Lecture Schedule 19

Cloud Computing Security and ethical challenges: Computer crime - Hacking

Cloud Computing

Cloud Computing tutorial provides basic and advanced concepts of Cloud Computing. Our Cloud Computing tutorial is designed for beginners and professionals.

Cloud computing is a virtualization-based technology that allows us to create, configure, and customize applications via an internet connection. The cloud technology includes a development platform, hard disk, software application, and database.

The term cloud refers to a network or the internet. It is a technology that uses remote servers on the internet to store, manage, and access data online rather than local drives. The data can be anything such as files, images, documents, audio, video, and more.

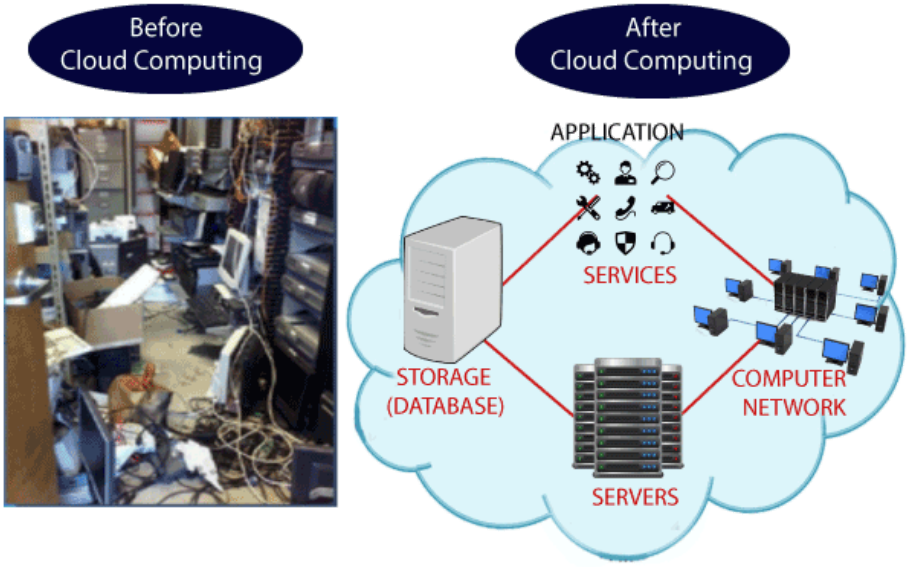
- Developing new applications and services
- Storage, back up, and recovery of data
- Hosting blogs and websites
- Delivery of software on demand
- Analysis of data
- Streaming videos and audios

Why Cloud Computing?

Small as well as large IT companies, follow the traditional methods to provide the IT infrastructure. That means **for any IT company, we need a Server Room that is the basic need of IT companies**.

In that server room, there should be a database server, mail server, networking, firewalls, routers, modem, switches, QPS (Query Per Second means how much queries or load will be handled by the server), configurable system, high net speed, and the maintenance engineers.

To establish such IT infrastructure, we need to spend lots of money. To overcome all these problems and to reduce the IT infrastructure cost, Cloud Computing comes into existence.



Characteristics of Cloud Computing

The characteristics of cloud computing are given below:

1) Agility

The cloud **works in a distributed computing environment**. It shares resources among users and works very fast.

2) High availability and reliability

The availability of servers is high and more reliable because the **chances of infrastructure failure are minimum**.

3) High Scalability

Cloud offers **"on-demand" provisioning of resources on a large scale**, without having engineers for peak loads.

4) Multi-Sharing

With the help of cloud computing, **multiple users and applications can work more efficiently** with cost reductions by sharing common infrastructure.

5) Device and Location Independence

Cloud computing enables the users to access systems using a web browser regardless of their location or what device they use e.g. PC, mobile phone, etc. **As infrastructure is off-site** (typically provided by a third-party) **and accessed via the Internet, users can connect from anywhere**.

6) Maintenance

Maintenance of cloud computing applications is easier, since they **do not need to be installed on each user's computer and can be accessed from different places**. So, it reduces the cost also.

7) Low Cost

By using cloud computing, the cost will be reduced because to take the services of cloud computing, **IT company need not to set its own infrastructure** and pay-as-per usage of resources.

8) Services in the pay-per-use mode

Application Programming Interfaces **(APIs) are provided to the users so that they can access services on the cloud** by using these APIs **and pay the charges as per the usage of services**.

Public clouds

Public clouds are cloud environments typically created from IT infrastructure not owned by the end user. Some of the largest public cloud providers include Alibaba Cloud, Amazon Web Services (AWS), Google Cloud, IBM Cloud, and Microsoft Azure.

Traditional public clouds always ran off-premises, but today's public cloud providers have started offering cloud services on clients' on-premise data centers. This has made location and ownership distinctions obsolete.

All clouds become public clouds when the environments are partitioned and redistributed to multiple tenants. Fee structures aren't necessary characteristics of public clouds anymore, since some cloud providers (like the Massachusettes Open Cloud) allow tenants to use their clouds for free. The bare-metal IT infrastructure used by public cloud providers can also be abstracted and sold as IaaS, or it can be developed into a cloud platform sold as PaaS.

Private clouds

Private clouds are loosely defined as cloud environments solely dedicated to a single end user or group, where the environment usually runs behind that user or group's firewall. All clouds

become private clouds when the underlying IT infrastructure is dedicated to a single customer with completely isolated access.

But private clouds no longer have to be sourced from on-prem IT infrastructure. Organizations are now building private clouds on rented, vendor-owned data centers located off-premises, which makes any location and ownership rules obsolete. This has also led to a number of private cloud subtypes, including:

Managed private clouds

Customers create and use a private cloud that's deployed, configured, and managed by a third-party vendor. Managed private clouds are a cloud delivery option that helps enterprises with understaffed or underskilled IT teams provide better private cloud services and infrastructure.

Dedicated clouds

A cloud within another cloud. You can have a dedicated cloud on a public cloud (e.g. Red Hat OpenShift Dedicated) or on a private cloud. For example, an accounting department could have its own dedicated cloud within the organization's private cloud.

Hybrid clouds

A hybrid cloud is a seemingly single IT environment created from multiple environments connected through local area networks (LANs), wide area networks (WANs), virtual private networks (VPNs), and/or APIs.

The characteristics of hybrid clouds are complex and the requirements can differ, depending on whom you ask. For example, a hybrid cloud may need to include:

- At least 1 private cloud and at least 1 public cloud
- 2 or more private clouds
- 2 or more public clouds
- A bare-metal or virtual environment connected to at least 1 public cloud or private cloud

But every IT system becomes a hybrid cloud when apps can move in and out of multiple separate-yet connected—environments. At least a few of those environments need to be sourced from consolidated IT resources that can scale on demand. And all those environments need to be managed as a single environment using an integrated management and orchestration platform.

Multiclouds

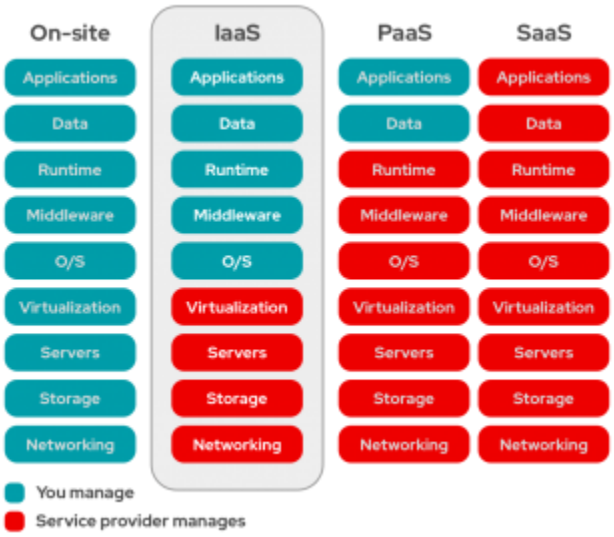
Multiclouds are a cloud approach made up of more than 1 cloud service, from more than 1 cloud vendor—public or private. All hybrid clouds are multiclouds, but not all multiclouds are hybrid clouds. Multiclouds become hybrid clouds when multiple clouds are connected by some form of integration or orchestration.

A multicloud environment might exist on purpose (to better control sensitive data or as redundant storage space for improved disaster recovery) or by accident (usually the result of shadow IT). Either way, having multiple clouds is becoming more common across enterprises that seek to improve security and performance through an expanded portfolio of environments.

Cloud services

Cloud services are infrastructure, platforms, or software that are hosted by third-party providers and made available to users through the internet. There are 3 main types of as-a-Service solutions: IaaS, PaaS, and SaaS. Each facilitates the flow of user data from front-end clients through the internet, to the cloud service provider's systems, and back—but vary by what's provided.

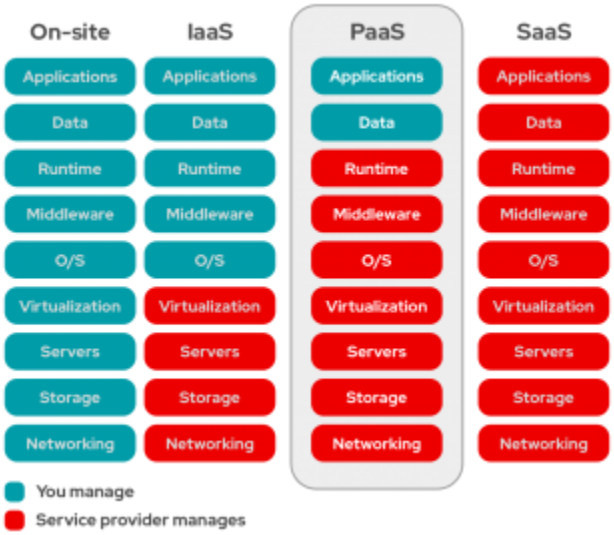
IaaS



IaaS means a cloud service provider manages the infrastructure for you—the actual servers, network, virtualization, and data storage—through an internet connection. The user has access through an API or dashboard, and essentially rents the infrastructure. The user manages things like the operating system, apps, and middleware while the provider takes care of any hardware,

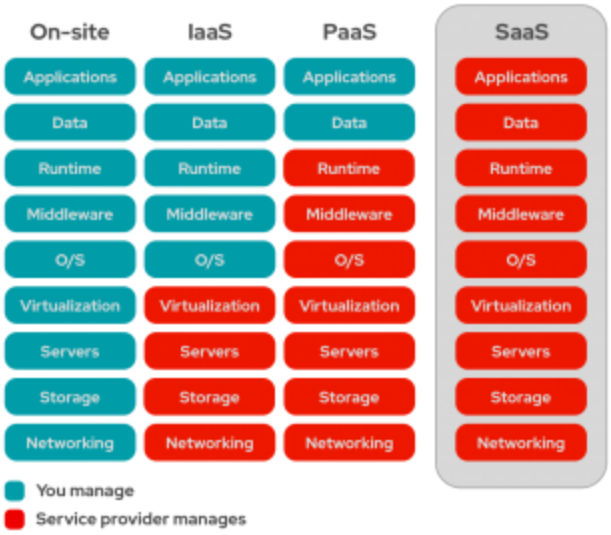
networking, hard drives, data storage, and servers; and has the responsibility of taking care of outages, repairs, and hardware issues. This is the typical deployment model of cloud storage providers.

PaaS



PaaS means the hardware and an application-software platform are provided and managed by an outside cloud service provider, but the user handles the apps running on top of the platform and the data the app relies on. Primarily for developers and programmers, PaaS gives users a shared cloud platform for application development and management (an important DevOps component) without having to build and maintain the infrastructure usually associated with the process.

SaaS



SaaS is a service that delivers a software application—which the cloud service provider manages—to its users. Typically, SaaS apps are web applications or mobile apps that users can access via a web browser. Software updates, bug fixes, and other general software maintenance are taken care of for the user, and they connect to the cloud applications via a dashboard or API. SaaS also eliminates the need to have an app installed locally on each individual user's computer, allowing greater methods of group or team access to the software.

Hacking

Gaining access to a system that you are not supposed to have access is considered as hacking. For example: login into an email account that is not supposed to have access, gaining access to a remote computer that you are not supposed to have access, reading information that you are not supposed to able to read is considered as hacking. There are a large number of ways to hack a system.

In 1960, the first known event of hacking had taken place at MIT and at the same time, the term **Hacker** was organized.

Ethical hacking

Ethical hacking is also known as **White hat Hacking or Penetration Testing**. Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system or data. Ethical hacking is used to improve the security of the systems and networks by fixing the vulnerability found while testing.

Ethical hackers improve the security posture of an organization. Ethical hackers use the same tools, tricks, and techniques that malicious hackers used, but with the permission of the

authorized person. The purpose of ethical hacking is to improve the security and to defend the systems from attacks by malicious users.

Types of Hacking

We can define hacking into different categories, based on what is being hacked. These are as follows:

1. Network Hacking
2. Website Hacking
3. Computer Hacking
4. Password Hacking
5. Email Hacking

1. **Network Hacking:** Network hacking means gathering information about a network with the intent to harm the network system and hamper its operations using the various tools like Telnet, NS lookup, Ping, Tracert, etc.
2. **Website hacking:** Website hacking means taking unauthorized access over a web server, database and make a change in the information.
3. **Computer hacking:** Computer hacking means unauthorized access to the Computer and steals the information from PC like Computer ID and password by applying hacking methods.
4. **Password hacking:** Password hacking is the process of recovering secret passwords from data that has been already stored in the computer system.
5. **Email hacking:** Email hacking means unauthorized access on an Email account and using it without the owner's permission.

Advantages of Hacking

There are various advantages of hacking:

1. It is used to recover the lost of information, especially when you lost your password.
2. It is used to perform penetration testing to increase the security of the computer and network.
3. It is used to test how good security is on your network.

Disadvantages of Hacking

There are various disadvantages of hacking:

1. It can harm the privacy of someone.

2. Hacking is illegal.
3. Criminal can use hacking to their advantage.
4. Hampering system operations.

Computer crime

Computer crime is an act that describes a large category of offenses, which is also known as hi-tech crime, e-crime, cybercrime, or electronic crime. It is performed by a computer user who has great knowledge about hacking. The hacker tries to gain unauthorized access to any particular account, personal information or steals a company's or individual's private information. In some cases, hackers can corrupt the computer or data files that can be very harmful to you.

On the basis of the person, situation, and individual frame of reference, the term computer crime has different meanings. For example, there are different communities like network administrators, private security, law enforcement, or prosecutors, but the investigation of computer crime does not need these communities. However, conventional or physical borders do not restrict computer crime as it is by its very nature.

The first definitional categories for computer crime are presented by Donn Parke, who is generally cited as the author. A higher-level definition to the term computer abuse was described by him, computer crime can be any event involving an planned act where a unauthorize person or offender wants to gain related to computers, but a victim suffered or could have suffered a loss.

Expanding on Parker's definitions Robert Taylor and company describe four major categories of computer crime:

1. **The computer as a target:** Computers can be the target of an illegal activity, which means the attacker has to main objective to deny the owners or legal users of the system to their data or computer. Unleashing a virus through email is one of the most common crimes at the time of targeting computers. An example of this category (computer as a target) is a Denial-of-Service attack or a virus. A virus is referred to destroy your system's data or even a computer system, which is a computer program
2. **The computer as an instrument of the crime:** In this category, a computer is used to accomplish complex financial schemes to defraud or use to gain some information or data, which data is further used for any illegal activity. For case, a computer system can be used by a hacker to steal personal information, which can be used for the criminal objective.
3. **The computer as incidental to a crime:** The computer may be incidental to a crime that means it can only facilitate the crime but may not the primary instrument of it. For example, the trading of child pornography and money laundering.

4. **Crimes associated with the prevalence of computers:** This category comprises of the actions such as software piracy, intellectual property theft, and other crimes against the computer industry.

Examples of computer crimes

In modern times, there are various kinds of computer crime available, which are discussed below:

- **Child pornography:** Child pornography is an example of computer crimes, which is a form of child sexual exploitation.
- **Cracking:** Another example of computer crime is cracking, in which the cracker decodes or breaks the codes that are designed to protect data. A cracker is an individual who uses a script or program to decipher codes or breakdown security systems for illegal activities. The program or script, which is used to break the security, is known as crack.
- **Copyright violation:** If anyone steals another person's copyrighted data, it is also a type of computer crime.
- **Cyber terrorism:** In this category, the attacks come, like blackmailing, hacking, threats towards a person or business to gain unauthorized access to perform illegal activities.
- **Cybersquatting:** Cybersquatting is a term, which is also referred to as domain squatting and typo squatting that is used to set up a domain of another person or company and hold it for resale at a premium price.
- **Cyberbully or Cyberstalking:** Cyberstalking is a kind of attack in which anyone harasses or stalks other persons online by posting inappropriate or unwanted things about them.
- **Creating Malware:** Malware is malicious software that is installed on your computer without your consent as it uses deceptive and unethical tactics. It is designed to watch browsing habits, delete software, or even open someone's computer to attack. For case, sometimes you mistakenly run software on your computer when you are visiting a website and get an unrequested download.
- **Denial of Service attack:** A DoS attack, which stands for denial of service attack, is a kind of computer crime in which an attacker sends an abnormally high number of requests to the victim that is led to the network slow down or fail. These requests cannot be served as normal requests.
- **Doxing:** It is another type of attack when someone shares another person's personal information with anyone without their consent. The personal information may be in the form of someone's full name, address, history, password, and other identifying information.
- **Espionage:** Espionage is the act of spying on a person or business to obtain secret or confidential information. A person who performs these kinds of activities is known as a

spy or espionage agent. Espionage agents can work in company or independent operations to uncover agencies or other secret information.

- **Fraud:** Fraud is the use of computers, internet services, or devices to manipulating data or defraud people or organizations; for example, to participate in credit card fraud or to transfer money to an account, changing banking records. Examples of illegal computer activities include: social engineering, DDoS, viruses, and phishing attacks are used to gain unauthorized access to another fund.
- **Harvesting:** A harvester is a software, also known as a web harvester, that is designed to gather account or account-related information of others, or it is also used to parse large amounts of data. For instance, large numbers of web pages may be processed by a web harvester to take out names, phone numbers, email addresses, account names from the website.
- **Human trafficking:** It is one of the serious crimes, which is an act of participating in buying or selling other humans. Basically, it graves a violation of human rights. There are thousands of men, women, and children who become a victim of traffickers. Approximately all countries in the world become a victim of attackers.
- **Identity theft:** Identity theft is an act to be a person you are not that one. In this category, attackers try to gain information illegally about someone else. Attackers or thieves can try to information such as phone number, credit card numbers, full name, maiden name, social security number, passwords, etc.
- **Illegal sales:** It is an act of purchasing or selling illicit goods online, such as psychotropic substances, drugs, guns, and more.
- **Intellectual property theft:** It is a category of property where a human creates something by using their own mind. In this case, if anyone steals practical or conceptual information that is created by other persons or organizations, it comes under intellectual property theft, which is known as a crime. Trade secrets, copyrights, trademarks, and patents are well-known types of intellectual property.
- **Phishing or vishing:** It is a term that is used to deceive individuals or groups to obtain secret information about that person. For that, they create web pages designed to gather personal information like a credit card, online bank, password, or other private information. They also do so with the help of sending emails.
- **Salami slicing:** Generally, it can be defined as stealing small amounts of money from each transaction that builds into a large sum of illegally gained money.
- **Scam:** A scam is a term that is used to trick people into believing something, which is not actually true. For example, people start a fraud scheme or business through which they gain money from an unsuspecting person. Online scams have increased because the world is more connected to the network. And, it depends on you to keep careful yourself from these kinds of online scams
- **Slander:** A slander is an act of posting libel against another organization or person.

- Software piracy: Generally, it describes illegally copying, distributing, or using software without ownership or legal rights. Today, most of the software may have installed on one computer to use as it is purchased as a single-user license. If you share that software with anyone or copy it on multiple computer devices without purchasing multiple licenses, it is illegal and comes under software piracy.
- **Spamming:** Spam is an e-mail distributed process that is used to promote a specific product or a scam to obtain other people's money by sending unsolicited e-mail to thousands and sometimes millions of people without their consent. It describes junk e-mail on the Internet that is also known as UCE (unsolicited commercial e-mail), mass e-mail marketing, and bulk e-mail.
- **Spoofing:** Generally, the term spoof describes hacking or deception that means to deceive a system by imitating another person, computer, hardware device. You do that bypassing security measures. IP spoofing is one of the well-known spoofing's.
- **Typosquatting:** Cybersquatting is a term used to describe a domain that is a misspelling of another domain. Generally, it is also known as domain squatting and typo squatting that means a company or individual knowingly buys a domain and holds it resale at a premium price.
- **Unauthorized access:** When someone tries to access a system, server, program, and service by using an illegal method or someone else's account information. Basically, unauthorized access means accessing a system on which you have no permission to access. For the case, you have a Gmail account, and someone kept guessing a password or username for your account and accessed this account, which is considered unauthorized access.
- **Wiretapping:** Wiretapping is the surreptitious electronic monitoring device that is used to connect a device to a phone line to listen to conversations.