Security Issues and Challenges in Cloud Computing

What is cloud computing?

- It is an internet based computing where all the shared resources ,software and information are provided to the computers and devices on demand.

- Users can access the information from anywhere and anytime

Features of cloud computing

- On demand-self service
- Broad Network access
- Resource pooling
- Rapid elasticity
- Measured service
- pricing

Types of clouds

- Private cloud

  --The cloud is managed by an organization and serve it solely.

- Public cloud

  --The cloud infrastructure is owned and managed by a large Cloud Service Provider (CSP).

- Community cloud

  --The cloud is managed by several organizations and supports a specific community that has the same interest.

- Hybrid cloud

  -- The cloud infrastructure is composed of two or more of the above models

Cloud service models

- **Software as a Service (SaaS):**

  --It offers renting application functionality from a service provider rather than buying, installing and running software by the user.

- **Platform as a Service (PaaS)** :

  --It provides a platform in the cloud, upon which applications can be developed and executed.

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

  -- vendors offer computing power and storage space on demand.

Data Related Security

- **Data Breach**: 1.Confidentiality
  2. Integrity

- **Data Lock in**: Users may lose data if they migrate from one vendor to another vendor.

- **Data Remanence:** It is the residual representation of data that have been nominally erased or removed in some way.

Data Related Security

- **Data Recovery:** Sometimes server may break down and cause damage or loss to users data. To avoid this, data should be backed up to be recovered in future

- **Data Locality:** In SaaS model of cloud environment, the user doesn't know where the data is stored which may be an issue. The issue can be solved by creating secure SaaS model which can provide reliability to the customer on the location of the data of the user.

Application related security issues

- **Cloud malware injection attack:** In this attack a malicious virtual machine or a service implementation is injected into the cloud system. one solution to prevent this is to perform the integrity check to the service instance.

- **Cookie poisoning:** In this an unauthorized access is made into the application by modifying the contents of the cookie. One solution is to clean up the cookie or encrypt the cookie data.

Application related security issues

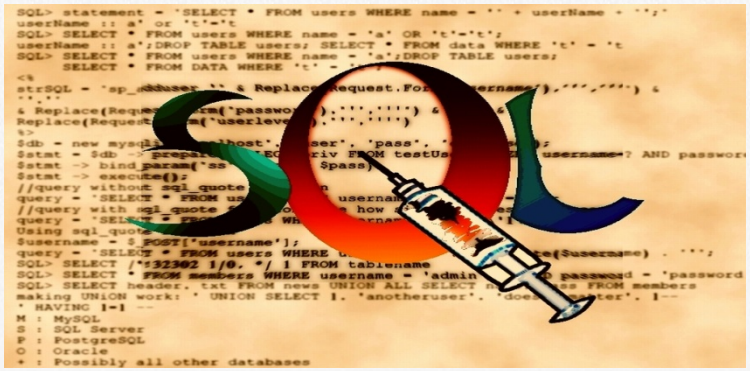
- **Backdoor and Debug Option:** Debug option is for the developers who use it to implement any changes requested at later stage in a website since these debug option provides back entry for the developers, sometimes these debug options are left enabled unnoticed, they may provide easy access to the hackers and allow them to make changes in the website.

- **Hidden Field Manipulation**: Certain fields are hidden in the web-site and is used by the developers. Hacker can easily modify on the web page**.**

CSP level attacks

- **Guest hopping attack:** An attacker will try get access to one virtual machine by penetrating another virtual machine hosted in the same hardware.

- **SQL injection:** It can be done by injecting the SQL commands into the database of an application to crash the database.



CSP level attacks

- **Malicious Insider:** In private cloud, its employee is granted access to the sensitive data of some or all customer administrators. Such privileges may expose information to security threats.

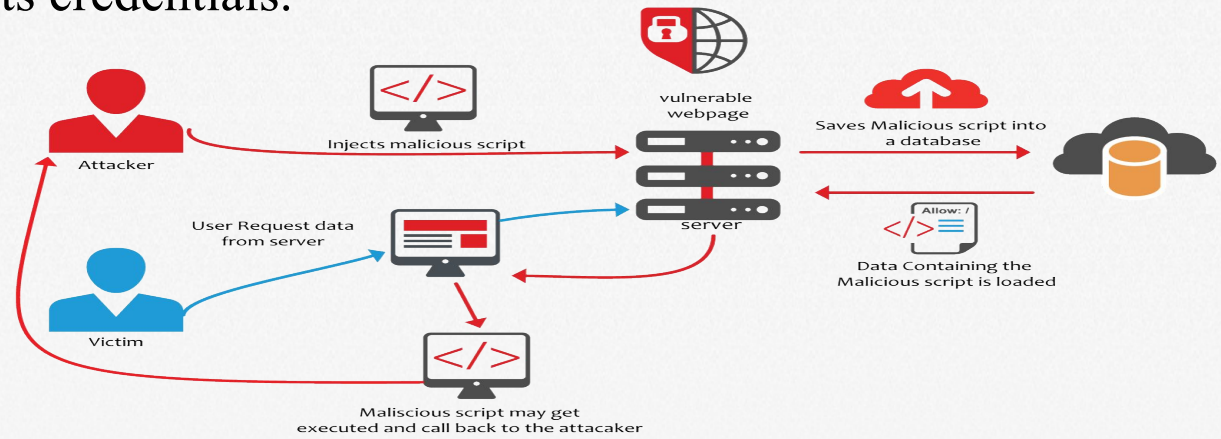
- **Side channel attack:** It occurs when an attacker places a malicious virtual machine on the same physical machine as the victim machine so that he can access all the confidential information on the victims machine.

Network level attacks

- DNS attacks:

Domain hijacking: Domain hijacking is defined as changing the name of a domain without the knowledge or permission from the domain's owner or creator. This enable the intruders to access the sensitive information.

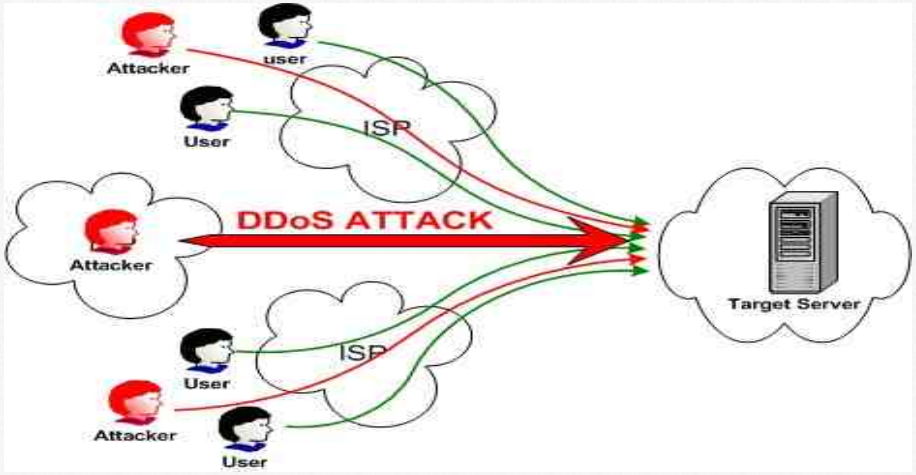
Cross site scripting: It is a type of attack in which user enters right URL of a website and hacker on the other site redirect the user to its own website and hack its credentials.



Network level attacks

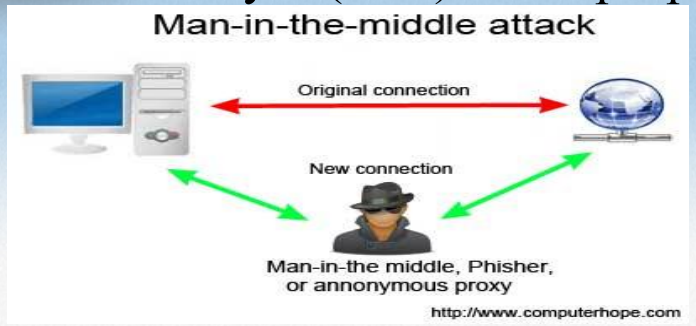
- **IP spoofing:**

  DOS attack: When hackers overflows a network server or web server with frequent request of services to damage the network, the denial of service cannot keep up with them, server could not legitimate client regular requests.

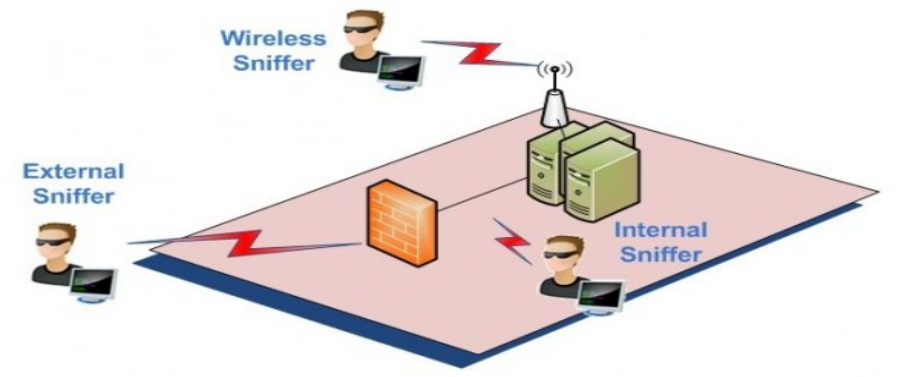


Network level attacks

- **Man in the middle attack:** This is another issue of network security that will happen if secure socket layer (SSL) is not properly configured.



- **Network Sniffing:** Another type of attack is network sniffer, it is a more critical issue of network security in which unencrypted data are hacked through network.



Security requirements for cloud computing

- Identification and Authenticity:
- Authorization
- Non-repudiation
- Availability

Challenges in cloud computing

- Security
- Costing model
- Charging model
- Service level agreement
- Cloud interoperability issue

Thank you