Network Security & Privacy(Cloud Computing)

What is Cloud computing?

Cloud computing is defined as “a style of computing where massively scalable IT enabled capabilities are delivered ‘as a service’ to external customers using Internet technologies”.

Cloud Computing Models

There are different model of services provided by a Cloud.

Software as a Service (SaaS): Specific online services(application programs) are provided by the Cloud providers e.g. Google Apps, Microsoft office365, Google docs, Gmail, Dropbox.

Infrastructure as a Service (IaaS): hardware resources (such as CPU, storage and communication bandwidth) are provided and managed for the customer by an external provider Examples are virtual servers such as Microsoft Azure, Amazon web services(AWS)

Platform as a Service (PaaS): in addition to infrastructure, a platform to develop an application is provided. PasS makes the development, testing and deployment of applications quick, simple and cost-effective.

Equipment as a Service (EaaS): the ease of connecting all sorts of equipment and devices in the Internet of Things (IoT), EaaS is also becoming more feasible and affordable

6 Facts about the Cloud Computing Industry

1. Companies like Amazon and Microsoft are receiving an ever-growing portion of their **revenues from the cloud**.
2. Security concerns about cloud computing are waning as more and **more IT experts feel confident in trusting the cloud** with sensitive data. A reported 60% feel adequately safeguarded against the potential risks of their databases being hacked.
3. An increased investment in cloud computing will likely be seen across all industries as the cloud helps businesses save money by using staff more efficiently.

6 Facts about the Cloud Computing Industry

4. Almost half of the agencies within the U.S. Government utilize the cloud. In fact, **the government is thought to be the largest user of cloud computing technology.**
5. **Banks are the most active users within the cloud** as a result of mobile banking apps, virtual transaction services like Paypal, and developing currencies like Bitcoin.
6. **For most companies, the cloud is used to store files and as a means for backup and recovery.** Currently the cloud is being utilized for storage more than it is used for things like application deployment. However, this could change as the demand for cloud services grows and enables new business models.

Advantages

1. **Economical:** Reduced Cost. No need of maintaining own systems. Cloud technology is paid incrementally, saving organizations money.
2. **Increased Storage:** Organizations can store more data than on private computer systems.
3. **Flexibility:** Cloud computing offers much more flexibility than past computing methods.
4. **More Mobility:** Employees can access information wherever they are, rather than having to remain at their desks. Scholars can also simulate their experience without caring about infrastructure
5. **Allows IT to Shift Focus:** Companies can rent a huge processing power for a period of time without spending a lot of money buying and maintaining infrastructure hardware such as servers, switches, routers, gateways, etc. They will be free to concentrate on reaching business goals and satisfying customers.

Advantages

6. **Insight :** Many cloud-based storage solutions offer integrated cloud analytics for a bird's-eye view of your data. With your information stored in the cloud, you can easily implement tracking mechanisms and build customized reports to analyze information organization-wide. From those insights, you can increase efficiencies and build action plans to meet organizational goals.

7. **Collaboration:** Cloud computing makes collaboration a simple process. Team members can view and share information easily and securely across a cloud-based platform. Some cloud-based services even provide collaborative social spaces to connect employees across your organization, therefore increasing interest and engagement

Advantages

8. **Quality Control in reporting :** In a cloud-based system, all documents are stored in one place and in a single format. With everyone accessing the same information, you can maintain consistency in data, avoid human error, and have a clear record of any revisions or updates.

9. **Disaster recovery:** Cloud-based services provide quick data recovery for all kinds of emergency scenarios‘ from natural disasters to power outages. This avoids the companies from having downtime in their services which leads to lost productivity, revenue, and brand reputation.

10. **Loss prevention:** With a cloud-based server, however, all the information you've uploaded to the cloud remains safe and easily accessible from any computer with an internet connection, even if the computer you regularly use isn't working.

Advantages

11. **Automatic software updates:** Cloud-based applications automatically refresh and update themselves, instead of forcing an IT department to perform a manual organization-wide update. This saves valuable IT staff time and money spent on outside IT consultation.

12. **Sustainability:** Cloud infrastructures support environmental proactivity, powering virtual services rather than physical products and hardware, and cutting down on paper waste, improving energy efficiency, and (given that it allows employees access from anywhere with an internet connection) reducing commuter-related emissions.

Disadvantages

1. Possible downtime.
2. Sometimes due to internet problem, the downloading and uploading process can be slow which can inhibit the work progress.
3. Security and legal issues.
4. Lack of support in some circumstances.
5. If company bankrupt data is lost.

Issues of Cloud Computing

Data breaches

A data breach might be the primary objective of a targeted attack or simply the result of human error, application vulnerabilities, or poor security practices.

It might involve any kind of information that was not intended for public release, including personal health information, financial information, personally identifiable information, trade secrets, and intellectual property.

The data is either accessed by a hacker or by the Cloud provider itself or a third party— A user may never know who and how his/her data will be abused, which can lead to several ethical challenges.

Hijacking of Accounts

Attackers now have the ability to use your (or your employees') login information to remotely access sensitive data stored on the cloud; additionally, attackers can falsify and manipulate information through hijacked credentials.

If attackers gain access to a user's credentials, they can eavesdrop on activities and transactions, manipulate data, return falsified information and redirect clients to illegitimate sites.

With stolen credentials, attackers can often access critical areas of cloud computing services, allowing them to compromise the confidentiality, integrity, and availability of those services.

Abuse of Cloud Services- Malware Injection

The expansion of cloud-based services has made it possible for both small and enterprise-level organizations to host vast amounts of data easily. However, the cloud's unprecedented storage capacity has also allowed both hackers and authorized users to easily host and spread malware, illegal software, and other digital properties.

Malware injections are scripts or code embedded into cloud services that act as "valid instances" and run as SaaS to cloud servers. This means that malicious code can be injected into cloud services and viewed as part of the software or service that is running within the cloud servers themselves.

Once an injection is executed and the cloud begins operating in tandem with it, attackers can eavesdrop, compromise the integrity of sensitive information, and steal data.

Shared Vulnerabilities

Data can be at risk due to weak protection system at the clients' systems.

Cloud security is a shared responsibility between the provider and the client.

This partnership between client and provider requires the client to take preventative actions to protect their data. While major providers like Box, Dropbox, Microsoft, and Google do have standardized procedures to secure their side, fine grain control is up to you, the client, such as the protection of user passwords, access restrictions to both files and devices, and multi-factor authentication – firmly in your hands.

Data Loss

Data on cloud services can be lost through a malicious attack, natural disaster, or a data wipe by the service provider. An accidental deletion by the cloud service provider, or a physical catastrophe such as a fire or earthquake, can lead to the permanent loss of customer data unless the provider or cloud consumer takes adequate measures to back up data, following best practices in business continuity and disaster recovery.

Losing vital information can be devastating to businesses that don't have a recovery plan. Amazon is an example of an organization that suffered data loss by permanently destroying many of its own customers' data in 2011.

Google was another organization that lost data when its power grid was struck by lightning four times.

Securing your data means carefully reviewing your provider's back up procedures as they relate to physical storage locations, physical access, and physical disasters.

Ethical Issue

Compliance:

A Cloud service should comply with a subset of the standards with respect to the application of the service. In other words, *compliance* covers a set of principles that should be considered during both development and maintenance process of the system.

If the Cloud provider conflicts with the compliance, then it cannot be chosen as a provider by the clients having the compliance requirements.

Ethical Issue

Spiteful Activity:

One of the most unfortunate disadvantages of cloud computing is the potential for spiteful people to do harm, which would be much more difficult to do with a physical server. There may be former employees, disgruntled employees, unhappy contractors, displeased business partners or even industry insiders working for the competition interested in doing harm to your data, network or system.

Ethical Issue

Policies ignoring customers' interest:

Nowadays IT professionals are making some decisions related to cloud computing that could have important results in the future. These professionals have been making decisions about how to manage and store the data. However, they must analyze ethical concepts when making such decisions.

Apply ethical methods of utilitarianism to the cloud computing technology, which would consider it everyone's utility. In other words, IT professionals must be able to develop new policies, standards and designs considering everyone who will utilize cloud computing. Protecting everyone's interests disregarding aspects like if the customer is an ordinary citizen, a big company or the government.

Ethical Issue

Intellectual Property:

Another ethical issue is the easy distribution of other people's intellectual properties due to the easy storage and transfer of media in digital form. Say one person has rightful access to a movie and they upload it onto a cloud network of their choice and others can download it without paying.

Ethical Issue

Discrimination:

In crisis situations, vendors may focus only on the needs of the big accounts that is of people paying more for the support and often end up ignoring the smaller accounts which is sort of discrimination because providers have a responsibility to all their customers – big or small.

Legal Issue

- All the user data is stored in data centres spread along the world. The **user does not know** where his/her information is stored and most times, does not know what kind of information about his/her activity is being recorded and who is managing it.
- If the data is stored in a different country from where the customer lives, they could be under different laws and the local government could apply regulations that the user does not know which would make him/her incompliance with the law. Also, transferring data through the **cloud can cause data** to go into the **jurisdiction** of other countries **where data is not protected**.
- If you process data in one country, store it in another country and send it through some other country, these regulation laws **could conflict and affect international relations** between countries.
- Users can sign agreements with providers specifying which countries they would like data to be stored in, but as clouds are proprietary technologies, it could be hard to keep track of this.

Legal Issue

- The responsibility for data must be clear for the users. Cloud computing providers must offer **insurance for the data** stored into their infrastructure once **they are vulnerable to disasters.**
- The customer needs to be aware if the providers' partners, usually **third-party companies, have access to or use the data.**
- Also, if some company stops using the cloud services, then the problem of who has the **rights over the left-out files** could be a major issue.
- Another aspect is that personals agree to terms and reliability but are **actually not reading** and complying with them**.**
- There is also an impact on sustainability due to the existence of large data centres used to store the data from cloud computing.
- In cases of wanting to store national records, a whole different set of legal rules could be in force.

Social issues

Cloud computing has many benefits, but it is has a cost.

For instance, if more computing resources such as storage, network bandwidth, etc. are needed, they must be purchased. However, sometimes, depending on the resources added by the user, the cost could be very high making it unaffordable.

One of the kind of people who will be disadvantaged with cloud computing would be those who cannot pay for use the service. When using some service on the cloud computing, for instance, a small company could not have the same resources/tools available that the biggest player in the same business has. This might make the small company not able to compete with the biggest one.

Also, **individual users or small companies** might not have the same attention to **solve issues** related to the service from the cloud computer provider that the **biggest ones** have.