Cloud Computing

Module 17

Ethical Hacking and Countermeasures v9

Module 17: Cloud Computing

Exam 312-50

Statistics: Cloud Predictions

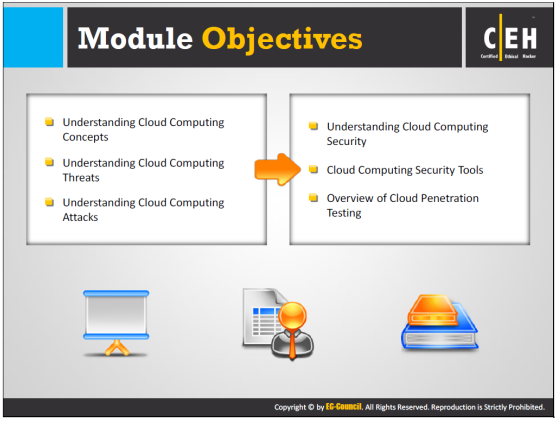
- More than 65% of enterprise IT organizations will commit to hybrid cloud technologies before 2016, vastly driving the rate and pace of change in IT organizations
- By 2017, 20% of enterprises will see enough value in community-driven open source standards/frameworks to adopt them strategically
- By 2017, 25% of IT organizations will formally support a "consumer tier" to allow workers to develop their own personal automation
- By 2017, IT buyers will actively channel 20% of their IT budgets through industry clouds to enable flexible collaboration, information sharing, and commerce
- By 2016, more than 50% of enterprise IT organizations building hybrid clouds will purchase new or updated workload-aware cloud management solutions

IDC FutureScape: Worldwide Cloud 2015 Predictions, *https://www.idc.com*

Statistics: Cloud Predictions (Cont'd)

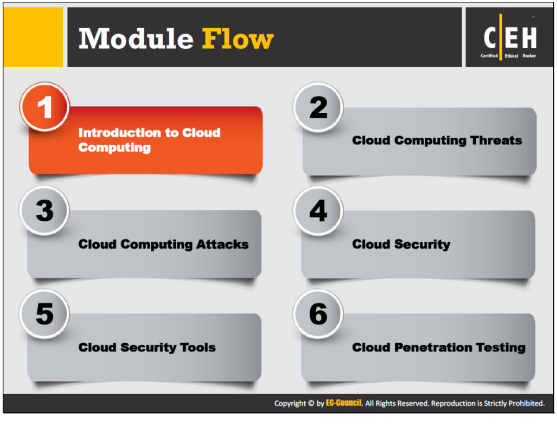
- 60% of SaaS applications will leverage new function-driven, micro-priced IaaS capabilities by 2018, adding innovation to a "commodity" service
- By 2015, 65% of the selection criteria for enterprise cloud workloads in global IT markets will be shaped by efforts to comply with data privacy legislation
- 75% of IaaS provider offerings will be redesigned, rebranded, or phased out in the next 12-24 months
- By 2016, there will be an 11% shift of IT budget away from traditional in-house IT delivery, towards various versions of cloud as a new delivery model
- By 2017, 35% of new applications will use cloud-enabled continuous delivery and DevOps lifecycles for faster rollout of new features and business innovation

IDC FutureScape: Worldwide Cloud 2015 Predictions, *https://www.idc.com*



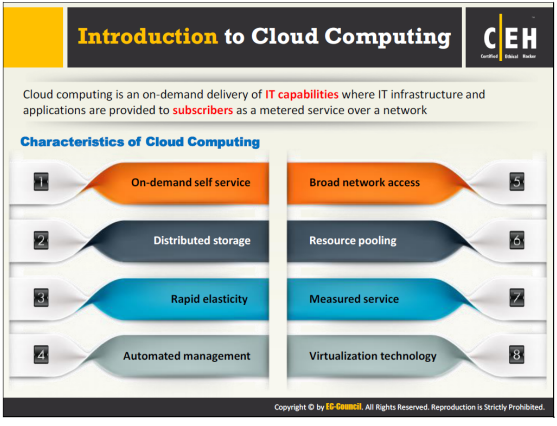
Cloud computing is an emerging technology that delivers computing services such as online business applications, online data storage, and webmail over the Internet. Cloud implementation enables a distributed workforce, reduces organization expenses, provides data security, and so on. As many enterprises are adopting the cloud, attackers make cloud as their target of exploit in order 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 an ethical hacker should follow to perform a security assessment of the cloud environment.



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.



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.

Discussed below are the characteristics of cloud computing that attract many business today to adapt 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, and so on, always on demand, without the need for human interaction with service providers.

- **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.

- **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.

- **Measured service**

  Cloud systems employ "pay-per-use" metering method. Subscribers pay for cloud services by monthly subscription or according to 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.

- **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 cloud consumer.

- **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.

- **Virtualization technology**

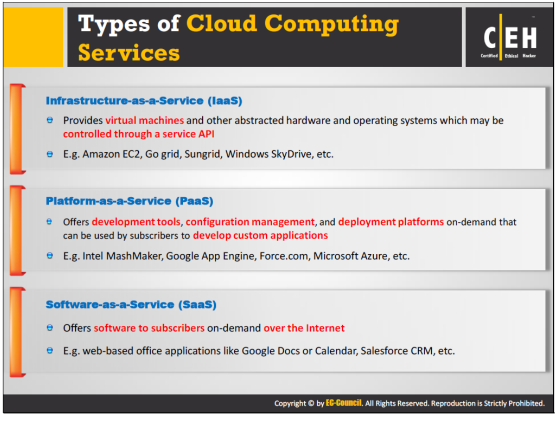
  Virtualization technology in cloud enables rapid scaling of resources in a way that non-virtualized environments could not achieve.

- **Automated management**

  By minimizing the user involvement, cloud automation speeds up the process, reduces labor costs, and reduces the possibility of human error.

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



Cloud services are broadly divided into three categories:

Infrastructure-as-a-Service (IaaS)

This type of cloud computing service enables subscribers to use fundamental IT resources such as computing power, virtualization, data storage, network, and so on, on demand. 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).

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 buy and manage the software and infrastructure underneath it, but have authority over deployed applications and perhaps application hosting environment configurations. Advantages of writing applications in the PaaS environment includes dynamic scalability, automated backups, and other platform services, without the need to specifically 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)

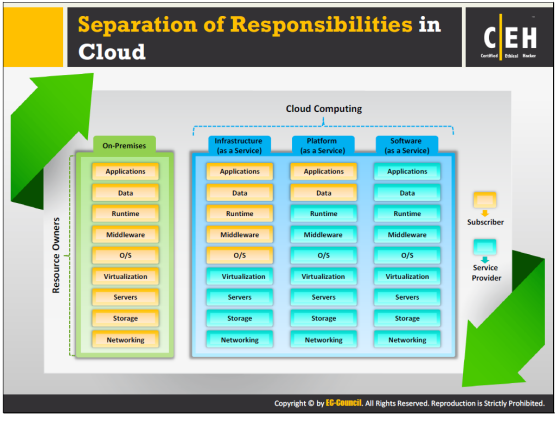
This type of cloud computing service offers application software to subscribers on demand over the Internet; the provider charges for it on a pay-per-use basis, by subscription, by advertising, or by sharing among multiple users.

Advantages:

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

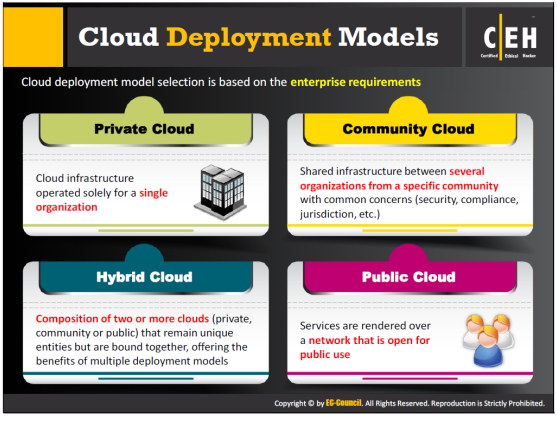
Disadvantages:

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



In cloud computing, separation of subscriber and service provider responsibilities 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: **Infrastructure-as-a-Service** (IaaS), **Platform-as-a-Service** (PaaS), and **Software-as-a-Service** (SaaS). It is important to know the limitations of each cloud service delivery model when accessing specific clouds and their models. The diagram on the slide illustrates the separation of cloud responsibilities specific to service delivery models:



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 common 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 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 private cloud is owned by the organization)
- Sarbanes Oxley, PCI DSS and HIPAA compliance data is much easier to attain

Disadvantages:

- Expensive
- On-site maintenance

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, 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 in the network level may be conflicted as it is 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 datacenters to overcome)
- Complex Service Level Agreements (SLAs)

Community Cloud

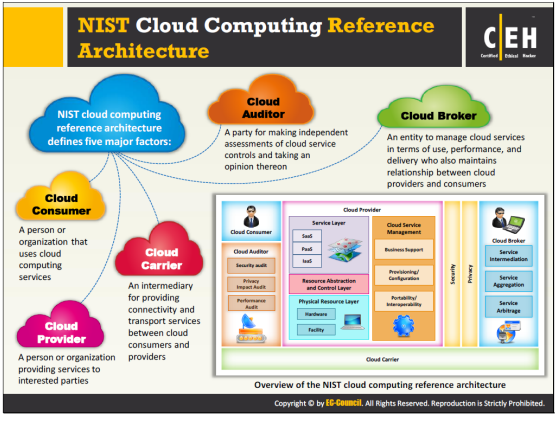
It is a multi-tenant infrastructure shared among organizations from a specific community with common computing concerns such as security, regulatory compliance, performance requirements, and jurisdiction. The community cloud can be either on-premises or off-premises, and governed by the organizations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



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

The five major actors are:

- **Cloud consumer**

  A cloud consumer is a person or organization that maintains business relationship with, and uses cloud computing services from cloud service providers. The cloud consumer browses the CSP's service catalogue 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 specify limitations and obligations if any that cloud consumer must accept.

  Services available to a cloud consumer in **SaaS**, **PaaS**, and **IaaS** 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 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 review of objective evidence. A cloud auditor can evaluate the services provided by a cloud provider in terms of 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 complex 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 in terms of use, performance, and delivery, and maintains the relationship between CSPs and cloud consumers.

Cloud brokers provide services in three categories:

- **Service Intermediation**

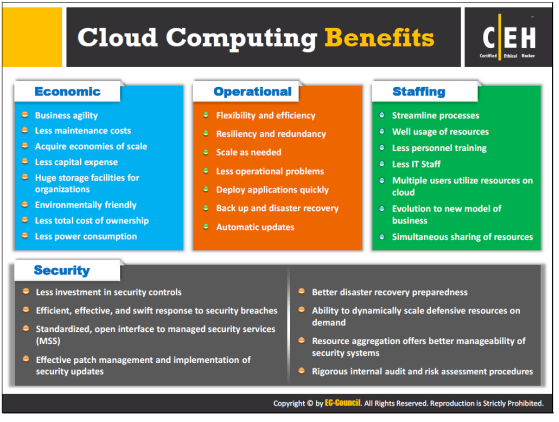
  Improves a given service by a specific capability and provides value-added services to cloud consumers

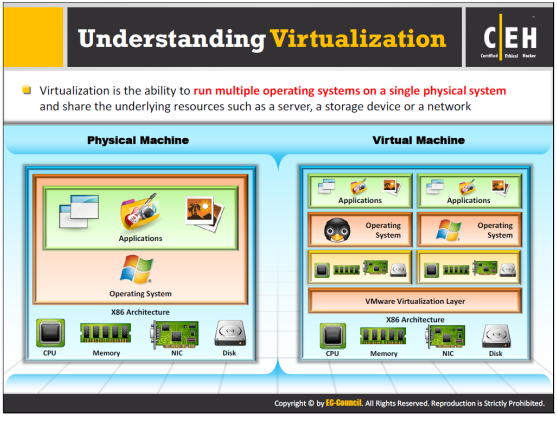
- **Service Aggregation**

  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 flexibility to choose services from multiple agencies)





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 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

Characteristics of virtualization in cloud computing technology:

- **Partitioning**

  The cloud supports many applications and multiple operating systems 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 one can identify it based on its service. Encapsulation protects each application from interfering with other applications.

Types of virtualization:

Storage Virtualization

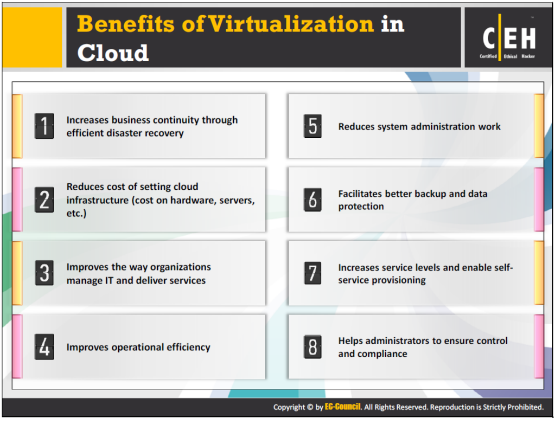
- It combines storage devices from multiple networks into a single storage device and helps in:
  - Expanding the storage capacity
  - Making changes to store configuration easy

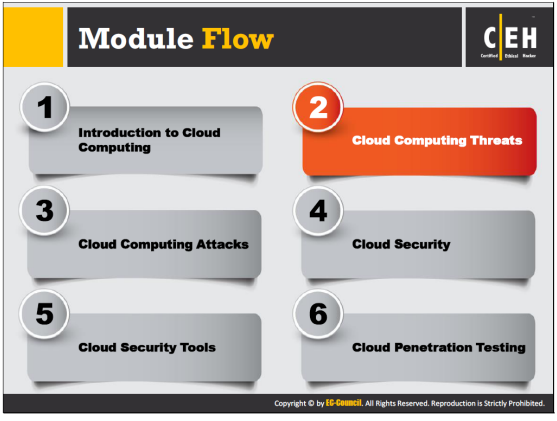
Network Virtualization

- 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





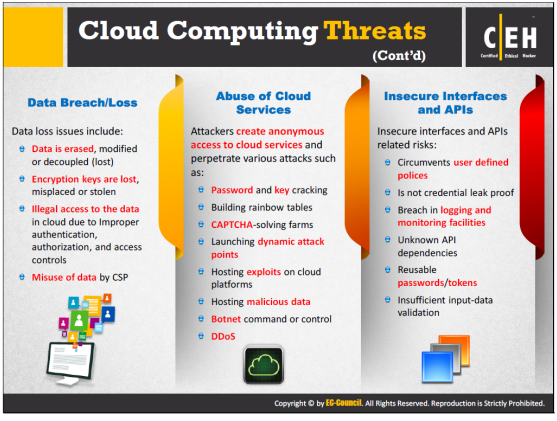
Most organizations adapt the cloud technology, as it reduces the cost via optimized and efficient computing. Tough cloud technology offers different types of services to end users, many people are concerned about critical cloud security risks and threats, which an attacker may take as an advantage to compromise data security, gain illegal access of network, and so on.

This section deals with major security threats and vulnerabilities affecting cloud systems.

Cloud Computing Threats

CEH Certified Ethical Hacker

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



Data Breach/Loss

Improperly designed cloud computing environment with multiple clients is at greater risk to data breach as a flaw in one client's application cloud allow attackers to access other client's data. Data loss or leakage is highly dependent on cloud architecture and its operation.

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 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.

Countermeasures:

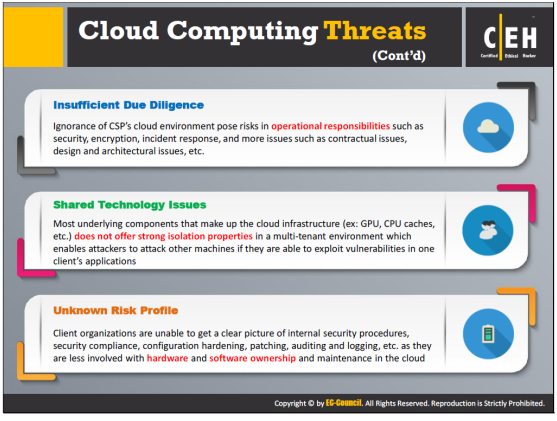
- Implement strong registration and validation process
- Monitor the client's traffic for any malicious activities

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.

Countermeasures:

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



Discussed below are some additional threats to cloud computing:

Insufficient Due Diligence

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 strong isolation properties in a multi-tenant environment. 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 strong authentication and access control for administrative access and operations

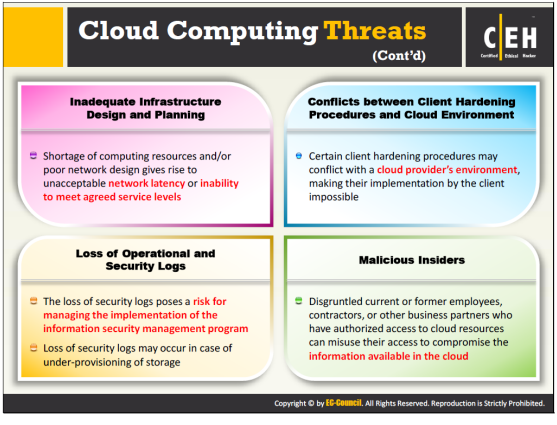
- Enforce service level agreements for patching and vulnerability remediation
- Conduct vulnerability scanning and configuration audits

Unknown Risk Profile

Software updates, threat analysis, intrusion detection, security practices, and others determine security posture of an organization. Organizations are unable to provide a clear picture on level of security, 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
- Partial/full disclosure of infrastructure details (e.g., patch levels, firewalls)
- Monitoring and alerting on necessary information



Some additional threats to cloud computing are:

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 restoring processes, and availability periods.

At times, cloud service providers may not satisfy the rapid rise in demand due to shortage of computing resources and/or poor network design (e.g., traffic flows through a single point, even though 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 by the client impossible. The reason for this is that, because a cloud is a multi-tenant environment, the colocation of many customers certainly 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 difficult to evaluate operational variables. The options for solving issues are limited when no data is available for analysis. Loss of security logs may occur in case of under-provisioning of storage.

Countermeasures:

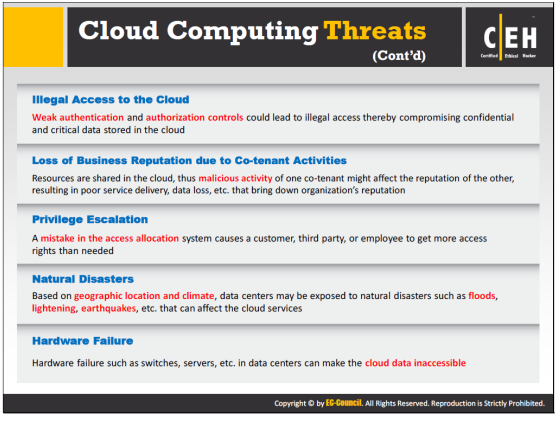
- Implement effective policies and procedures
- Monitor operational and security logs on regular basis

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. 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 into overall information security and management practices, as well as compliance reporting
- Determine security breach notification processes



Additional threats to cloud computing are:

Illegal Access to the Cloud

Countermeasures:

- Enforce strong 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.

Countermeasure:

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

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 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

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.

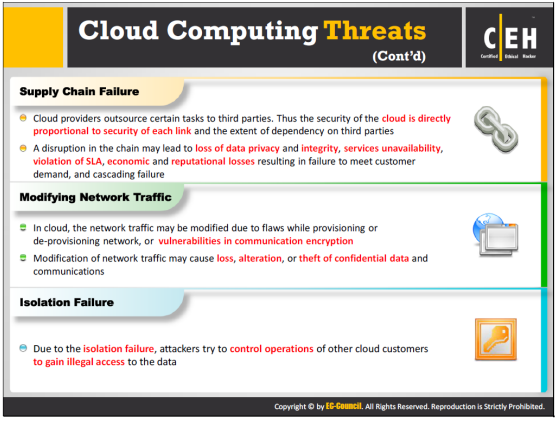
Countermeasures:

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

Natural Disasters

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



Additional threats to cloud computing are:

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.

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 who offers information on the security posture of counterparties

Modifying Network Traffic

This threat arises because of user-provisioning and de-provisioning vulnerabilities, communication encryption vulnerabilities, and so on.

Countermeasure:

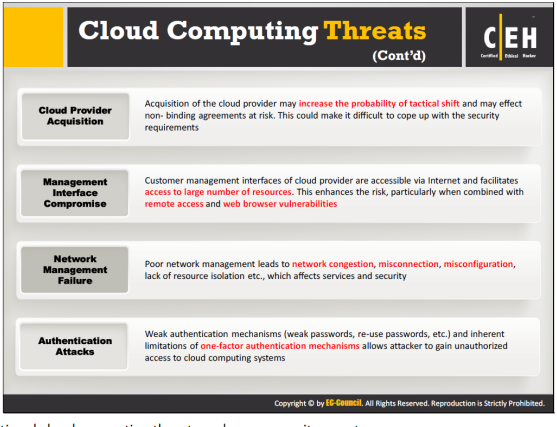
- Perform network traffic analysis using tools to find abnormalities, if any

Isolation Failure

Multi-tenancy and shared resources are the characteristics of cloud computing. Strong isolation or compartmentalization of storage, memory, routing, and reputation between 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



Additional cloud-computing threats and some security countermeasures are:

Cloud Provider Acquisition Countermeasure:

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

Management Interface Compromise Countermeasures:

This threat arises due to the improper configuration, system and application vulnerabilities, remote access to the management interface, and so on.

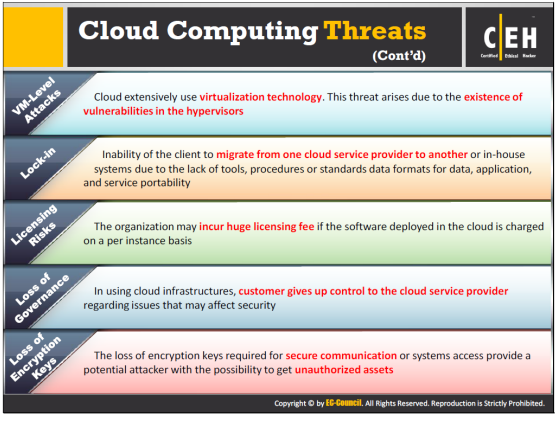
- Use secure protocol to provide access in order to mitigate threats arising because of remote access
- Regularly update the patches for web browser vulnerabilities

Network Management Failure Countermeasures:

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

Authentication Attacks Countermeasures:

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



Additional threats to cloud computing are:

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

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 huge 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. In addition, 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 audit, and others.

Loss of governance results in not complying with security requirements, lack of confidentiality, integrity, and availability of data, poor performance and quality of service, and so on.

Countermeasure:

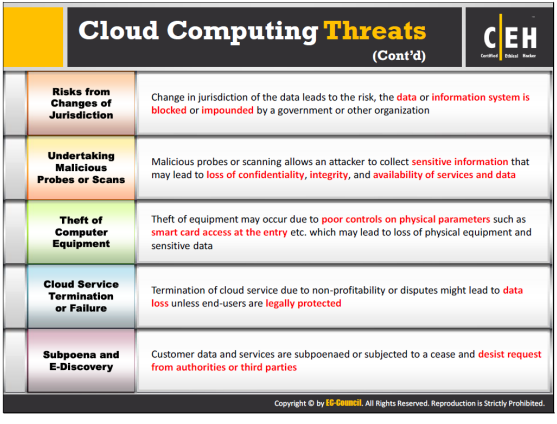
- Workout persistent and careful efforts for execution of service-level agreements (SLA)

Loss of Encryption Keys

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 DES to generate keys



Additional threats to cloud computing are:

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 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. 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

Countermeasure:

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

Theft of Computer Equipment

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, quality of service, and so on. Furthermore, failures in the services outsourced to the CSP may affect cloud customers' ability to meet its duties and commitments to its own customers.

Countermeasure:

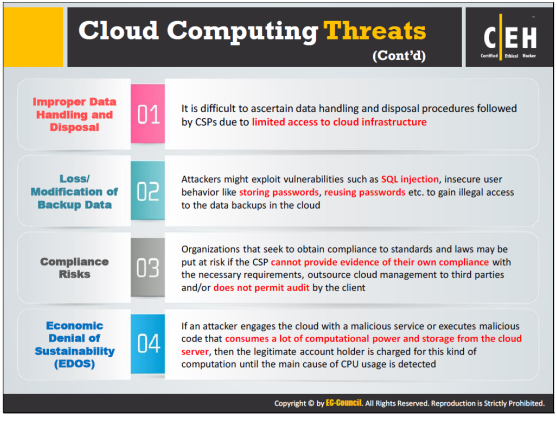
- Ensure that the cloud providers define clear and auditable procedures for termination of the service. This includes how the cloud provider will transfer data back to the customer and guarantee that all data is disposed of securely, according to the terms of agreement.

Subpoena and E-Discovery

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



Additional threats to cloud computing are:

Improper Data Handling and Disposal

When clients request data deletion, a result could be that the data is not truly wiped:

- 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 clients data and ensure that data is completely removed from the main 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

This threat is due to the lack of governance over audits and industry standard assessments. Thus, clients are not aware into 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

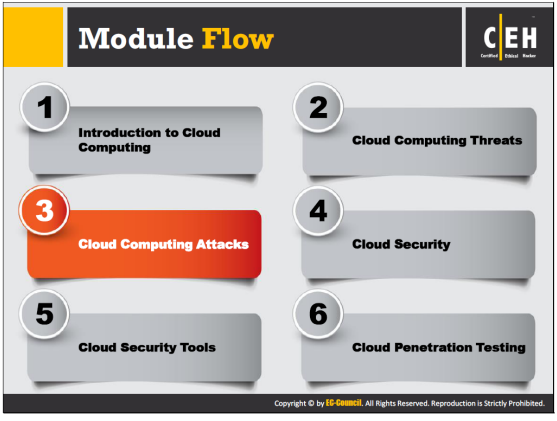
Economic Denial of Sustainability (EDoS)

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 economic resources; in the worst case, this could lead to customer bankruptcy or other serious economic impact.

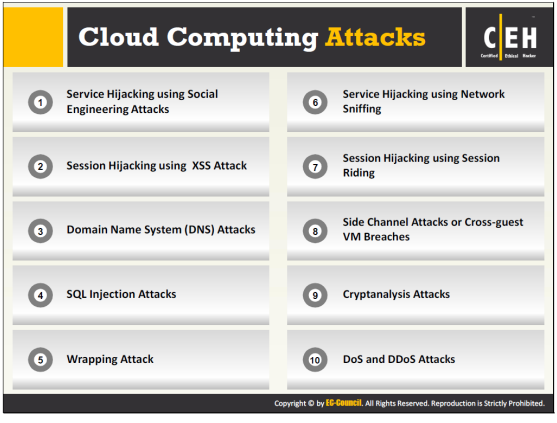
Countermeasure:

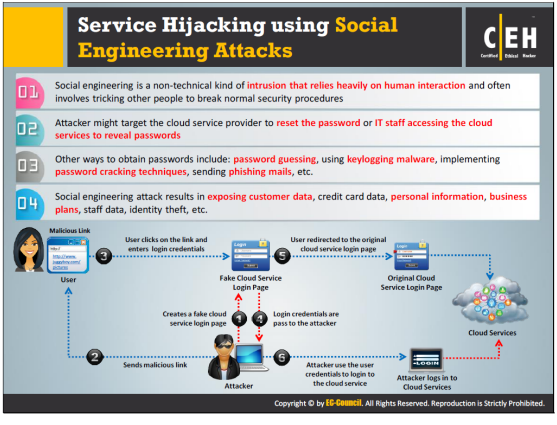
- Use a reactive/on-demand, in-cloud **eDDoS mitigation service** (scrubber Service) to mitigate application- and network-layer DDoS attacks, making use of the client-puzzle approach



Though most organizations adopt cloud technologies, as they offer a wide variety of services with cost reduction, security is the biggest 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 various types of attacks on cloud systems.





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.

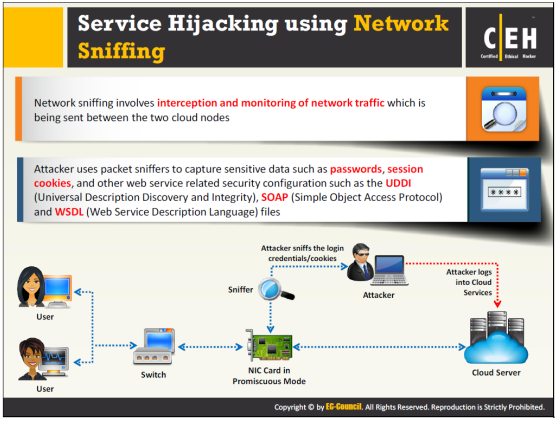
Social engineering is a nontechnical kind of intrusion that relies heavily on human interaction and often involves tricking others into break normal security procedures. Attackers might target cloud service providers to reset passwords, or IT staff to access their cloud services to reveal passwords.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

In the diagram above, the attacker first creates a fake cloud service login page and then 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 login 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 strong 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 across all security layers for others



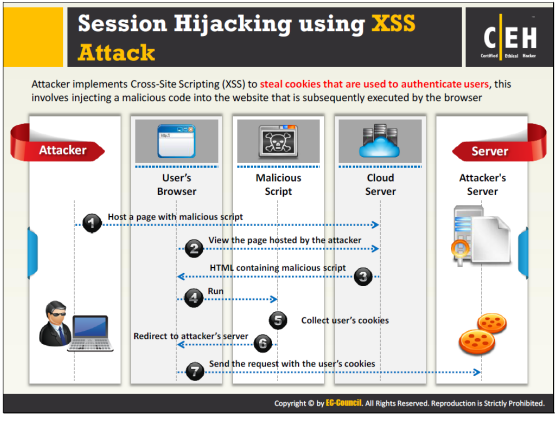
Network sniffing involves interception and monitoring of network traffic sent between two cloud nodes. Unencrypted sensitive data (such as login credentials) during transmission across a network is at greater risk.

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. 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



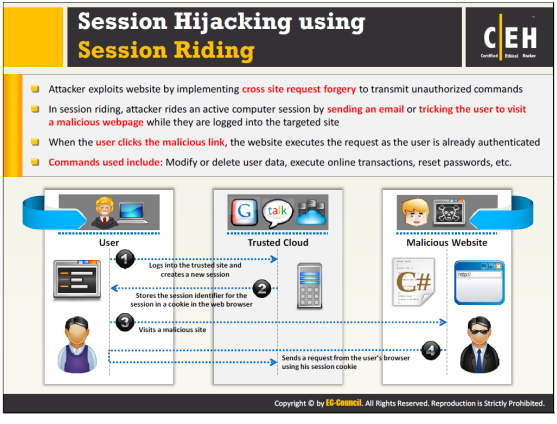
An attacker implements cross-site scripting (XSS) to steal cookies used in user authentication process; this involves injecting a malicious code into the website. Using the stolen cookies attacker exploits active computer sessions, thereby gaining unauthorized access to the data.

Note: Attacker can also predict or sniff session IDs.

In the diagram above, attacker hosts a web page with 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

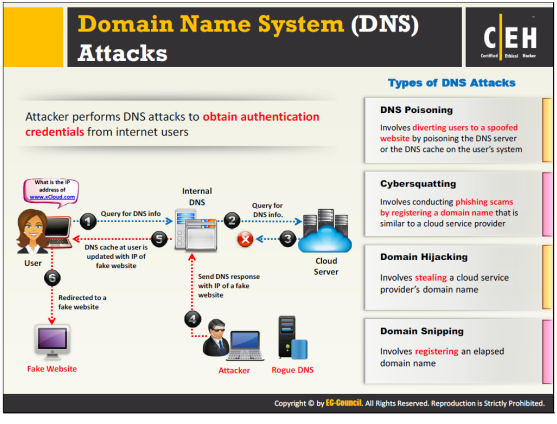


Attackers exploit websites by engaging in cross-site request forgeries to transmit unauthorized commands. In session riding, attackers "ride" an active computer session by sending an email or tricking users to visit a malicious webpage, during login, to an actual target site. When users clicks the malicious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

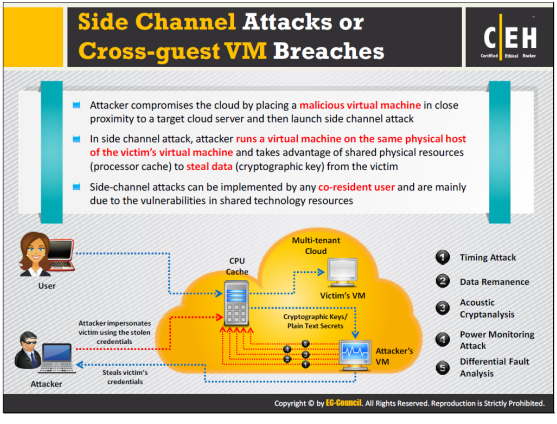


A domain name system (DNS) server translates a human readable domain name (e.g., www.google.com) into a numerical IP address that routes communications between nodes. The attacker performs DNS attacks to obtain authentication credentials from Internet users.

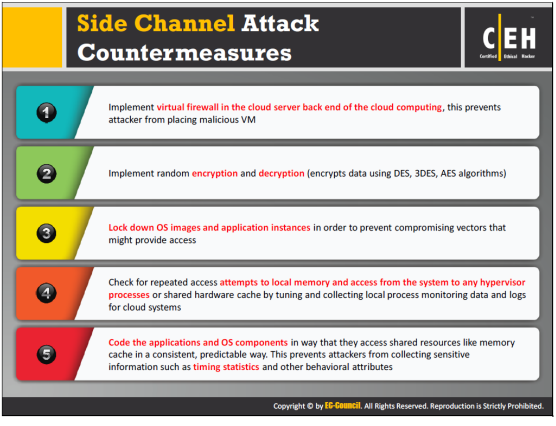
In the diagram above, the attacker performs DNS cache poisoning, directing users to a fake website. Here, the user queries the internal DNS server for DNS information (e.g., What is the IP address of www.xCloud.com?). The internal DNS server then queries the respective cloud server for DNS information. 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 fake website and automatically directs the user to the fake website.

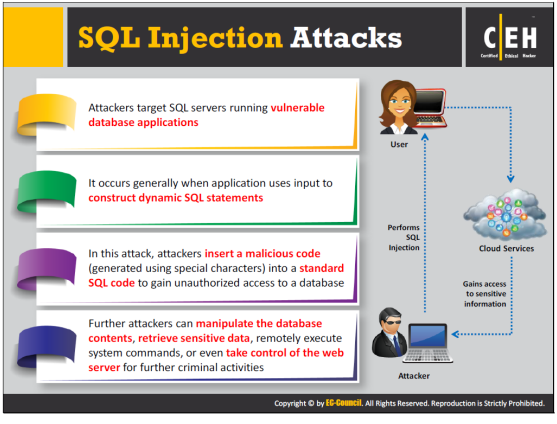
Countermeasures:

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



In the diagram above, an attacker compromises the cloud by placing his/her malicious virtual machine (VM) in close proximity to a target cloud server. He/she 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.





Structured Query Language (SQL) is a programming language meant for database management systems. In SQL injection attack, 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.

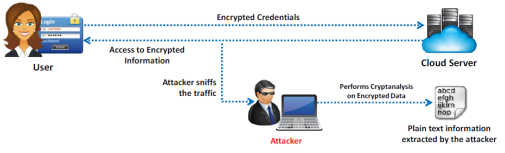
In the diagram above, the attacker performs SQL injection on the cloud web application accessed by the user and gains access to the sensitive information hosted on the cloud.

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

Cryptanalysis Attacks

- **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 (ex: weak random number generation) might turn strong encryption to weak or broken, also there exists 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**



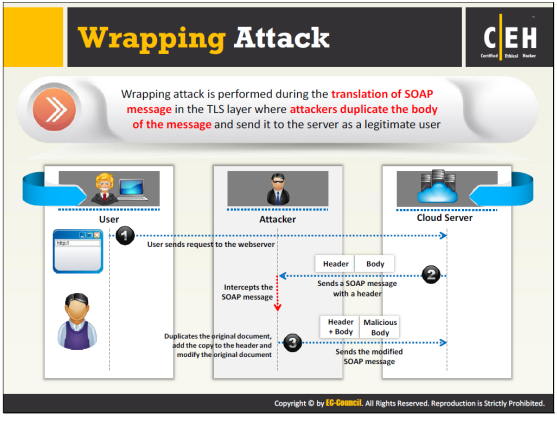
Cryptanalysis Attack Countermeasures

1

Use **Random Number Generators** that generate cryptographically strong random numbers to provide robustness to cryptographic material like Secure shell (**SSH**) keys and Domain Name System Security extensions (**DNSSEC**)

2

Do not use faulty **cryptographic algorithms**



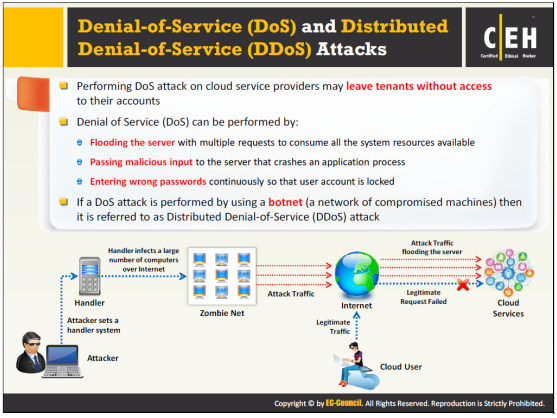
When users send a request from their VM through a browser, the request first reaches a web server, which generates a SOAP message containing structural information, which it will exchange with the browser during message passing. Before message passing occurs, the browser needs to sign the XML document and canonicalize it. In addition, 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 checks its integrity. As a result, the adversary is able to intrude in the cloud and can run malicious code to interrupt the usual functioning of the cloud servers.

In the diagram above, user sends a request to the cloud webserver. 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



Performing 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 generates bogus data that could be resource requests or a type of code that can run in applications of legitimate users.

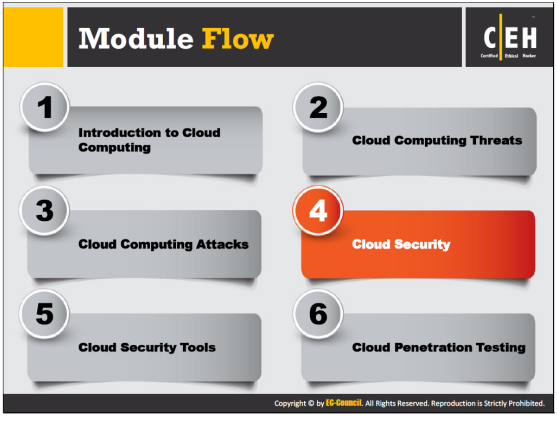
Computing such malware requests engages a server's CPU, memory, and all other devices. Once the server reaches its threshold limit, it starts offloading its jobs to another nearest specific server. The same happens to other inline servers, and finally, the attacker will succeed in engaging the whole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

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

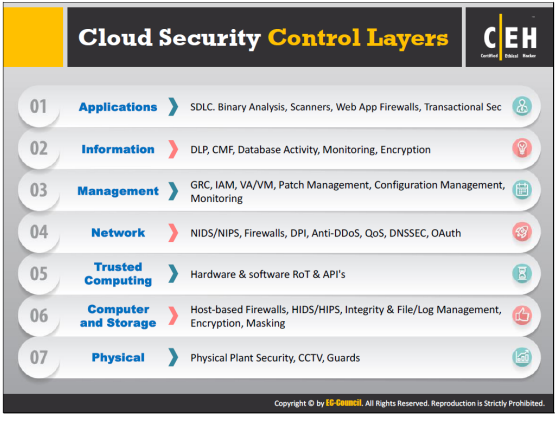
Countermeasures:

- 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



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.



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 web application. It should meet and comply with appropriate regulatory and business requirements.

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.

Management Layer:

This layer covers the cloud security administrative tasks, which can facilitate continued, uninterrupted, and effective services of cloud. Cloud consumers should look for the above mentioned policies to avail better services.

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.

Trusted Computing:

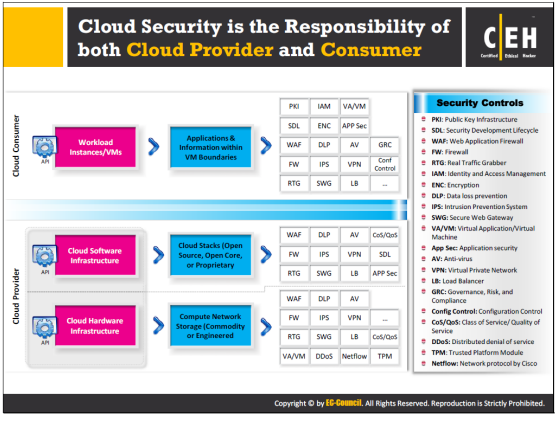
Trust computing defines secured computational environment that implements internal control, auditability, and maintenance to ensure availability and integrity of cloud operations.

Computation and Storage:

In cloud due to the lack of physical control of the data and the machine, the service provider may not be able to manage the data and computation well managed and lose 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 meets with statutory, regulatory, contractual, or business requirements and compliance.

Physical Layer:

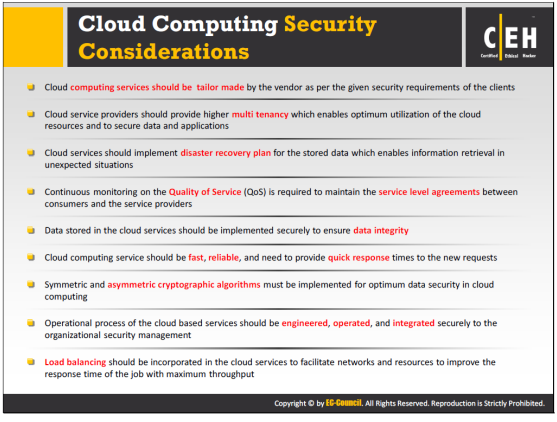
This layer includes security measures for cloud infrastructure, data centers, and physical resources. Security entities that come under this perimeter are fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, security patrols, and so on.

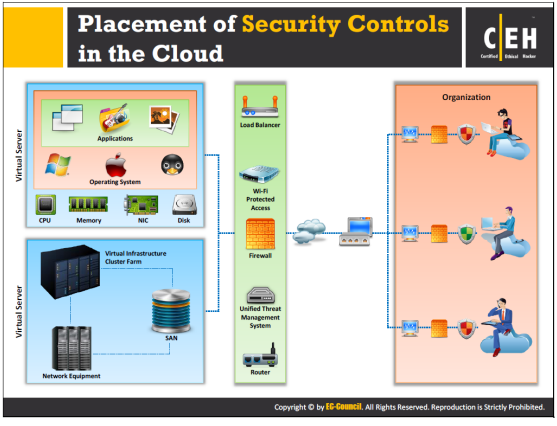


Security is a shared responsibility in cloud systems, in which both cloud consumers and cloud service providers have varying levels of control over available computing resources. Compared to traditional IT systems, in which a single organization has authority over the complete stack of computing resources 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.





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 implementations are in place, for the cloud security architecture to be effective. Many security controls exists that when put in proper place will safeguard any vulnerabilities in the system and reduces the effect of an attack.

Categories of security controls:

- **Deterrent controls** – these controls reduces attacks on the cloud system.

  Example: warning sign on fence or a property to inform adverse consequences for potential attackers if they proceed to attack.

- **Preventive controls** – these controls strengthens the system against incidents, probably by minimizing or eliminating vulnerabilities.

  Example: Strong authentication mechanism to prevent unauthorized usage of cloud systems.

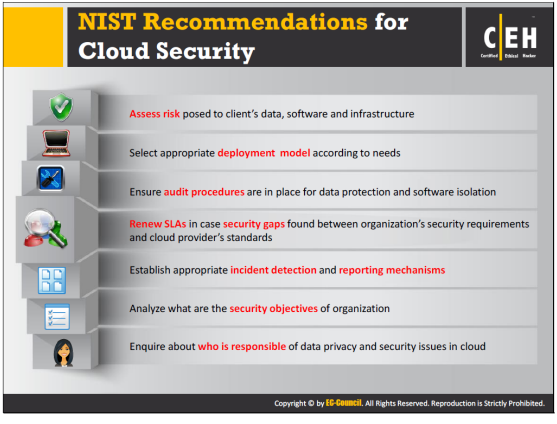
- **Detective controls** – these controls detects and reacts appropriately to the incidents that happen.

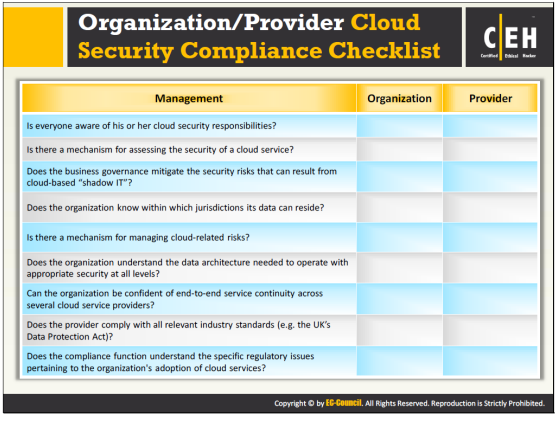
  Example: Employing IDSs, IPSs, etc. helps to detect attacks on cloud systems

- **Corrective controls** – these controls minimizes the consequences of an incident, probably by limiting the damage

  Example: Restoring system backups

Adopting cloud technology has both benefits as well as security risks. Although there is no perfect remedy or solution to secure the cloud environment, implementing best practices could protect data in cloud to a considerable extent.





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?	❑
If the organization's security policies consider the cloud infrastructure?	❑
If security team has ever been involved in implementing cloud infrastructure?	❑
If organization has defined security assessment procedures for cloud infrastructure?	❑
If organization has ever been audited for cloud security threats?	❑
If the organization's cloud adoption will be in compliance with the security standards that organization follows?	❑
Has security governance been adapted to include cloud?	❑
If the team has adequate resources to implement cloud infrastructure and security?	❑

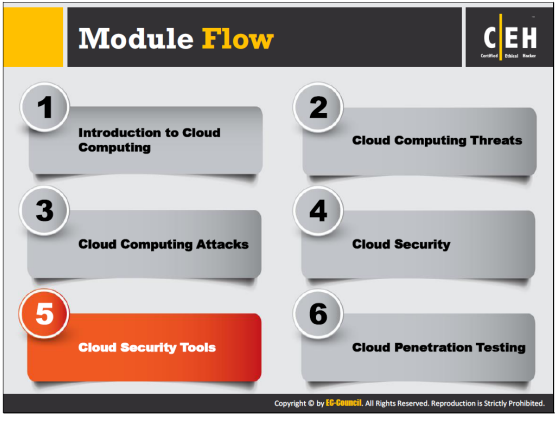
TABLE 17.1: Checklist to determine if the security team is fit and ready for cloud security

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

TABLE 17.2: Checklist to determine if the organization/provider is fit and ready for cloud security based on its operations

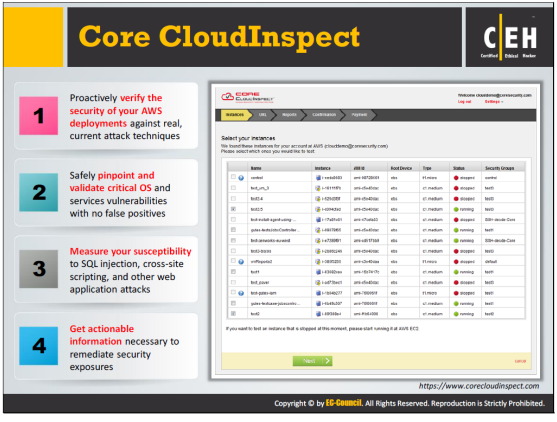
Technology	Organization	Provider
Are there appropriate access controls (e.g. federated single sign-on) that give users controlled access to cloud applications?	❑	❑
Is data separation maintained between the organization's information and that of other customers of the provider, at runtime and during backup (including data disposal)?	❑	❑
Has the organization considered and addressed backup, recovery, archiving and decommissioning of data stored in a cloud environment?	❑	❑
Are mechanisms in place for authentication, authorization, and key management in a cloud environment?	❑	❑
Are mechanisms in place to manage network congestion, misconnection, misconfiguration, lack of resource isolation etc., which affects services and security?	❑	❑
Has organization implemented sufficient security controls on the client devices used to access the cloud?	❑	❑
Are all cloud-based systems, infrastructure, and physical locations suitably protected?	❑	❑
Are the network designs suitably secure for the organization's cloud adoption strategy?	❑	❑

TABLE 17.3: Checklist to determine if the organization/provider is fit and ready for cloud security based on its technology



Tough migrating to cloud has enormous benefits, security issues are the major 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 Core CloudInspect, CloudPassage Halo, and Symantec O3.



Core CloudInspect helps validate when your 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

Source: *https://www.corecloudinspect.com*

The CloudPassage Halo software-defined security (SDSec) platform was purpose-built to protect private clouds, public IaaS, and hybrid/multi-cloud infrastructure. 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 operating system 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 constantly monitoring for unauthorized or malicious changes to important 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 your cloud deployments and lets you integrate your security platform with your other systems.

Source: *http://www.cloudpassage.com*

Discussed below are a few more cloud security tools with which one can secure data hosted on cloud systems:

Alert Logic

Source: *https://www.alertlogic.com*

Alert Logic solutions specially built only for the cloud, with a multi-tenant architecture and scalable platform that enables integration of security and compliance solutions for organizations transitioning to the cloud. It offers solutions such as intrusion detection, vulnerability scanning, log management, and web-application firewall.

SecludIT

Source: *http://secludit.com*

SecludIT has developed a set of products and services specifically designed to help cloud infrastructure providers and business-critical cloud users to safely move towards cloud technologies adoption. The core service provided is Elastic Detector, which offers a comprehensive and dynamic view of cloud infrastructure to identify security vulnerabilities affecting networks, servers, applications, and data availability.

Dell Cloud Manager

Source: *http://www.enstratius.com*

Dell Cloud Manager (formerly Enstratius) enables deployment and management of enterprise-class applications across private, public and hybrid clouds. It provides a suite of tools for

managing cloud infrastructure, including the provisioning, management, and automation of applications across the leading private and public cloud platforms.

Nessus Enterprise for AWS

Source: http://www.tenable.com

Nessus Enterprise for AWS is purpose-built for and deployed in the AWS (Amazon Web Services) cloud. It is pre-authorized to scan AWS instances for vulnerabilities, advanced threats, web application security, and compliance violations.

Qualys Cloud Suite

Source: https://www.qualys.com

The Qualys Cloud Platform consists of a suite of IT security and compliance solutions that leverage shared and extensible core services and a highly scalable multi-tenant cloud infrastructure. It enables organizations to simplify the process and reduce the cost of securing their IT assets and achieving compliance with internal policies and external regulations.

Trend Micro's Instant-On Cloud Security

Source: http://www.trendmicro.com

For Amazon Web Services (AWS) customers, protecting EC2 instances is a shared responsibility. Customers running workloads on AWS potentially face additional security and compliance requirements to protect their applications and data. Trend Micro's Instant-On Cloud Security supports the AWS environment to address those security needs.

Features:

- Prevent data breaches and business disruptions
- Maximize operational cost reductions with AWS
- Achieve cost-effective compliance

Symantec O3

Source: http://www.symantec.com

Symantec O3 is a cloud information protection platform that provides three layers of protection for the cloud: identity and access control, information security and information management. It helps organizations with a context-aware, policy-driven layer to protect cloud users, applications, and information.

Cloud Application Visibility

Source: http://www.zscaler.com

One requires cloud application visibility—to see what employees are doing; require the ability to set acceptable usage policy—to ensure regulatory and corporate compliance; and cloud application security—to protect against advanced threats.

Porticor

Source: *http://www.porticor.com*

Porticor infuses trust into the cloud with secure, easy to use, and scalable solutions for data encryption and key management. It enables companies to safeguard their data, comply with regulatory standards, and streamline operations. It combines state of the art encryption with patented key management to protect critical data in public, private and hybrid cloud environments.

Panda Cloud Office Protection

Source: *http://www.cloudantivirus.com*

Panda Cloud Office Protection is cloud-based antivirus and endpoint protection that helps to forget security – complexity, overhead, and threats.

Features:

- **Maximized Protection**

  Provides protection for files, emails, HTTP/FTP, downloads, and instant messaging

- **Continuous Updates**

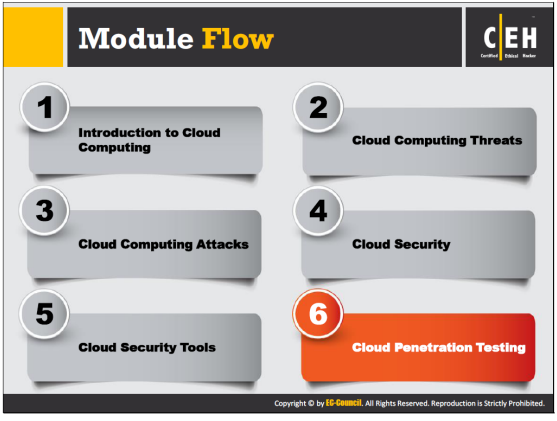
  Ensures protection against the latest threats by continuously updating security signatures

- **No System Slowdowns**

  Transfers most of the processor-intensive activities to the cloud, reducing systems slowdowns

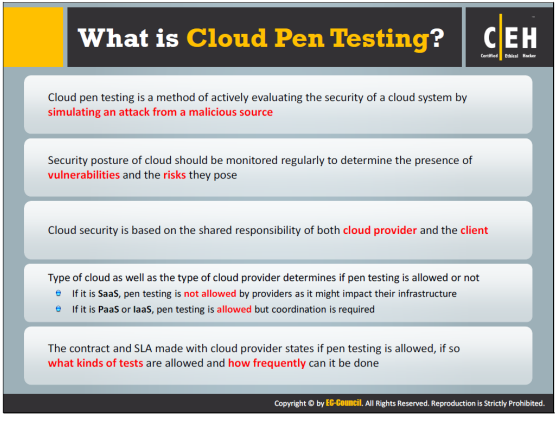
- **No Servers or VPNs**

  Enables management of endpoint protection using a standard web browser, eliminating the need for antivirus server infrastructure and VPNs



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, an others. Black box pen testing (i.e., testing the cloud infrastructure without prior knowledge of the cloud administrators) is most effective way of assessing security posture of a cloud service provider.

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



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 by means of automated software applications such as Core CloudInspect, CloudPassage Halo, Alert Logic, and SecludIT.

Pen testing cloud involves three phases:

- **Preparation**

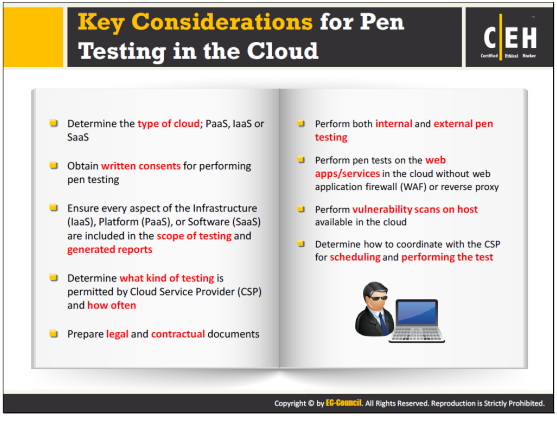
  It involves signing formal agreements to ensure protection of both parties (Cloud Service Provider [CSP] and client). It defines the policy and course of action the CSP and client should take in finding potential vulnerabilities and their mitigation. Pen testing also consider other users who might be using the same infrastructure under testing.

- **Execution**

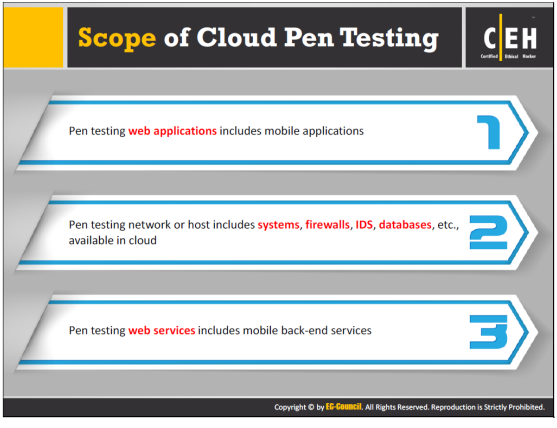
  It involves executing the cloud pen-testing plan to find out potential vulnerabilities, if any, existing in the cloud.

- **Delivery**

  Once cloud pen testing is complete, document all the exploits/vulnerabilities in it, and hand over the document to the provider to take whatever action is necessary.

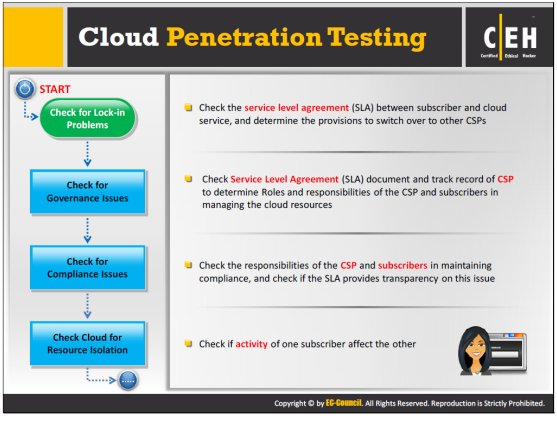


Most organizations around the world—small and large—are adopting cloud services to handle business-critical data. Tough cloud technology offers many benefits such as improved efficiency, reduced costs, improved accessibility, and flexibility. There also exists many security risks such as issues with 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.



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



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 to resources outside the cloud
- Source escrow agreement
- Vulnerability assessment process
- Certification schemes adapted to cloud infrastructures
- Jurisdictions over CSP for SLA related issues

- Completeness and transparency in terms of use
- Cloud asset ownership

Step 3: Check for Compliance Issues

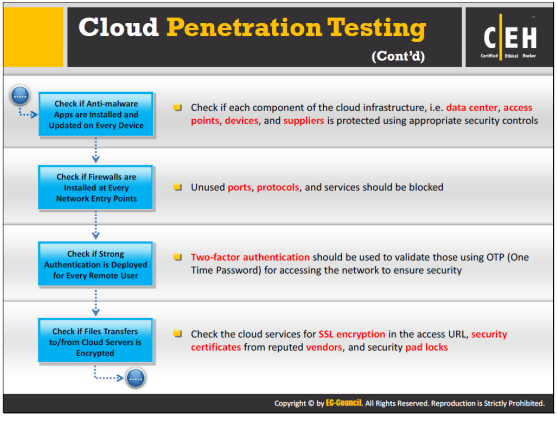
Cloud compliance issues arise from the use of cloud storage or backup services. Recommendations to check for compliance issues include:

- Compliance to 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

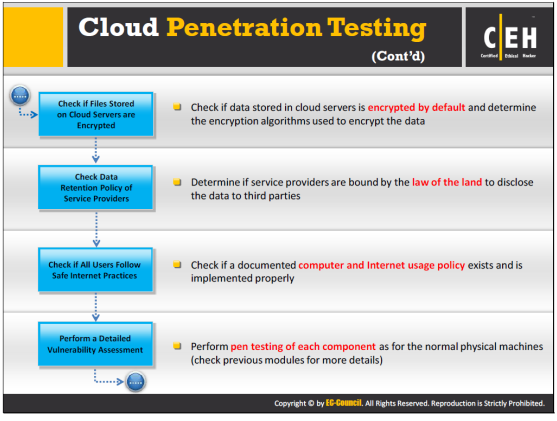
- Check whether the firewalls are installed at every network entry point
- Unused ports, protocols, and services should be blocked

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 in nature
- 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 pad locks
- 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 data stored in cloud servers is encrypted by default 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

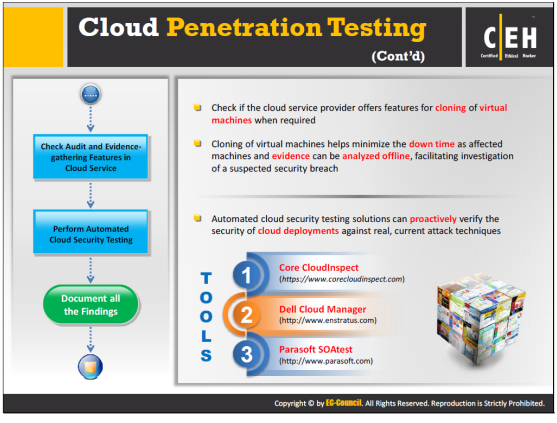
Step 11: Check whether All Users Follow Safe Internet Practices

- 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 down time 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:

  - **Core CloudInspect**

    Source: *https://www.corecloudinspect.com*

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

- **Dell Cloud Manager**

  Source: *http://www.enstratus.com*

  Dell Cloud Manager provides cloud governance, automation, and independence for enterprises. It supports the provisioning, management and automation of applications in all public and private clouds. Dell Cloud Manager is available as Software as a Service, or as on-premises software that enables you to control the cloud from within your own data centers.

  Dell Cloud Manager provides:

  - **Governance** – enables you to meet your governance needs with flexible access controls, logging, financial controls, and integration into the internal management systems and access directories.
  - **Automation** – helps to meet the economic and operational advantages of cloud computing through a variety of automation tools including auto-provisioning, auto-scaling, automated backups, etc.
  - **Independence** – supports over 20 of the public clouds and private cloud platforms.

- **Parasoft SOAtest**

  Source: *http://www.parasoft.com*

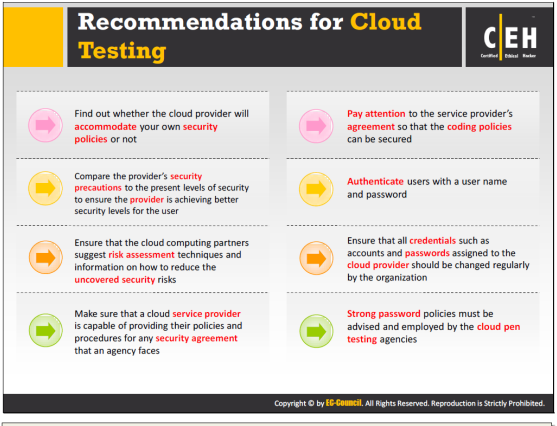
  Parasoft SOAtest automates web application testing, message/protocol testing, cloud testing, security testing, and application behavior virtualization. Parasoft SOAtest and Parasoft Load Test (packaged together) ensure secure, reliable, compliant business processes.

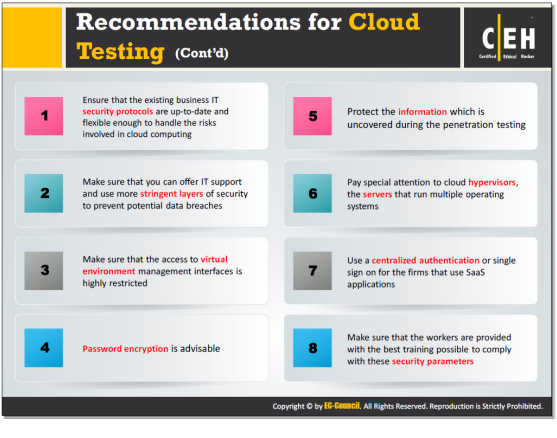
  Parasoft SOAtest provides an integrated solution for the following:

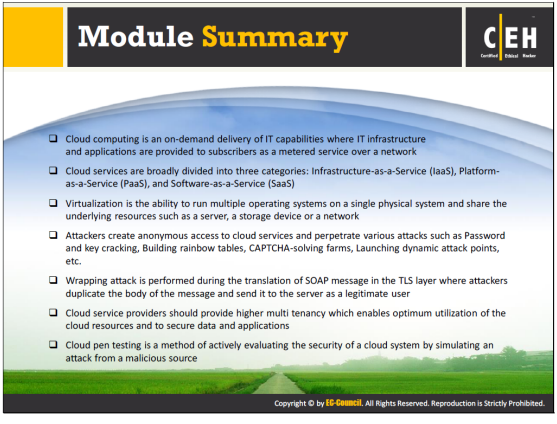
  - End-to-end testing
  - Environment management
  - Quality governance
  - Process visibility and control

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 in order to reduce the risk of security compromise to an acceptable level.







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.