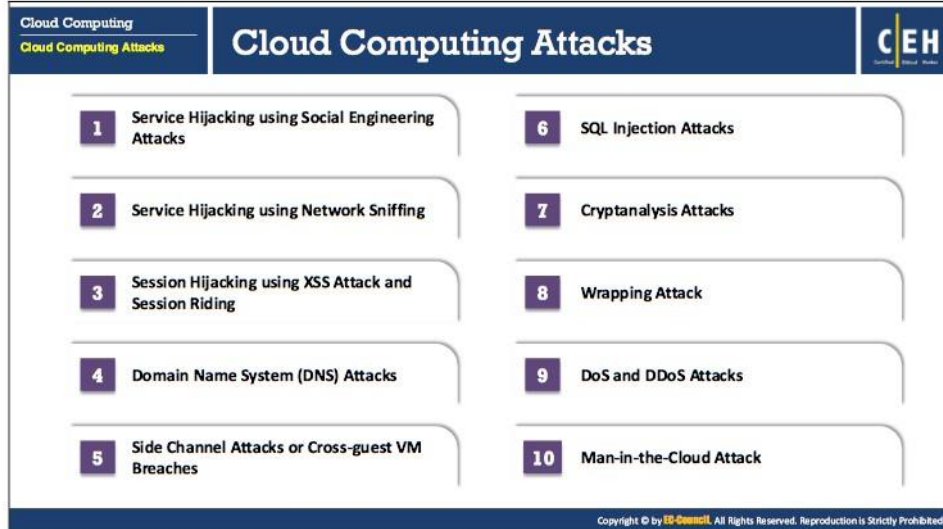
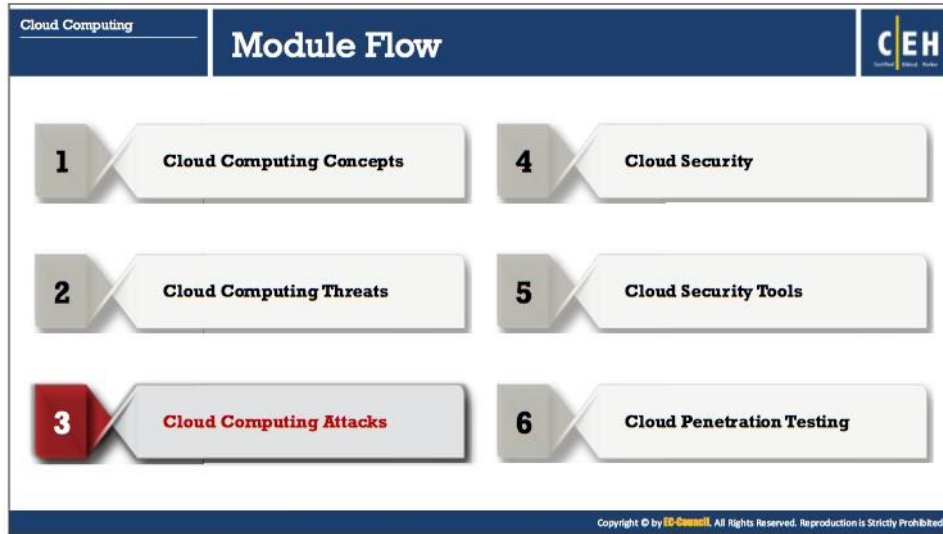
- Cloud providers should ensure that clients' data is not compromised
- Review cloud providers' internal audit processes

- **Economic Denial of Sustainability (EDoS)**

The payment method in a cloud system is “**No use, no bill**”: the CSP charges the customer according to the recorded data involved when customers make requests, the duration of requests, the amount of data transfer in the network, and the number of CPU cycles consumed. Economic denial of service destroys financial resources; in the worst case, this could lead to customer bankruptcy or another serious economic impact. If an attacker engages the cloud with a malicious service or executes malicious code that consumes a lot of computational power and storage from the cloud server, then the legitimate account holder is charged for this kind of computation until the primary cause of CPU usage is detected.

**Countermeasure:**

- Use a reactive/on-demand, in-cloud eDDoS mitigation service (scrubber Service) to mitigate application- and network-layer DDoS attacks, making use of the client-puzzle approach



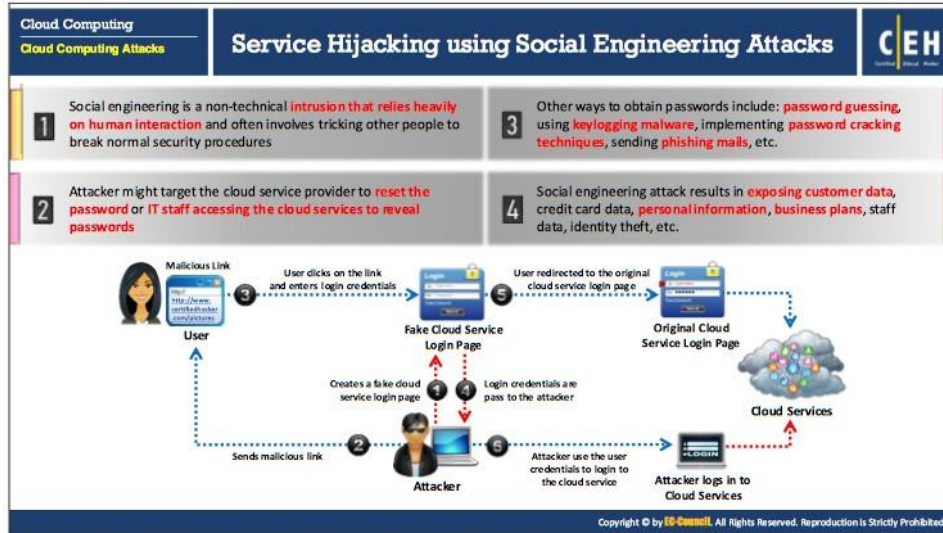
## Cloud Computing Attacks

Though most organizations adopt cloud technologies, as they offer a wide variety of services with cost reduction, security is the most significant concern, as it depends on sharing. Security gaps and vulnerabilities of the underlying technologies can allow attackers to launch various types of cloud attacks, affecting confidentiality, integrity, and availability of resources and services in cloud systems. This section discusses different types of attacks on cloud systems.

This section discusses following cloud computing attacks:

- Service hijacking using social engineering attacks
- Service hijacking using network sniffing
- Session hijacking using XSS attack
- Session hijacking using session riding
- Domain Name System (DNS) attacks
- Side channel attacks or cross-guest VM breaches
- SQL injection attacks
- Cryptanalysis attacks
- Wrapping attack
- DoS and DDoS attacks
- Man-in-the-Cloud attack





### Service Hijacking using Social Engineering Attacks

In account or service hijacking, an attacker steals a CSP's or client's credentials by methods such as phishing, pharming, social engineering, and exploitation of software vulnerabilities. Using the stolen credentials, the attacker gains access to the cloud computing services and compromises data confidentiality, integrity, and availability.

Social engineering is a nontechnical kind of intrusion that relies heavily on human interaction and often involves tricking others to break routine security procedures. Attackers might target cloud service providers to reset passwords, or IT staff to access their cloud services to reveal passwords. Other ways to obtain passwords include password guessing, keylogging malware, implementing password-cracking techniques, sending phishing emails, and others. Social engineering attacks result in exposed customer data, credit-card data, personal information, business plans, staff data, identity theft, etc.

In the diagram above, the attacker first creates a fake cloud service login page and sends a malicious link to the cloud service user. The user on receiving the link, clicks on it and enters login credentials failing to notice it as a fake login page. When the user hits enter, the attacker receives login credentials of the user, and the page automatically redirects to the original cloud service login page. Now, the attacker uses the stolen user credentials to log in to the cloud service to perform various malicious activities.

#### Countermeasures:

- Protect the credentials from being stolen
- Do not share account credentials between users and services
- Implement robust two-factor authentication mechanism wherever possible
- Train the staff to recognize social engineering attacks

- Strictly follow the security policies framed
- Use “least privilege” principles to restrict access to services
- Divide responsibilities among cloud service provider’s administrators and your administrators, this restricts free access to all security layers for others

Cloud Computing  
Cloud Computing Attacks

## Service Hijacking using Network Sniffing

CEH

Network sniffing involves **interception and monitoring of network traffic** which is being sent between the two cloud nodes

Attacker uses packet sniffers to capture sensitive data such as **passwords, session cookies**, and other web service related security configuration such as the **UDDI** (Universal Description Discovery and Integrity), **SOAP** (Simple Object Access Protocol) and **WSDL** (Web Service Description Language) files

The diagram illustrates the process of service hijacking. On the left, two 'User' icons are connected to a 'Switch'. The switch is connected to a 'NIC Card in Promiscuous Mode', which is connected to a 'Sniffer'. The sniffer is connected to an 'Attacker' icon. A dashed arrow points from the sniffer to the attacker, labeled 'Attacker sniffs the login credentials/cookies'. The attacker is then connected to a 'Cloud Server' icon. A dashed arrow points from the attacker to the cloud server, labeled 'Attacker logs into Cloud Services'.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Service Hijacking using Network Sniffing

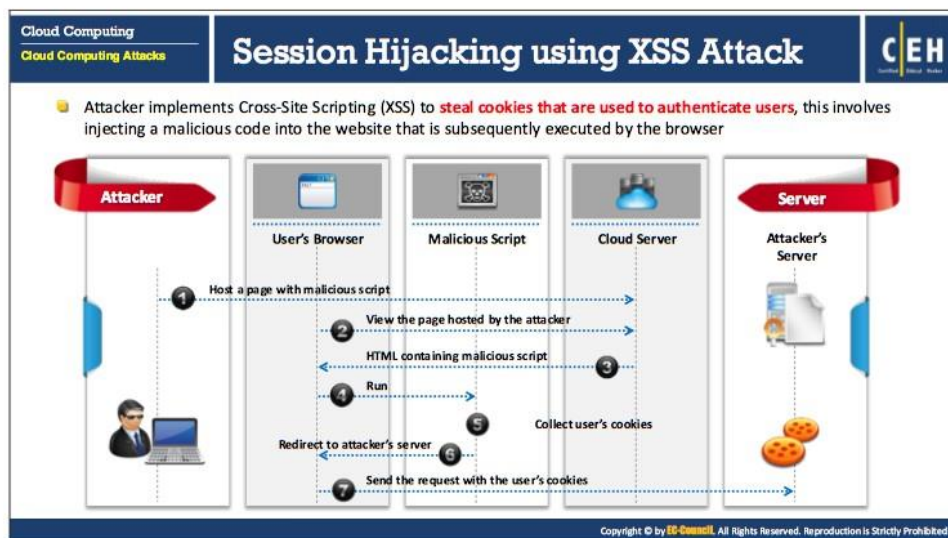
Network sniffing involves interception and monitoring of network traffic sent between two cloud nodes. Unencrypted sensitive data (such as login credentials) during transmission across a network is at higher risk.

Attacker uses packet sniffers (e.g., Wireshark, Cain, and Abel) to capture sensitive data such as passwords, session cookies, and other web service–related security configuration such as the UDDI (Universal Description Discovery and Integrity), SOAP (Simple Object Access Protocol), and WSDL (Web Service Description Language) files.

In the diagram above, when the user enters login credentials to access cloud services. The attacker sniffs these login credentials/cookies during their transmission across a network using packet sniffers such as **Wireshark, Capsa Network Analyzer**, etc. The attacker then logs into cloud services via stolen credentials.

#### Countermeasures:

- Encrypt sensitive data over the network
- Encrypt sensitive data in configuration files
- Detect NICs running in promiscuous mode



### Session Hijacking using cross-site scripting (XSS) Attack

An attacker implements cross-site scripting (XSS) to steal cookies used in user authentication process; this involves injecting malicious code into the website that is subsequently executed by the browser. Using the stolen cookies attacker exploits active computer sessions, thereby gaining unauthorized access to the data.

**Note:** Attacker can also predict or sniff session IDs.

In the diagram above, attacker hosts a web page with the malicious script on to the cloud server. When the user views the page hosted by the attacker, the HTML containing malicious script runs on the user's browser. The malicious script will collect user's cookies and redirects the user to the attacker's server; it also sends the request with the user's cookies.


#### Countermeasures:

- Using Secure Socket Layer (SSL), firewalls, antivirus, and code scanner might safeguard a cloud from session hijacking

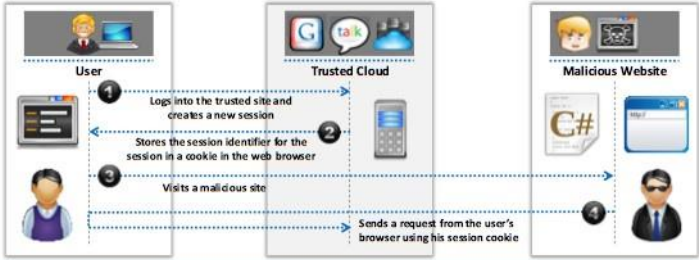


**Cloud Computing**  
**Cloud Computing Attacks**

## Session Hijacking using Session Riding



- Attacker exploits website by implementing **cross-site request forgery** to transmit unauthorized commands
- In session riding, attacker rides an active computer session by **sending an email** or **tricking the user to visit a malicious webpage** while they are logged into the targeted site
- When the **user clicks the malicious link**, the website executes the request as the user is already authenticated
- **Commands used include:** Modify or delete user data, execute online transactions, reset passwords, etc.



The diagram illustrates the process of session hijacking using session riding. It shows three main components: a User, a Trusted Cloud, and a Malicious Website. 1. The User logs into the Trusted Cloud and creates a new session. 2. The Trusted Cloud stores the session identifier for the session in a cookie in the user's web browser. 3. The User visits a malicious site. 4. The Malicious Website sends a request from the user's browser using the stolen session cookie to the Trusted Cloud.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

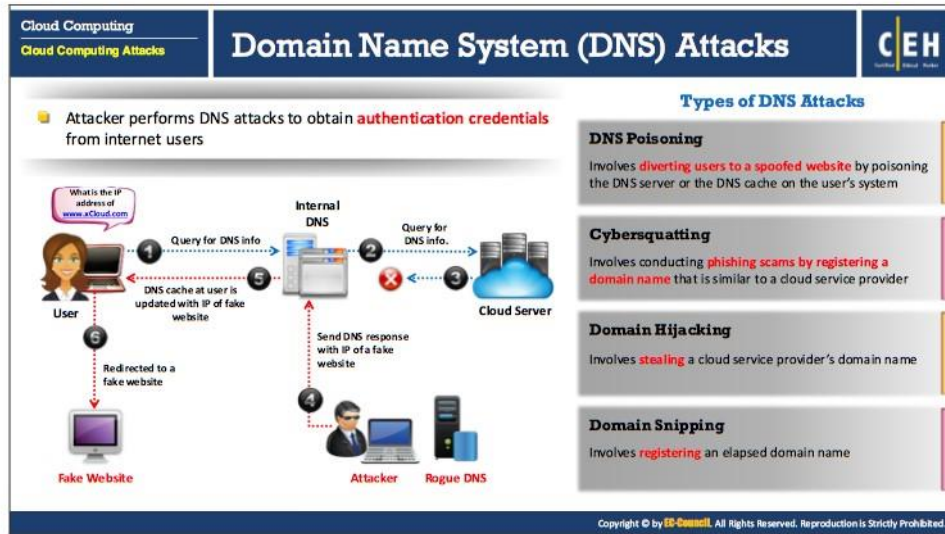
### Session Hijacking using Session Riding

Attackers exploit websites by engaging in cross-site request forgeries to transmit unauthorized commands. In session riding, attackers “ride” an active computer session by sending an email or tricking users to visit a malicious webpage, during login, to an actual target site. When users click the malicious link, the website executes the request as if the user had already authenticated it. Commands used include modifying or deleting user data, performing online transactions, resetting passwords, and others.

In the diagram above, the user logs into the trusted site and creates a new session. The server stores the session identifier for the session in a cookie in the web browser. Attacker lures the victim to visit a malicious website set up by him/her. The attacker then sends a request to the cloud server from the user’s browser using a stolen session cookie.

#### Countermeasures:

- Do not allow your browser and websites to save login details
- Check the HTTP Referrer header and when processing a POST, ignore URL parameters



### Domain Name System (DNS) Attacks

A domain name system (DNS) server translates a human-readable domain name (e.g., www.google.com) into a numerical IP address that routes communications between nodes. The attacker performs DNS attacks to obtain authentication credentials from Internet users.

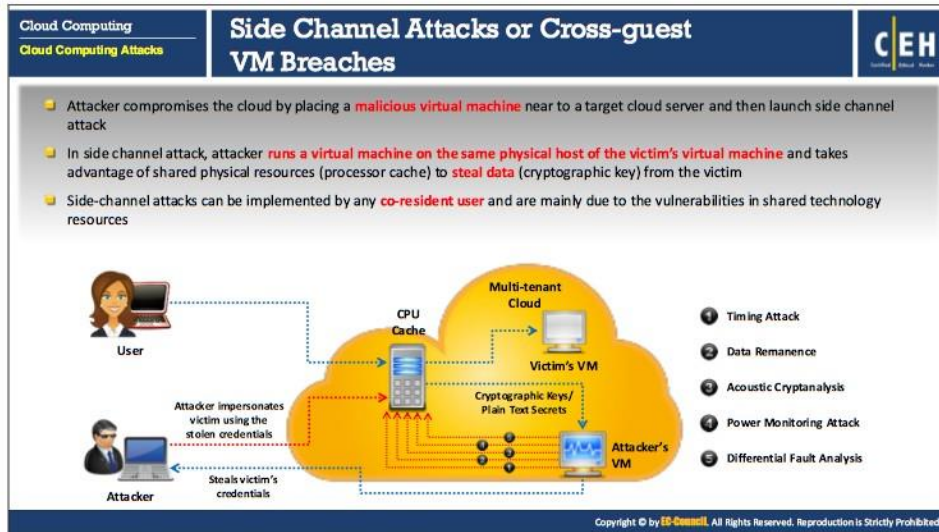
#### Types of DNS Attacks:

- **DNS Poisoning:** Involves diverting users to a spoofed website by poisoning the DNS server or the DNS cache on the user's system.
- **Cybersquatting:** Involves conducting phishing scams by registering a domain name that is similar to a cloud service provider.
- **Domain Hijacking:** Involves stealing a cloud service provider's domain name.
- **Domain Snipping:** Involves registering an elapsed domain name.

In the diagram above, the attacker performs DNS cache poisoning, directing users to a fake website. Here, the user queries the internal DNS server for DNS information (e.g., what is the IP address of www.xCloud.com?). The internal DNS server then asks the respective cloud server for DNS information. At this point, attacker blocks the DNS response from the cloud server and sends DNS response with IP of a fake website to the internal DNS server. Thus, the internal DNS server cache updates itself with the IP of counterfeit websites and automatically directs the user to that website.

#### Countermeasures:

- Using Domain Name System Security Extensions (DNSSEC) reduces the effects of DNS threats to some extent



### Side Channel Attacks or Cross-guest VM Breaches

Attacker compromises the cloud by placing a malicious virtual machine near a target cloud server and then launch side channel attack. Inside channel attack, the attacker runs a virtual machine on the same physical host of the victim's virtual machine and takes advantage of shared physical resources (processor cache) to steal data (cryptographic key) from the victim. Side-channel attacks can be implemented by any co-resident user and are mainly due to the vulnerabilities in shared technology resources.

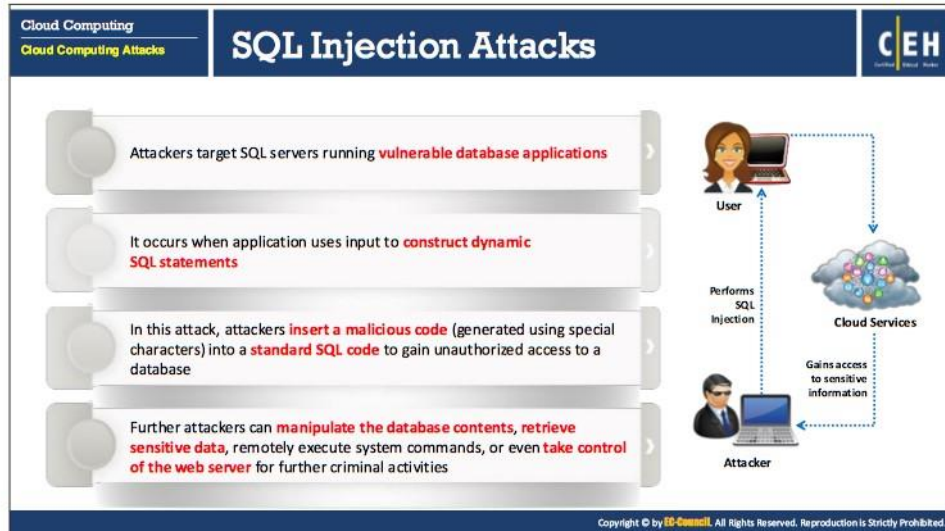
In the diagram above, an attacker compromises the cloud by placing malicious virtual machine (VM) near a target cloud server. Attacker runs the VM on the same physical host of the victim's VM and takes advantage of shared physical resources (processor cache), launches side-channel attacks (timing attack, data remanence, acoustic cryptanalysis, power monitoring attack, and differential fault analysis) to extract cryptographic keys/plain text secrets to steal the victim's credentials. The attacker then uses the stolen credentials to impersonate the victim.

### Side Channel Attack Countermeasures

- Implement virtual firewall in the cloud server back end of the cloud computing; this prevents attacker from placing malicious VM
- Implement random encryption and decryption (encrypts data using RSA, 3DES, AES algorithms)
- Lockdown OS images and application instances to prevent compromising vectors that might provide access
- Check for repeated access attempts to local memory and access from the system to any hypervisor processes or shared hardware cache by tuning and collecting local process monitoring data and logs for cloud systems



- Code the applications and OS components in a way that they access shared resources like memory cache in a consistent and predictable way. This coding prevents attackers from collecting sensitive information such as timing statistics and other behavioral attributes



### Structured Query Language (SQL) Injection Attacks

Structured Query Language (SQL) is a programming language meant for database management systems. In SQL injection attack, attackers target SQL servers running vulnerable database applications. Attackers insert malicious code (generated using special characters) into a standard SQL code to gain unauthorized access to a database and ultimately to other confidential information. It generally occurs when an application uses the input to construct dynamic SQL statements. Further attackers can manipulate the database contents, retrieve sensitive data, remotely execute system commands, or even take control of the web server for additional criminal activities.

In the diagram above, the attacker performs SQL injection on the cloud web application accessed by the user and gains access to the sensitive information hosted on the cloud.

#### Countermeasures:

- Use filtering techniques to sanitize the user input
- Validate input length, range, format, and type
- Regularly update and patch servers and applications
- Use database monitoring technologies and Intrusion Prevention Systems (IPSs)
- Implement a cloud-based web application firewall

Cloud Computing  
Cloud Computing Attacks

## Cryptanalysis Attacks

CEH

- **Insecure or obsolete encryption** makes cloud services susceptible to cryptanalysis
- Data present in the cloud may be encrypted to prevent it from being read if accessed by malicious users. However **critical flaws in cryptographic algorithm** implementations (e.g.: weak random number generation) might turn strong encryption to weak or broken, also there exist novel methods to break the cryptography
- Partial information can also be obtained from encrypted data by monitoring **clients' query access patterns** and **analyzing accessed positions**

The diagram shows a User on the left and a Cloud Server on the right. A dashed arrow labeled 'Encrypted Credentials' points from the User to the Cloud Server. A dashed arrow labeled 'Access to Encrypted Information' points from the Cloud Server back to the User. An Attacker is positioned in the middle, with a dashed arrow labeled 'Attacker sniffs the traffic' pointing from the communication line to the Attacker. From the Attacker, a dashed arrow labeled 'Performs Cryptanalysis on Encrypted Data' points to a document icon labeled 'Plain text information extracted by the attacker'. At the bottom right of the diagram area, there is a small copyright notice: 'Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.'

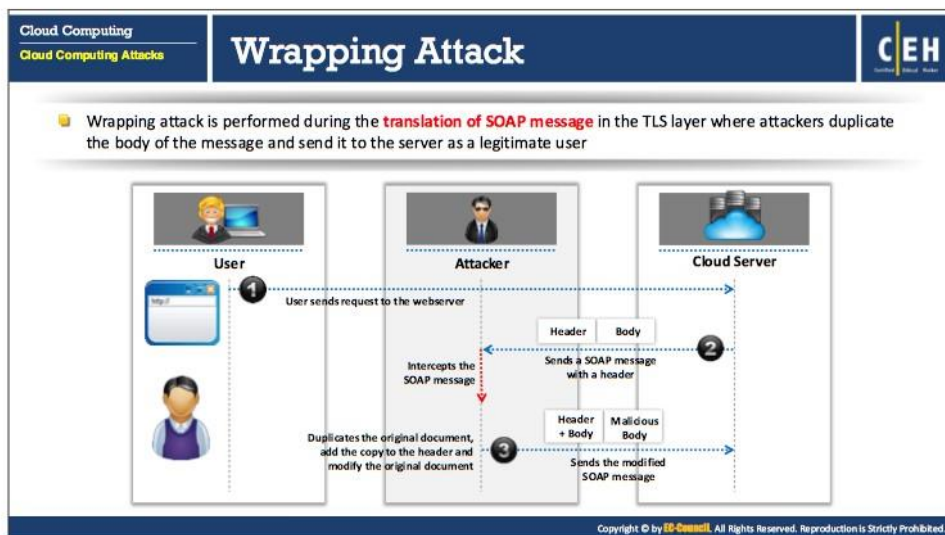
### Cryptanalysis Attacks

Insecure or obsolete encryption makes cloud services susceptible to cryptanalysis. Data present in the cloud may be encrypted for the prevention from being read if accessed by malicious users. However, critical flaws in cryptographic algorithm implementations (e.g.: weak random number generation) might turn strong encryption to weak or broken, also there exist novel methods to break the cryptography. Partial information can also be obtained from encrypted data by monitoring clients' query access patterns and analyzing accessed positions.

#### Cryptanalysis Attack Countermeasures:

- Use Random Number Generators that generate cryptographically secure random numbers to provide robustness to cryptographic material like Secure Shell (SSH) keys and Domain Name System Security Extensions (DNSSEC)
- Do not use faulty cryptographic algorithms





### Wrapping Attack

Wrapping attack is performed during the translation of SOAP message in the TLS layer where attackers duplicate the body of the message and send it to the server as a legitimate user. When users send a request from their VM through a browser, the request first reaches to a web server, which generates a SOAP message containing structural information, which it will exchange with the browser during passing the message. Before message passing occurs, the browser needs to sign the XML document and canonicalize it. Also, it should append the signature values to the document. Finally, the SOAP header should contain all the necessary information for the destination after computation.

For a wrapping attack, the adversary does its deception during the translation of the SOAP message in the TLS (transport layer service) layer. The attacker duplicates the body of the message and sends it to the server as a legitimate user. The server checks the authentication by the Signature Value (which is also duplicated) and verifies its integrity. As a result, the adversary can intrude in the cloud and can run malicious code to interrupt the usual functioning of the cloud servers.


In the diagram above, the user sends a request to the cloud web server. The cloud server sends a SOAP message with a header. The attacker intercepts the SOAP message, then duplicates the original message, adds the copy to the header, and modifies the original document. The attacker then sends the modified SOAP message to the cloud server.

#### Countermeasures:


- XML Schema validation helps to detect SOAP message
- Apply authenticated encryption in the XML Encryption specification

**Cloud Computing**  
**Cloud Computing Attacks**

## Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks



- Performing DoS attack on cloud service providers may **leave tenants without access** to their accounts
- DoS can be performed by:
  - **Flooding the server** with multiple requests to consume all the system resources available
  - **Passing malicious input** to the server that crashes an application process
  - **Entering wrong passwords** continuously so that user account is locked
- If a DoS attack is performed by using a **botnet** (a network of compromised machines) then it is referred to as DDoS attack



The diagram illustrates a DDoS attack process. On the left, an **Attacker** sets a **Handler** system. The handler infects a large number of computers over the Internet, creating a **Zombie Net**. This zombie net then sends **Attack traffic** through the **Internet** to **Cloud Services**. Simultaneously, **Legitimate traffic** from a **Cloud User** is sent through the Internet to the Cloud Services. However, the attack traffic floods the server, causing the legitimate request to fail.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks

Performing Denial of Service (DoS) attacks on cloud service providers could leave tenants without access to their accounts. In the cloud infrastructure, multi-tenants share CPU, memory, disk space, bandwidth, and so on. Thus, if attackers gain access to the cloud, they generate false data that could be resource requests or a type of code that can run in applications of legitimate users.

Computing such malware requests engage a server's CPU, memory, and all other devices. Once the server reaches its threshold limit, it starts offloading its jobs to another nearest specific server. The same happens to other inline servers, and finally, the attacker will succeed in engaging the whole cloud system just by interfering the usual processing of one server. This makes legitimate users of the cloud unable to access its services.

DoS can be performed by flooding the server with multiple requests to consume all the system resources available, passing malicious input to the server that crashes an application process, entering wrong passwords continuously so that user account is locked, etc.

If the attacker performs a DoS attack by using a **botnet** (a network of compromised machines), then it is a **distributed DoS** (DDoS) attack. A DDoS attack involves a multitude of compromised systems attacking a single target, thereby causing a denial of service for users of the targeted system.

In the diagram above, the attacker sets a handler that infects a large number of computers over the Internet (zombie net). Then attacker floods the cloud server with multiple requests, thus resulting in the consumption of excess resources thereby making legitimate users unable to access the cloud services.


**Countermeasures:**

- Follow least privilege concept for the users connecting to the server
- Install IDS in physical as well as virtual machines of cloud to mitigate DoS and DDoS attacks

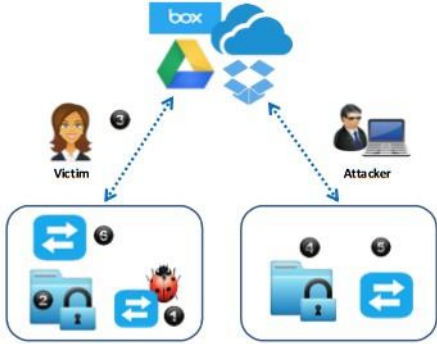


**Cloud Computing**  
**Cloud Computing Attacks**

## Man-in-the-Cloud Attack



- Man-in-the-Cloud (MITC) attacks are an advanced version of Man-in-the-middle (MITM) attacks
- In the MITM attacks, an **attacker uses an exploit** that intercepts and manipulates the communication between two parties while the MITC attacks are carried out by **abusing cloud file synchronization services** such as Google Drive or Drop Box for **Data compromise, command and control (C&C), data exfiltration, and remote access**
- The attacker tricks the victim to **install a malicious code** which plants attacker's **synchronization token** on the victim's drive
- Then, the attacker steals the victim's synchronization token and uses the stolen token to **gain access** of victim's files
- Later, attacker **restores the malicious token** with the original synchronized token of the victim, returning the drive application to its **original state** and stays undetected



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Man-in-the-Cloud (MITC) Attack

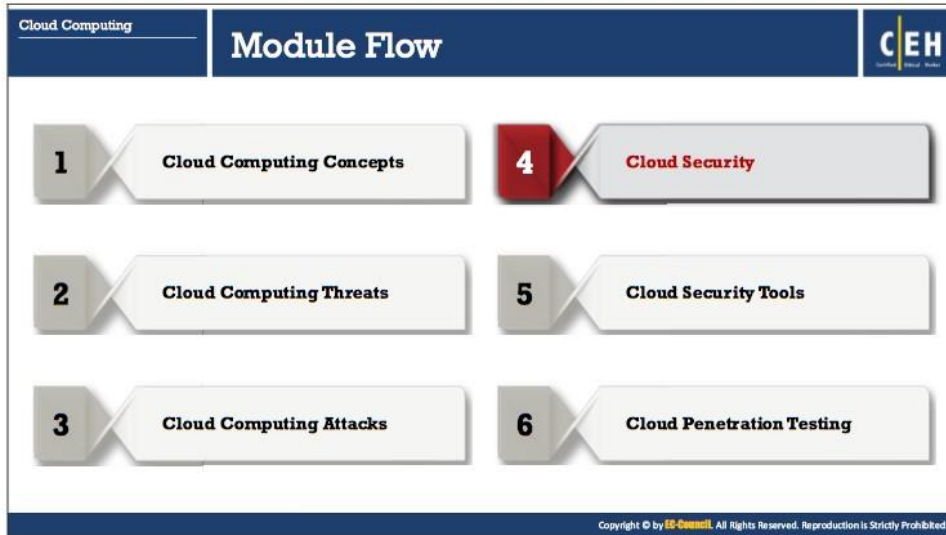
Man-in-the-Cloud (MITC) attacks are an advanced version of Man-in-the-Middle (MITM) attacks. In the MITM attacks, an attacker uses an exploit that intercepts and manipulates the communication between two parties while the MITC attacks are carried out by abusing cloud files synchronization services such as Google Drive or DropBox for Data compromise, command and control (C&C), data exfiltration, and remote access. Synchronization tokens are used for application authentication on cloud, and they cannot identify the malicious traffic from the normal traffic. The attacker abuses this weakness in cloud accounts to perform MITC attacks.

In the diagram shown above, the attacker tricks the victim to install a malicious code which plants attacker's synchronization token on the victim's drive. Then, the attacker steals the victim's synchronization token and uses the stolen synchronization token to gain access to victim's files. Later, attacker restores the malicious token with the original synchronized token of the victim, returning the drive application to its original state and stays undetected.

#### Countermeasures:

- Use an email security gateway to detect the social engineering attacks that can lead to MITC
- Hardening the policies of token expiration can prevent this kind of attacks
- Use efficient antivirus software that can detect and delete the malware
- Implement cloud access security broker (CASB) to monitor cloud traffic for detection of anomalies with the generated instances
- Monitor the employee activities to detect any significant signs of cloud synchronization token abuses

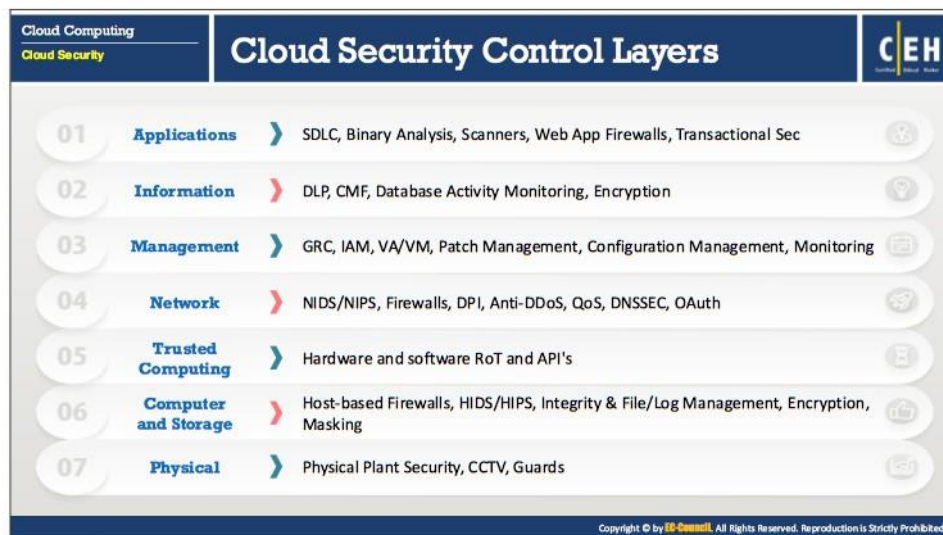




## Cloud Security

There are various risks and threats associated with cloud service adoption and migrating business-critical data to third-party systems. However, following security guidelines and countermeasures strengthens the business case for cloud adoption.

This section deals with various cloud standards, countermeasures, and best practices to secure data hosted in the cloud.



### Cloud Security Control Layers

The following layers show the mapping of Cloud model to the security control model:

- **Application Layer**

To harden the application layer, establish the policies that match with industry adoption security standards, for example, OWASP for a web application. It should meet and comply with appropriate regulatory and business requirements. Some of the application layer controls include SDLC, binary analysis, scanners, web app firewalls, transactional sec, etc.
- **Information Layer**

Develop and document an information security management program (ISMP), which includes administrative, technical, and physical safeguards to protect information against unauthorized access, modification, or deletion. Some of the information layer security controls include DLP, CMF, database activity monitoring, encryption, etc.
- **Management Layer**

This layer covers the cloud security administrative tasks, which can facilitate continued, uninterrupted, and effective services of the cloud. Cloud consumers should look for the above-mentioned policies to avail better services. Some of the management layer security controls include GRC, IAM, VA/VM, patch management, configuration management, monitoring, etc.
- **Network Layer**

It deals with various measures and policies adopted by a network administrator to monitor and prevent illegal access, misuse, modification, or denial of network-accessible

resources. Some of the additional network layer security controls include NIDS/NIPS, firewalls, DPI, anti-DDoS, QoS, DNSSEC, OAuth, etc.

- **Trusted Computing**

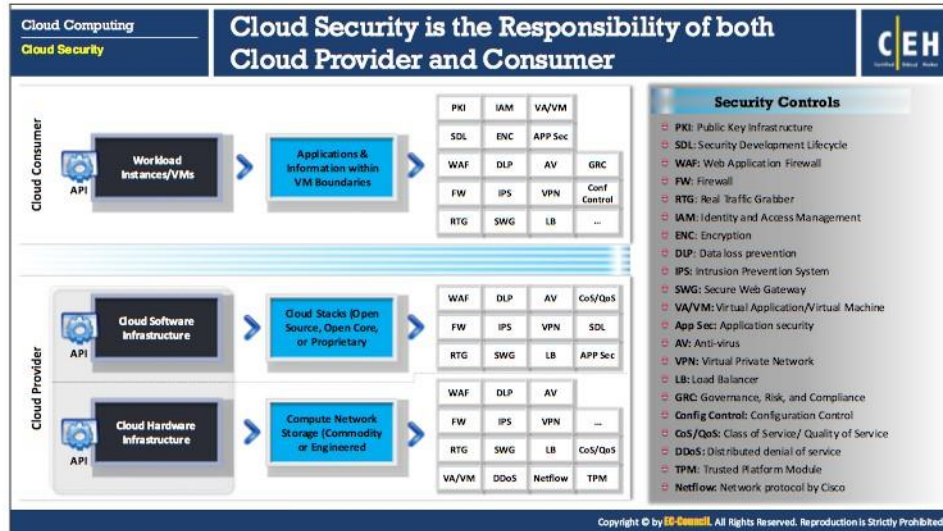
Trust computing defines secured computational environment that implements internal control, auditability, and maintenance to ensure availability and integrity of cloud operations. Hardware and software RoT & API's are few security controls for trusted computing.

- **Computation and Storage**

In cloud due to the lack of physical control of the data and the machine, the service provider may be unable to manage the data and computation and lose the trust of the cloud consumers. Cloud provider must establish policies and procedures for data storage and retention. Cloud provider should implement appropriate backup mechanisms to ensure availability and continuity of services that meet with statutory, regulatory, contractual, or business requirements and compliance. Host-based firewalls, HIDS/HIPS, integrity and file/log management, encryption, masking are some security controls in computation and storage.

- **Physical Layer**

This layer includes security measures for cloud infrastructure, data centers, and physical resources. Security entities that come under this perimeter are physical plant security, fences, walls, barriers, guards, gates, electronic surveillance, CCTV, physical authentication mechanisms, security patrols, and so on.



### Cloud Security is the Responsibility of both Cloud Provider and Consumer

Security is a shared responsibility in cloud systems, in which both cloud consumers and cloud service providers have varying levels of control over available computing resources. Compared to traditional IT systems, in which a single organization has authority over the complete stack of computing resources and the entire life cycle of systems, cloud service providers and consumers work together to design, build, deploy, and operate cloud-based systems. Therefore, both parties share responsibilities to maintain adequate security to these systems. Different cloud service models (IaaS, PaaS, and SaaS) imply varying levels of controls between cloud service providers and cloud consumers.

#### Example:

In the IaaS model, usually, an IaaS platform provider performs account management controls for initial system privileged users, whereas a cloud consumer controls user account management for applications deployed in an IaaS, but not by the cloud provider.

Following are some of the cloud security controls:


- **PKI:** Public Key Infrastructure
- **SDL:** Security Development Lifecycle
- **WAF:** Web Application Firewall
- **FW:** Firewall
- **RTG:** Real Traffic Grabber
- **IAM:** Identity and Access Management
- **ENC:** Encryption
- **DLP:** Data loss prevention
- **IPS:** Intrusion Prevention System
- **SWG:** Secure Web Gateway
- **VA/VM:** Virtual Application/Virtual Machine
- **App Sec:** Application security



- **AV:** Anti-virus
- **VPN:** Virtual Private Network
- **LB:** Load Balancer
- **GRC:** Governance, Risk, and Compliance
- **Config Control:** Configuration Control
- **CoS/QoS:** Class of Service/ Quality of Service
- **DDoS:** Distributed denial of service
- **TPM:** Trusted Platform Module
- **Netflow:** Network protocol by Cisco


**Cloud Computing**  
**Cloud Security**

## Cloud Computing Security Considerations



- Cloud **computing services should be tailor made** by the vendor as per the given security requirements of the clients
- Cloud service providers should provide higher **multi tenancy** which enables optimum utilization of the cloud resources and to secure data and applications
- Cloud services should implement **disaster recovery plan** for the stored data which enables information retrieval in unexpected situations
- Continuous monitoring on the **Quality of Service (QoS)** is required to maintain the **service level agreements** between consumers and the service providers
- Data stored in the cloud services should be implemented securely to ensure **data integrity**

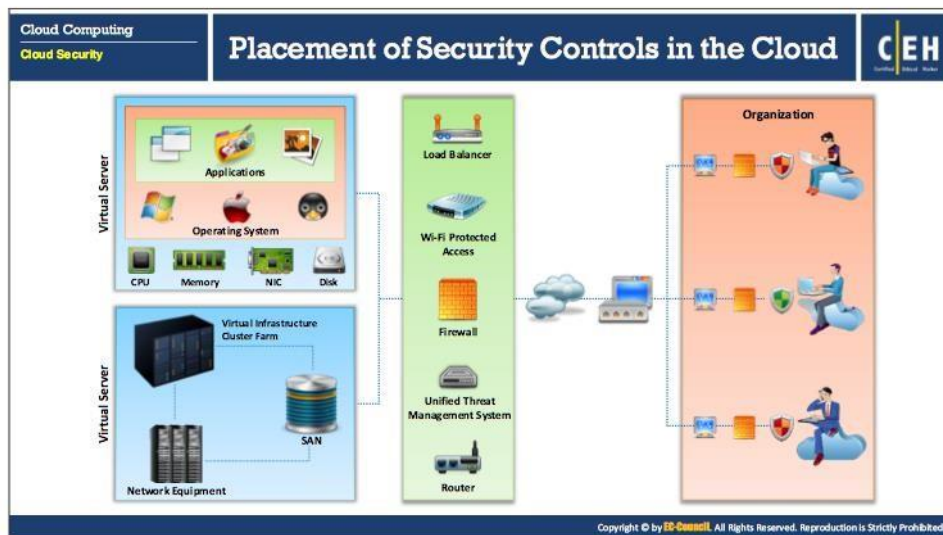
- Cloud computing service should be **fast, reliable**, and need to provide **quick response** times to the new requests
- Symmetric and **asymmetric cryptographic algorithms** must be implemented for optimum data security in cloud computing
- Operational process of the cloud based services should be **engineered, operated, and integrated** securely to the organizational security management
- **Load balancing** should be incorporated in the cloud services to facilitate networks and resources to improve the response time of the job with maximum throughput



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

### Cloud Computing Security Considerations

- Cloud computing services should be tailor-made by the vendor as per the given security requirements of the clients
- Cloud service providers should provide higher multi-tenancy which enables optimum utilization of the cloud resources and to secure data and applications
- Cloud services should implement disaster recovery plan for the stored data which allows information retrieval in unexpected situations
- Continuous monitoring of the Quality of Service (QoS) is required to maintain the service level agreements between consumers and the service providers
- Data stored in the cloud services should be implemented securely to ensure data integrity
- Cloud computing service should be fast, reliable, and need to provide quick response times to the new requests
- Symmetric and asymmetric cryptographic algorithms must be implemented for optimum data security in cloud computing
- Operational process of the cloud-based services should be engineered, operated, and integrated securely to the organizational security management
- Load balancing should be incorporated into the cloud services to facilitate networks and resources to improve the response time of the job with maximum throughput



### Placement of Security Controls in the Cloud

It is a best practice to choose information security controls and implement them in proportion to the risks, generally by assessing threats, vulnerabilities, and impacts. One must ensure that correct defensive implementation is in place, for the cloud security architecture to be efficient. Many security controls exist that when kept in proper place will safeguard any vulnerability in the system and reduces the effect of an attack.

Categories of security controls:

- **Deterrent controls** – These controls reduce attacks on the cloud system.  
Example: Warning sign on the fence or property to inform adverse consequences for potential attackers if they proceed to attack.
- **Preventive controls** – These controls strengthen the system against incidents, probably by minimizing or eliminating vulnerabilities.  
Example: Strong authentication mechanism to prevent unauthorized use of cloud systems.
- **Detective controls** – These controls detect and react appropriately to the incidents that happen.  
Example: Employing IDSs, IPSs, etc. helps to detect attacks on cloud systems.
- **Corrective controls** – These controls minimize the consequences of an incident, probably by limiting the damage.  
Example: Restoring system backups



Cloud Computing  
Cloud Security

## Best Practices for Securing Cloud

CEH

Enforce <b>data protection, backup, and retention</b> mechanisms	Implement strong <b>authentication, authorization and auditing</b> mechanisms
Enforce <b>SLAs</b> for patching and vulnerability remediation	Check for <b>data protection</b> at both design and runtime
Vendors should regularly undergo <b>AICPA SAS 70 Type II audits</b>	Implement <b>strong key generation</b> , storage and management, and destruction practices
Verify one's own cloud in <b>public domain blacklists</b>	Monitor the <b>client's traffic</b> for any malicious activities
Enforce <b>legal contracts</b> in employee behavior policy	Prevent unauthorized server access using <b>security checkpoints</b>
Prohibit <b>user credentials sharing</b> among users, applications, and services	Disclose applicable <b>logs and data</b> to customers

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing  
Cloud Security

## Best Practices for Securing Cloud (Cont'd)

CEH

Analyze <b>cloud provider security policies</b> and SLAs	Leverage strong <b>two-factor authentication</b> techniques where possible
Assess security of <b>cloud APIs</b> and also log customer <b>network traffic</b>	Baseline <b>security breach notification</b> process
Ensure that cloud undergoes regular <b>security checks and updates</b>	Analyze <b>API dependency chain software</b> modules
Ensure that physical security is a <b>24 x 7 x 365</b> affair	Enforce stringent <b>registration and validation process</b>
Enforce <b>security standards</b> in installation/ configuration	Perform vulnerability and configuration <b>risk assessment</b>
Ensure that the memory, storage, and network access is <b>isolated</b>	Disclose infrastructure information, <b>security patching</b> , and firewall details

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The infographic is titled "Best Practices for Securing Cloud (Cont'd)" and is part of a "Cloud Security" series. It lists ten best practices, numbered 1 through 10. The practices are:

1. Enforce stringent **cloud security compliance**, SCM (Software Configuration Management), and management practice transparency
2. Employ security devices such as IDS, IPS, firewall, etc. to guard and stop **unauthorized access** to the data stored in the cloud
3. Enforce strict **supply chain** management and conduct a comprehensive supplier assessment
4. Enforce stringent **security policies and procedures** like access control policy, information security management policy and contract policy
5. Ensure **infrastructure security** through proper management and monitoring, availability, secure VM separation and service assurance
6. Use **VPNs** to secure the clients data and ensure that data is **completely deleted** from the main servers along with its replicas when requested for data disposal
7. Ensure **Secure Sockets Layer (SSL)** is used for sensitive and confidential data transmission
8. Analyze the **security model** of cloud provider interfaces
9. Understand terms and conditions in **SLA** like **minimum level of uptime** and **penalties** in case of failure to adhere to the agreed level
10. Enforce basic information security practices namely strong **password policy**, **physical security**, device security, **encryption**, data security, network security, etc.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

### Best Practices for Securing Cloud

- Enforce data protection, backup, and retention mechanisms
- Enforce SLAs for patching and vulnerability remediation
- Vendors should regularly undergo AICPA SAS 70 Type II audits
- Verify one's cloud in public domain blacklists
- Enforce legal contracts in employee behavior policy
- Prohibit user credentials sharing among users, applications, and services
- Implement secure authentication, authorization, and auditing mechanisms
- Check for data protection at both design and runtime
- Implement strong key generation, storage and management, and destruction practices
- Monitor the client's traffic for any malicious activities
- Prevent unauthorized server access using security checkpoints
- Disclose applicable logs and data to customers
- Analyze cloud provider security policies and SLAs
- Assess security of cloud APIs and also log customer network traffic
- Ensure that cloud undergoes regular security checks and updates
- Ensure that physical security is a 24 x 7 x 365 affair
- Enforce security standards in installation/ configuration
- Ensure that the memory, storage, and network access is isolated
- Leverage strong two-factor authentication techniques where possible

- Baseline security breach notification process
- Analyze API dependency chain software modules
- Enforce stringent registration and validation process
- Perform vulnerability and configuration risk assessment
- Disclose infrastructure information, security patching, and firewall details to customers
- Enforce stringent cloud security compliance, SCM (Software Configuration Management), and management practice transparency
- Employ security devices such as IDS, IPS, firewall, etc. to guard and stop unauthorized access to the data stored in the cloud
- Enforce strict supply chain management and conduct a comprehensive supplier assessment
- Enforce stringent security policies and procedures like access control policy, information security management policy and contract policy
- Ensure infrastructure security through proper management and monitoring, availability, secure VM separation and service assurance
- Use VPNs to secure the client's data and ensure that data is completely deleted from the primary servers along with its replicas when requested for data disposal
- Ensure Secure Sockets Layer (SSL) is used for sensitive and confidential data transmission
- Analyze the security model of cloud provider interfaces
- Understand terms and conditions in SLA like minimum level of uptime and penalties in case of failure to adhere to the agreed level
- Enforce basic information security practices namely strong password policy, physical security, device security, encryption, data security, network security, etc.



The infographic is titled "NIST Recommendations for Cloud Security" and is part of a "Cloud Security" series. It lists seven recommendations, each with a corresponding icon and a brief description:

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### NIST Recommendations for Cloud Security

- Assess risk posed to client's data, software, and infrastructure
- Select 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 found between organization's security requirements and cloud provider's standards
- Establish appropriate incident detection and reporting mechanisms
- Analyze what are the security objectives of organization
- Enquire about who is responsible for data privacy and security issues in cloud

Cloud Computing Cloud Security	Organization/Provider Cloud Security Compliance Checklist		CEH
Management	Organization	Provider	
Is everyone aware of his or her cloud security responsibilities?			
Is there a mechanism for assessing the security of a cloud service?			
Does the business governance mitigate the security risks that can result from cloud-based "shadow IT"?			
Does the organization know within which jurisdictions its data can reside?			
Is there a mechanism for managing cloud-related risks?			
Does the organization understand the data architecture needed to operate with appropriate security at all levels?			
Can the organization be confident of end-to-end service continuity across several cloud service providers?			
Does the provider comply with all relevant industry standards (e.g. the UK's Data Protection Act)?			
Does the compliance function understand the specific regulatory issues pertaining to the organization's adoption of cloud services?			

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

**Organization/Provider Cloud Security Compliance Checklist**

Provided below are checklists for determining whether the security team, the rest of the organization, and any proposed cloud provider can assure cloud security:

**Checklist to determine if the security team is fit and ready for cloud security:**

	Security Team
If the members of security team are formally trained in cloud technologies?	<input type="checkbox"/>
If the organization's security policies consider the cloud infrastructure?	<input type="checkbox"/>
If security team has ever been involved in implementing cloud infrastructure?	<input type="checkbox"/>
If an organization has defined security assessment procedures for cloud infrastructure?	<input type="checkbox"/>
If an organization has ever been audited for cloud security threats?	<input type="checkbox"/>
If the organization's cloud adoption will comply with the security standards that organization follows?	<input type="checkbox"/>
Has security governance been adapted to include cloud?	<input type="checkbox"/>
If the team has adequate resources to implement cloud infrastructure and security?	<input type="checkbox"/>

TABLE 19.1: Checklist to determine if the security team is fit and ready for cloud security

Operation	Organization	Provider
Are regulatory compliance reports, audit reports and reporting information available from the provider?	<input type="checkbox"/>	<input type="checkbox"/>
If the organization's incident handling and business continuity policies	<input type="checkbox"/>	<input type="checkbox"/>

and procedures are designed considering cloud security issues?		
If the cloud service provider's compliance and audit reports are accessible to the organization?	<input type="checkbox"/>	<input type="checkbox"/>
If the CSP's SLA address incident handling and business continuity concerns?	<input type="checkbox"/>	<input type="checkbox"/>
If the CSP has clear policies and procedures to handle digital evidence in the cloud infrastructure?	<input type="checkbox"/>	<input type="checkbox"/>
If the CSP itself is compliant with the industry standards?	<input type="checkbox"/>	<input type="checkbox"/>
If the CSP has skilled and sufficient staff for incident resolution and configuration management?	<input type="checkbox"/>	<input type="checkbox"/>
If the CSP has defined procedures to support the organization in case of incidents involving several clients in a multi-tenant environment?	<input type="checkbox"/>	<input type="checkbox"/>
Does using a cloud provider give the organization an environmental advantage?	<input type="checkbox"/>	<input type="checkbox"/>
Does the organization know in which application or database each data entity is stored or mastered?	<input type="checkbox"/>	<input type="checkbox"/>
Is the cloud-based application maintained and disaster tolerant (i.e., would it recover from an internal or externally caused disaster)?	<input type="checkbox"/>	<input type="checkbox"/>
Are all personnel appropriately vetted, monitored, and supervised?	<input type="checkbox"/>	<input type="checkbox"/>
If the CSP provides flexibility of service relocation and switchovers?	<input type="checkbox"/>	<input type="checkbox"/>
If the CSP has implemented perimeter security controls such as IDS, firewalls, etc. and provides regular activity logs to the organization?	<input type="checkbox"/>	<input type="checkbox"/>
If the CSP provide reasonable assurance of quality or availability of service?	<input type="checkbox"/>	<input type="checkbox"/>
Is it easy to securely integrate the cloud-based applications at runtime and contract termination?	<input type="checkbox"/>	<input type="checkbox"/>
If the CSP provides 24/7 support for cloud operations and security-related issues?	<input type="checkbox"/>	<input type="checkbox"/>
Do the procurement processes contain cloud security requirements?	<input type="checkbox"/>	<input type="checkbox"/>

TABLE 19.2: Checklist to determine if the organization/provider is fit and ready for cloud security based on its operations

<b>Technology</b>	<b>Organization</b>	<b>Provider</b>
Are there appropriate access controls (e.g., federated single sign-on) that give users controlled access to cloud applications?	<input type="checkbox"/>	<input type="checkbox"/>
Is data separation maintained between the organization's information and that of other customers of the provider, at runtime and during backup (including data disposal)?	<input type="checkbox"/>	<input type="checkbox"/>
Has the organization considered and addressed backup, recovery,	<input type="checkbox"/>	<input type="checkbox"/>

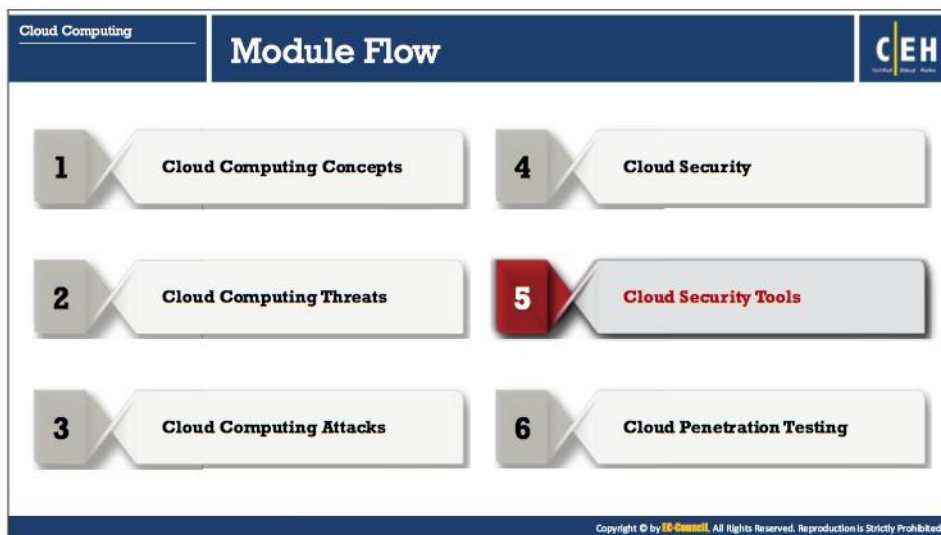


archiving and decommissioning of data stored in a cloud environment?		
Are mechanisms in place for authentication, authorization, and key management in a cloud environment?	<input type="checkbox"/>	<input type="checkbox"/>
Are mechanisms in place to manage network congestion, misconnection, misconfiguration, lack of resource isolation, etc., which affects services and security?	<input type="checkbox"/>	<input type="checkbox"/>
Has organization implemented sufficient security controls on the client devices used to access the cloud?	<input type="checkbox"/>	<input type="checkbox"/>
Are all cloud-based systems, infrastructure, and physical locations suitably protected?	<input type="checkbox"/>	<input type="checkbox"/>
Are the network designs suitably secure for the organization's cloud adoption strategy?	<input type="checkbox"/>	<input type="checkbox"/>

TABLE 19.3: Checklist to determine if the organization/provider is fit and ready for cloud security based on its technology

<b>Management</b>	<b>Organization</b>	<b>Provider</b>
Is everyone aware of his or her cloud security responsibilities?	<input type="checkbox"/>	<input type="checkbox"/>
Is there a mechanism for assessing the security of a cloud service?	<input type="checkbox"/>	<input type="checkbox"/>
Does the business governance mitigate the security risks that can result from cloud-based "shadow IT"?	<input type="checkbox"/>	<input type="checkbox"/>
Does the organization know within which jurisdictions its data can reside?	<input type="checkbox"/>	<input type="checkbox"/>
Is there a mechanism for managing cloud-related risks?	<input type="checkbox"/>	<input type="checkbox"/>
Does the organization understand the data architecture needed to operate with appropriate security at all levels?	<input type="checkbox"/>	<input type="checkbox"/>
Can the organization be confident of end-to-end service continuity across several cloud service providers?	<input type="checkbox"/>	<input type="checkbox"/>
Does the provider comply with all relevant industry standards (e.g., the UK's Data Protection Act)?	<input type="checkbox"/>	<input type="checkbox"/>
Does the compliance function understand the specific regulatory issues about the organization's adoption of cloud services?	<input type="checkbox"/>	<input type="checkbox"/>

TABLE 19.4: Checklist to determine if the organization/provider is fit and ready for cloud security based on its management



## Cloud Security Tools

Tough migrating to the cloud has enormous benefits; security issues are the primary concern for enterprise cloud adoption. However, many security services or tools are available that can be used to automate the process of cloud pen testing to ensure confidentiality, integrity, and security of data hosted in the cloud.

This section deals with some of the cloud security tools such as Qualys Cloud Platform, CloudPassage Halo, Core CloudInspect, etc.

Cloud Computing  
Cloud Security Tools

## Cloud Security Tools

### Qualys Cloud Platform

- Qualys Cloud Platform is a **end-to-end IT security solution** that provides a continuous, always-on **assessment of the global security** and compliance posture, with visibility across all IT assets irrespective of where they reside

<https://www.qualys.com>

<https://www.cloudpassage.com>

### CloudPassage Halo

CloudPassage Halo is the **cloud server security platform** with all the security functions you need to safely deploy servers in public and hybrid clouds

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing  
Cloud Security Tools

## Cloud Security Tools (Cont'd)

### Core CloudInspect

- Core Cloudinspect **helps validate** when cloud deployment is secure—and gives **actionable remediation information** when it is not secured
- The service conducts **proactive, real-world security tests** using the techniques employed by attackers seeking to **breach your AWS cloud-based systems** and applications

<https://www.coresecurity.com>

**Nessus Enterprise for AWS**  
<https://www.tenable.com>

**Symantec Cloud Workload Protection**  
<https://www.symantec.com>

**Alert Logic**  
<https://www.alertlogic.com>

**Deep Security**  
<https://www.trendmicro.com>

**SecludIT**  
<https://secludit.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

### Cloud Security Tools

- **Qualys Cloud Platform**

Source: <https://www.qualys.com>

Qualys Cloud Platform is an end-to-end IT security solution that provides a continuous, always-on assessment of the global security and compliance posture, with visibility across all your IT assets irrespective of where they reside.

Module 19 Page 2153

Ethical Hacking and Countermeasures Copyright © by **EC-Council**  
 All Rights Reserved. Reproduction is Strictly Prohibited.



**Features:**

- Sensors provide continuous visibility
- All your data can be analyzed in real time
- Respond to threats immediately
- Active vulnerability ICMP Timestamp Request
- Visualize results in one place with AssetView

▪ **CloudPassage Halo**

Source: <https://www.cloudpassage.com>

The CloudPassage Halo software-defined security (SDSec) platform was purpose-built to protect private clouds, public IaaS, and hybrid/multi-cloud infrastructure. It is a security and compliance automation from development to deployment, across clouds, data centers, servers, and containers – at DevOps speed and cloud scale. It automates and orchestrates layered access control, vulnerability management, compromise prevention, compliance monitoring, and security intelligence collection.

**Features:**

- **Workload Firewall Management:** Deploy and manage dynamic firewall policies across public, private, and hybrid cloud environments.
- **Multifactor Network Authentication:** Enables secure remote network access using two-factor authentication via SMS to a mobile phone, or using a YubiKey with no additional software or infrastructure.
- **Configuration Security Monitoring:** Automatically monitors OS and application configurations, processes, network services, privileges, and so on.
- **Software Vulnerability Assessment:** Scans for vulnerabilities in your packaged software rapidly and automatically, across all of your cloud environments.
- **File Integrity Monitoring:** Protects the integrity of your cloud servers by continually monitoring for unauthorized or malicious changes to essential system binaries and configuration files.
- **Server Account Management:** Evaluates who has accounts on which cloud servers, what privileges they operate under, and the usage of accounts.
- **Event Logging and Alerting:** Detects a broad range of events and system states, alerting you when they occur.
- **Halo REST API:** Provides full automation of the cloud deployments and integrate security platform with other systems.

▪ **Core CloudInspect**

Source: <https://www.coresecurity.com>

Core CloudInspect helps to validate when cloud deployment is secure and gives actionable remediation information when it is not. The service conducts proactive, real-

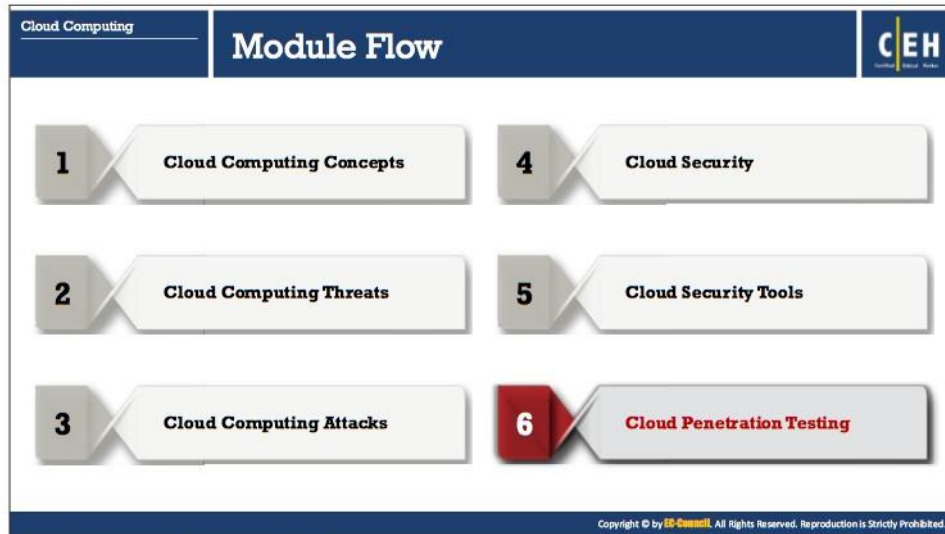
world security tests using the techniques employed by attackers seeking to breach your AWS cloud-based systems and applications.

Core CloudInspect enables you to:

- Proactively verify the security of your AWS deployments against real, current attack techniques
- Safely pinpoint and validate critical OS and services vulnerabilities with no false positives
- Measure your susceptibility to SQL injection, cross-site scripting, and other web-application attacks
- Validate security controls required by industry and government regulations
- Get actionable information necessary to apply patches and implement code fixes
- Certify systems before they go live and frequently test to reconfirm security posture over time

Some of the additional cloud security tools include:

- Nessus Enterprise for AWS (<https://www.tenable.com>)
- Symantec Cloud Workload Protection (<https://www.symantec.com>)
- Alert Logic (<https://www.alertlogic.com>)
- Deep Security (<https://www.trendmicro.com>)
- SecludIT (<https://secludit.com>)
- Panda Cloud Office Protection (<https://www.pandasecurity.com>)
- Data Security Cloud (<https://www.informatica.com>)
- Cloud Application Control (<https://www.zscaler.com>)
- Intuit Data Protection Services (<https://security.intuit.com>)



## Cloud Penetration Testing

Cloud penetration testing is the security testing methodology for cloud systems. It involves an active analysis of the cloud system for potential vulnerabilities that may result from hardware or software flaws, sharing resources, system misconfiguration, operational weaknesses, and others. Black box pen testing (i.e., testing the cloud infrastructure without prior knowledge of the cloud administrators) is a most effective way of assessing the security posture of a cloud service provider.

This section deals with cloud pen testing, key considerations for pen testing in the cloud, the scope of cloud pen testing, cloud pen-testing methodology, and recommendations for cloud testing.



The slide is titled "What is Cloud Pen Testing?" and is part of a presentation on "Cloud Computing" and "Cloud Penetration Testing". It features a blue header with the CEH logo. The main content is divided into two sections: a list of three bullet points and a section titled "Scope of Cloud Pen Testing".

- Cloud pen testing is a method of actively evaluating the security of a cloud system by **simulating an attack from a malicious source**
- Security posture of cloud should be monitored regularly to determine the presence of **vulnerabilities** and the **risks** they pose
- Cloud security is based on the shared responsibility of both **cloud provider** and the **client**

**Scope of Cloud Pen Testing**

The scope of cloud pen testing depends on the type of cloud service used by the client

- **Infrastructure-as-a-Service (IaaS)** – virtualization security, solution stack, application layer, APIs, etc.
- **Platform-as-a-Service (PaaS)** – application and API layers
- **Software-as-a-Service (SaaS)** – usually **third party pen testing** is not allowed by SaaS vendors until unless it is explicitly mentioned in the Service Level Agreement (SLA)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### What is Cloud Pen Testing?

Cloud pen testing is a method of actively evaluating the security of a cloud system by simulating an attack from a malicious source. Security posture of the cloud should regularly be monitored to determine the presence of vulnerabilities and the risks they pose. Cloud security is based on the shared responsibility of both cloud provider and the client. Pen testing a cloud ensures confidentiality, integrity, and security of the data it hosts. Any organization, regardless of its size, needs to ensure that all its information assets are auditable, comply with industry regulations and do not jeopardize the organization's data and programs.

Carry out cloud pen testing either manually, using industry standard techniques or using automated software applications such as Qualys Cloud Platform, Core CloudInspect, CloudPassage Halo, Alert Logic, and SecludIT.

#### Pen testing cloud involves three phases:

- **Preparation:** It consists in signing formal agreements to ensure the protection of both parties (Cloud Service Provider [CSP] and client). It defines the policy and course of action the CSP and client should take in finding potential vulnerabilities and their mitigation. Pen testing also considers other users who might be using the same infrastructure under testing.
- **Execution:** It involves executing the cloud pen-testing plan to find out potential vulnerabilities, if any, existing in the cloud.
- **Delivery:** Once cloud pen testing is complete, document all the exploits/vulnerabilities, and hand over the document to the provider to take necessary action.

### **Scope of Cloud Pen Testing**

Because a cloud is a multi-tenant environment, it is essential to determine the scope of pen testing before executing it in a CSP's network. The scope defines what to test, how to test, and the extent of testing. As resources such as dynamic IP addresses change in the environment, as a penetration tester, one need to be very cautious during testing, to prevent accidental testing of resources that the client does not own, as it may lead to a violation of legal terms and services. The scope of cloud pen testing depends on the type of cloud service used by the client.


- IaaS – virtualization security, solution stack, application layer, APIs, etc.
- PaaS – application and API layers
- SaaS – usually third party pen testing is not allowed by SaaS vendors until unless it is mentioned explicitly in the Service Level Agreement (SLA)
- Pen testing web applications should include mobile applications as well
- Pen testing network or host comprises systems, firewalls, IDS, databases, etc., that are available in cloud
- Pen testing web services should consist of mobile back-end services

Cloud Computing  
Cloud Penetration Testing

## Key Considerations for Pen Testing in the Cloud

CEH

- Determine the **type of cloud**; PaaS, IaaS or SaaS
- Obtain **written consents** for performing pen testing
- Ensure every aspect of the Infrastructure (IaaS), Platform (PaaS), or Software (SaaS) are included in the **scope of testing** and **generated reports**
- Determine **how often and what kind of testing** is permitted by Cloud Service Provider (CSP)
- Prepare **legal** and **contractual** documents
- Perform both **internal** and **external pen testing**
- Perform pen tests on the **web apps/services** in the cloud without web application firewall (WAF) or reverse proxy
- Perform **vulnerability scans on host** available in the cloud
- Determine how to coordinate with the CSP for **scheduling** and **performing the test**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Key Considerations for Pen Testing in the Cloud

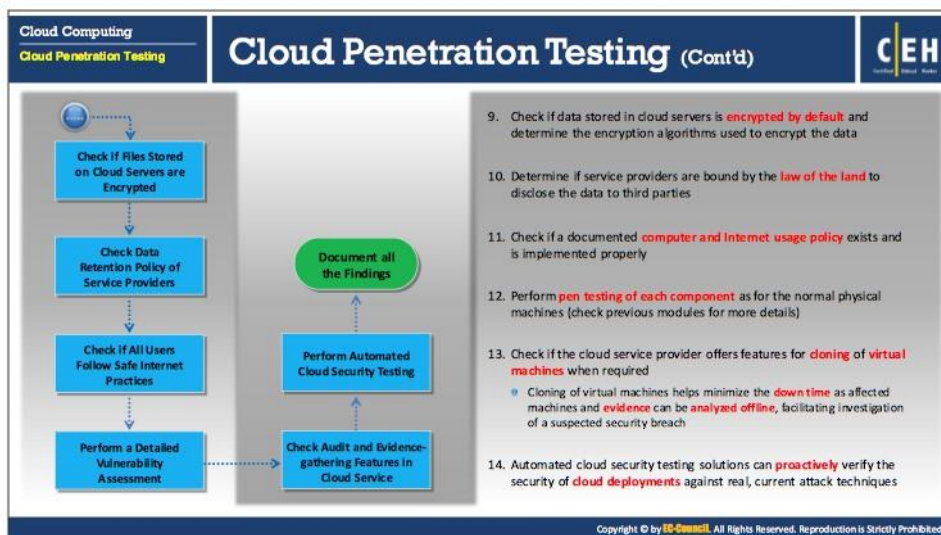
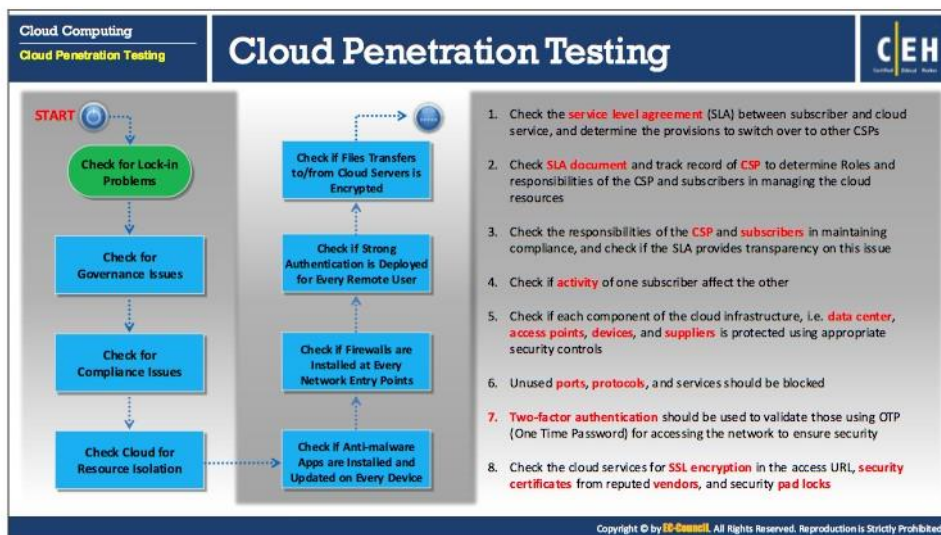
Most organizations around the world—small and large—are adopting cloud services to handle business-critical data. Robust cloud technology offers many benefits such as improved efficiency, reduced costs, improved accessibility, and flexibility. There also exist many security risks such as issues with encryption, risk factors associated with virtual machines, vulnerabilities arising from shared resources, and so on. Thus, organizations depending on cloud computing technology need to perform pen testing of their critical assets present in the cloud, which makes it possible to address vulnerabilities and the associated risks beforehand, preventing attackers from exploiting them.

Following are some of the critical considerations for pen testing cloud:

- Determine the type of cloud; PaaS, IaaS or SaaS as well as the type of cloud provider determines if pen testing is allowed or not
  - If it is SaaS, pen testing is not permitted by providers as it might impact their infrastructure
  - If it is PaaS or IaaS, pen testing is permitted, but coordination is required
  - The contract and SLA made with cloud provider states if pen testing is permitted, if so what kinds of tests are allowed and how frequently can it be performed
- Obtain written consents for performing pen testing
- Ensure every aspect of the Infrastructure (IaaS), Platform (PaaS), or Software (SaaS) are included in the scope of testing and generated reports
- Determine what kind of testing is permitted by CSP and how often
- Prepare legal and contractual documents



- Perform both internal and external pen testing
- Perform pen tests on the web apps/services in the cloud without web application firewall (WAF) or reverse proxy
- Perform vulnerability scans on host available in the cloud
- Determine how to coordinate with the CSP for scheduling and performing the test



### Cloud Penetration Testing

Discussed below are the steps involved in the cloud pen-testing process:

- **Step 1: Check for Lock-in Problems**

Lock-in refers to a situation in which a subscriber cannot switch to another CSP. Check the service-level agreement (SLA) between subscriber and cloud service, and determine the provisions to switch over to other CSPs.

▪ **Step 2: Check for Governance Issues**

Check the SLA document, and track the record of the CSP to determine:

- Roles and responsibilities of CSP and subscribers in managing the cloud resources (network bandwidth, storage, computing power, memory management, virtual machines, etc.)
- Any discrepancy in SLA clauses and their implementation
- Visibility of CSP's audit or certification to customers
- Hidden dependency on resources outside the cloud
- Source escrow agreement and vulnerability assessment process
- Certification schemes adapted to cloud infrastructures
- Jurisdictions over CSP for SLA related issues
- Completeness and transparency regarding use
- Cloud asset ownership

▪ **Step 3: Check for Compliance Issues**

Cloud compliance issues arise from the use of cloud storage or backup services. Recommendations to check for compliance issues include:

- Compliance with PCI, SOX, and other acts is a major concern for shifting to cloud computing
- Check the SLA for whether the CSP is regularly audited and certified for compliance issues
- Determine the regulations that the CSP complies with
- Check the responsibilities of the CSP and subscribers in maintaining compliance, and check if the SLA provides transparency on this issue

▪ **Step 4: Check Cloud for Resource Isolation**

Recommendations to check cloud for resource isolation:

- Check if activity of one subscriber affects the other
- Check the CSP's client feedback and expert reviews
- Check the track record and any security of CSP's services

▪ **Step 5: Check if Anti-malware Applications are Installed and Updated on Every Device**

- Check whether each component of the cloud infrastructure (i.e., data center, access points, devices, and suppliers) is protected using appropriate security controls
- Check for updates, outbreak alerts, and automatic scans

▪ **Step 6: Check if CSP has installed Firewalls at Every Network Entry Points**

- Check whether the firewalls are installed at every network entry point



- Unused ports, protocols, and services should be blocked
- **Step 7: Check if the provider has deployed Strong Authentication for Every Remote User**
  - All the remote users should use an eight-character password which is alphanumeric
  - Two-factor authentication should be used to validate those using OTP (one-time password) for accessing the network to ensure security
- **Step 8: Check whether the Provider Encrypts Files Transferred to/from Cloud Servers**
  - Check the cloud services for SSL encryption in the access URL, security certificates from reputed vendors, and security padlocks
  - Check if VPN and secure email services are used for communication
  - Check security and privacy policies of the cloud service
- **Step 9: Check whether Files Stored on Cloud Servers are Encrypted**
  - Check if default encrypts data stored in cloud servers and determine the encryption algorithms used to encrypt the data
  - Check whether cloud service providers or service users hold the algorithmic keys for the encryption
- **Step 10: Check the Data Retention Policy of Service Providers**
  - Determine if service providers are bound by the law of the land to disclose the data to third parties
  - Check the duration of the data retention in the cloud and procedures to delete the data from the cloud
  - Check how data retention will be handled in case the service provider is acquired by another service provider or ceases to exist due to any other reasons
- **Step 11: Check whether All Users Follow Safe Internet Practices**
  - Check if a documented computer and Internet usage policy exists and is implemented properly
  - Check if firewalls, IDS/IPS systems, and anti-malware applications are configured properly
  - Check if the staff is regularly educated not to engage in and how to respond to risks such as sharing passwords, responding to phishing emails, and downloading files without verifying the source
- **Step 12: Perform a Detailed Vulnerability Assessment**
  - Perform pen testing of each component as for the normal physical machines (check previous modules for more details)

▪ **Step 13: Check Audit and Evidence-Gathering Features in the Cloud Service**

- Check if the cloud service provider offers features for cloning of virtual machines when required
- Cloning of virtual machines helps minimize the downtime as affected machines and evidence can be analyzed offline, facilitating investigation of a suspected security breach
- Multiple clones can also save the investigation time and improve chances of tracing perpetrators

▪ **Step 14: Perform Automated Cloud Security Testing**

- Automated cloud security testing solutions can proactively verify the security of cloud deployments against real, current attack techniques

Tools used to perform Automated Cloud Security Testing:

- Qualys Cloud Platform (<https://www.qualys.com>)
- CloudPassage Halo (<https://www.cloudpassage.com>)
- Core CloudInspect (<https://www.coresecurity.com>)

▪ **Step 15: Document all the Findings**

Once cloud pen testing is complete, collect and document all information you obtained at every stage. You can use this document to study, understand, and analyze the security posture of the client's cloud environment. Address vulnerabilities and resultant risks and suggest mitigation techniques to apply to reduce the risk of security compromise to an acceptable level.

Cloud Computing  
Cloud Penetration Testing

## Recommendations for Cloud Testing

CEH

- 1 Find out whether the cloud provider will accommodate your own security policies or not
- 2 Compare the provider's security precautions to the present levels of security to ensure the provider is achieving better security levels for the user
- 3 Ensure that the cloud computing partners suggest risk assessment techniques and information on how to reduce the uncovered security risks
- 4 Make sure that a cloud service provider is capable of providing their policies and procedures for any security agreement that an agency faces
- 5 Pay attention to the service provider's agreement so that the coding policies can be secured
- 6 Authenticate users with a user name and password
- 7 Ensure that all credentials such as accounts and passwords assigned to the cloud provider should be changed regularly by the organization
- 8 Strong password policies must be advised and employed by the cloud pen testing agencies

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing  
Cloud Penetration Testing

## Recommendations for Cloud Testing (Cont'd)

CEH

- 9 Ensure that the existing business IT security protocols are up-to-date and flexible enough to handle the risks involved in cloud computing
- 10 Make sure that IT support can be offered and use more stringent layers of security to prevent potential data breaches
- 11 Make sure that the access to virtual environment management interfaces is highly restricted
- 12 Password encryption is advisable
- 13 Protect the information which is uncovered during the penetration testing
- 14 Pay special attention to cloud hypervisors, the servers that run multiple operating systems
- 15 Use a centralized authentication or single sign on for the firms that use SaaS applications
- 16 Make sure that the workers are provided with the best training possible to comply with these security parameters

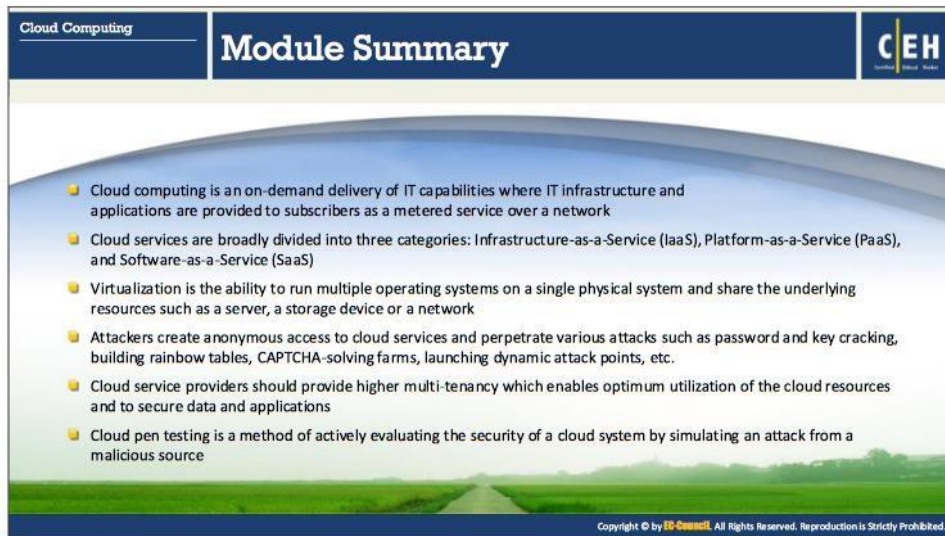
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Recommendations for Cloud Testing

- Find out whether the cloud provider will accommodate your security policies or not
- Compare the provider's security precautions to the present levels of security to ensure the provider is achieving better security levels for the user
- Ensure that the cloud computing partners suggest risk assessment techniques and information on how to reduce the uncovered security risks



- Make sure that a cloud service provider is capable of providing their policies and procedures for any security agreement that an agency faces
- Pay attention to the service provider's agreement to secure the coding policies
- Authenticate users with a username and password
- Ensure that all credentials such as accounts and passwords assigned to the cloud provider should regularly be changed by the organization
- Strong password policies must be advised and employed by the cloud pen testing agencies
- Ensure that the existing business IT security protocols are up-to-date and flexible enough to handle the risks involved in cloud computing
- Make sure that you can offer IT support and use more stringent layers of security to prevent potential data breaches
- Make sure that the access to virtual environment management interfaces is highly restricted
- Password encryption is advisable
- Protect the information which is uncovered during the penetration testing
- Pay particular attention to cloud hypervisors, the servers that run multiple OSs
- Use centralized authentication or single sign-on for the firms that use SaaS applications
- Make sure that the workers are provided with the best training possible to comply with these security parameters



The slide features a dark blue header with 'Cloud Computing' on the left and 'Module Summary' in the center. On the right is the CEH logo. The main content area has a light blue background with a list of six bullet points. At the bottom, there is a green landscape image and a small copyright notice.

Cloud Computing

## Module Summary

CEH

- Cloud computing is an on-demand delivery of IT capabilities where IT infrastructure and applications are provided to subscribers as a metered service over a network
- Cloud services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS)
- Virtualization is the ability to run multiple operating systems on a single physical system and share the underlying resources such as a server, a storage device or a network
- Attackers create anonymous access to cloud services and perpetrate various attacks such as password and key cracking, building rainbow tables, CAPTCHA-solving farms, launching dynamic attack points, etc.
- Cloud service providers should provide higher multi-tenancy which enables optimum utilization of the cloud resources and to secure data and applications
- Cloud pen testing is a method of actively evaluating the security of a cloud system by simulating an attack from a malicious source

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Module Summary

This module ends with an overview discussion of cloud-computing concepts, threats and attacks, security, and pen testing. In the next module, we will discuss cryptography.

---

This page is intentionally left blank.