What is cloud sourcing

Cloud sourcing is a process by which specialized cloud products and services and their deployment and maintenance are outsourced to and provided by one or more cloud service providers.

Cloud sourcing enables organizations to procure their entire IT infrastructure from a cloud, easily integrates with any platform and requires no management overhead. Cloud sourcing is believed to be the future of cloud computing and business as we see it, where organizations of all sizes are rapidly looking to the cloud to meet their IT needs.

Cloud portability - the ability to move applications and data from one cloud computing environment to another with minimal disruption.

Enables the migration of cloud services from one cloud provider to another or between a public cloud and a private cloud.

Digital resilience – Be prepared so that if there is a digital/cyber-attack, you are prepared to go against that.

Need of Cloud Computing:  
Before using Cloud Computing, most of the large as well as small IT companies used traditional methods i.e., they store data in Server, and they need a separate Server room for that. In that Server Room, there should be a database server, mail server, firewalls, routers, modems, high net speed devices, etc. For that IT companies have to spend lots of money. In order to reduce all the problems with cost Cloud computing came into existence and most companies shift to this technology.

Security Issues in Cloud Computing:   
There is no doubt that Cloud Computing supplies various Advantages but there are also some security issues in cloud computing. Below are some following Security Issues in Cloud Computing as follows.

Data Loss –   
Data Loss is one of the issues faced in Cloud Computing. This is also known as Data Leakage. As we know that our sensitive data is in the hands of Somebody else, and we do not have full control over our database. So, if the security of cloud services is to be broken by hackers, then it may be possible that hackers will get access to our sensitive data or personal files.

Interference of Hackers and Insecure API’s –   
As we know if we are talking about the cloud and its services it means we are talking about the Internet. Also, we know that the easiest way to communicate with Cloud is using API. So, it is important to protect the Interface’s and API’s which are used by an external user. But also in cloud computing, few services are available in the public domain. And is the vulnerable part of Cloud Computing because it may be possible that these services are accessed by some third parties. So, it may be possible that with the help of these services hackers can easily hack or harm our data.

User Account Hijacking –   
Account Hijacking is the most serious security issue in Cloud Computing. If somehow the Account of User or an Organization is hijacked by Hacker. Then the hacker has full authority to perform Unauthorized Activities.

Changing Service Provider –  
Vendor lock in is also an important Security issue in Cloud Computing. Many organizations will face different problems while shifting from one vendor to another. For example, An Organization wants to shift from AWS Cloud to Google Cloud Services then they ace various problem’s like shifting of all data, also both cloud services have different techniques and functions, so they also face problems regarding that. Also, it may be possible that the charges of AWS are different from Google Cloud, etc.

Lack of Skill –   
While working, shifting to another service provider, need an extra feature, how to use a feature, etc. are the main problems caused in IT Company who doesn’t have skilled Employee. So, it requires a skilled person to work with cloud Computing.

Denial of Service (DoS) attack –   
This type of attack occurs when the system receives too much traffic. Mostly DoS attacks occur in large organizations such as the banking sector, government sector, etc. When a DoS attack occurs, data is lost. So, in order to recover data, it requires a great amount of money as well as time to handle it.

**Twitter urges all users to change passwords after glitch**

Twitter told more than 330 millions of its users to change their passwords after a glitch caused some passwords to be stored in readable text on its internal computer system rather than disguised by a process known as ‘hashing’

Botnets - A recent cyber-attack occurred where a botnet type attack targeted a major US defense firm. No physical damage occurred to the firms network, but significant technological secrets about a new surveillance and targeting system from the firm, Defense Applications International (DAI), appear to have been compromised.

DDoS - Amazon Web Services (AWS) reports that in February 2020, they defended against a 2.3 -terabit-per-second (Tbps) distributed denial of service (DDoS) attack!

Malware - Emotet, trojan, 2018

Emotet became known in 2018 after the US Department of Homeland Security deemed it the most threatening and devastating malware. Emotet is a trojan used for financial information theft, such as bank logins and cryptocurrencies.

Emotet propagates itself via malicious emails in the form of spam and phishing emails. Two remarkable Emotet malware attacks are the case of the city of Allentown, Pennsylvania, with damages rising to $1 million, and the case of the Chilean bank Consorcio, with losses worth $2 million.

Social engineering - Toyota Boshoku Corporation, an auto parts supplier, was the victim of a social engineering and BEC (Business Email Compromise) attack in 2019. The money lost amounts to USD 37 million. Using persuasion, attackers persuaded a finance executive to change recipient’s bank account information in a wire transfer.

Insecure API – Experian API

A researcher is claiming that the credit scores of almost every American were exposed through an API tool used by the Experian credit bureau, that he said was left open on a lender site without even basic security protections.

Use of ad hoc - Handling issues on a short-term basis comes with risks, such as the focus on a specific issue, which may ignore other important factors that can impact the overall organization’s effectiveness. Temporary actions taken to address a specific problem may result in an unintended negative impact on other operational functions of an organization.

For example, an ad hoc committee formed to address an unexpected cash flow crisis may recommend terminating or laying off a considerable number of employees. While the move may solve the immediate problem, it may also end up creating larger problems for the company in the future as a result of losing valuable personnel and negatively affecting employee morale among the remaining staff.

Man in the middle attacks - 1. When a victim requests a webpage, the host of the victim makes the request to the host of the attacker’s.

2. The attacker’s host receives the request and fetches the real page from the legitimate website.

3. The attacker can alter the legitimate webpage and apply any transformations to the data they want to make.

4. The attacker sends the requested page to the victim.

Hacking - The Jeep Hack

The IBM security intelligence website reported the Jeep hack a few years ago, saying, “It was just one, but it was enough. In July [2015], a team of researchers was able to take total control of a Jeep SUV using the vehicle’s CAN bus.

By exploiting a firmware update vulnerability, they hijacked the vehicle over the Sprint cellular network and discovered they could make it speed up, slow down, and even veer off the road. Its proof of concept for the emerging Internet of Things (IoT) hacks: While companies often ignore the security of peripheral devices or networks, the consequences can be disastrous.”

We need to develop better security protocols, strategies, and standards if the IoT revolution is to continue to deliver value to people without compromising their security and privacy. But how shall we do this? Industry leaders need to put their heads together.