#

# Subject: Cloud computing

# Assignment No: #1

# Submitted by: Ahmed Tariq (13457)

# Date of Submission: 11/11/2020

# Submitted to: Mam Sana Jehan

# ****Q1: Mention 5 Issues that Are co-related with Cloud Computing .****

# ****1: Hijacking of Accounts****

Many people have extremely weak password security, including password reuse and the use of weak passwords. This problem exacerbates the impact of phishing attacks and data breaches since it enables a single stolen password to be used on multiple different accounts.

Account hijacking is one of the more serious cloud security issues as organizations are increasingly reliant on cloud-based infrastructure and applications for core business functions. An attacker with an employee’s credentials can access sensitive data or functionality, and compromised customer credentials give full control over their online account. Additionally, in the cloud, organizations often lack the ability to identify and respond to these threats as effectively as for on-premises infrastructure.

**2: Cyber attacks**

Cybercrime is a business, and cybercriminals select their targets based upon the expected profitability of their attacks. Cloud-based infrastructure is directly accessible from the public Internet, is often improperly secured, and contains a great deal of sensitive and valuable data. Additionally, the cloud is used by many different companies, meaning that a successful attack can likely be repeated many times with a high probability of success. As a result, organizations’ cloud deployments are a common target of cyber-attacks.

**3: Unauthorized Access**

Unlike an organization’s on-premises infrastructure, their cloud-based deployments are outside the network perimeter and directly accessible from the public Internet. While this is an asset for the accessibility of this infrastructure to employees and customers, it also makes it easier for an attacker to gain unauthorized access to an organization’s cloud-based resources. Improperly-configured security or compromised credentials can enable an attacker to gain direct access, potentially without an organization’s knowledge.

**4: Malware Injection**

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.

**5: Vendor Lock-In**

 Vendor lock-in becomes an issue when an organization considers moving its assets/operations from one CSP to another. The organization discovers the cost/effort/schedule time necessary for the move is much higher than initially considered due to factors such as non-standard data formats, non-standard APIs, and reliance on one CSP's proprietary tools and unique APIs.

**6: Insufficient Due Diligence Increases Cyber security Risk.**

Organizations migrating to the cloud often perform insufficient due diligence. They move data to the cloud without understanding the full scope of doing so, the security measures used by the CSP, and their own responsibility to provide security measures. They make decisions to use cloud services without fully understanding how those services must be secured.