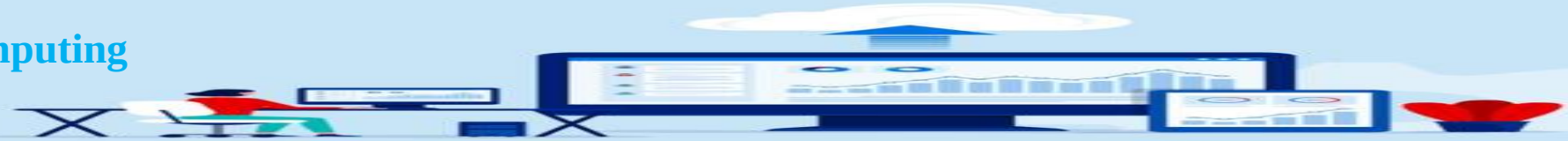
Introduction to Cloud Computing

Dr. Rastgoo

Cloud Computing Attacks



What is Cloud Computing Attack?

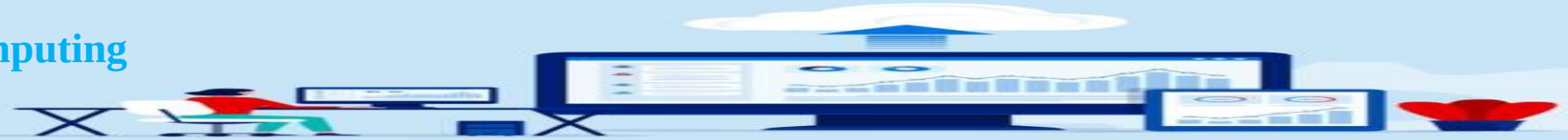
- A cloud attack is a cyber attack that targets cloud-based service platforms, such as computing services, storage services, or hosted applications in a platform as a service (PaaS) or software as a service (SaaS) model.

- Cloud attacks can have serious consequences, such as data breaches, data loss, unauthorized access to sensitive information, and disruption of services.

A data breach is a security violation, in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen, altered or used by an individual unauthorized to do so. Other terms are unintentional information disclosure, data leak, information leakage and data spill.

Data loss is an error condition in information systems in which information is destroyed by failures or neglect in storage, transmission, or processing. Information systems implement backup and disaster recovery equipment and processes to prevent data loss or restore lost data.

Disruption would be a service is temporarily unavailable, or that a system or equipment fails to function in a normal or satisfactory manner.

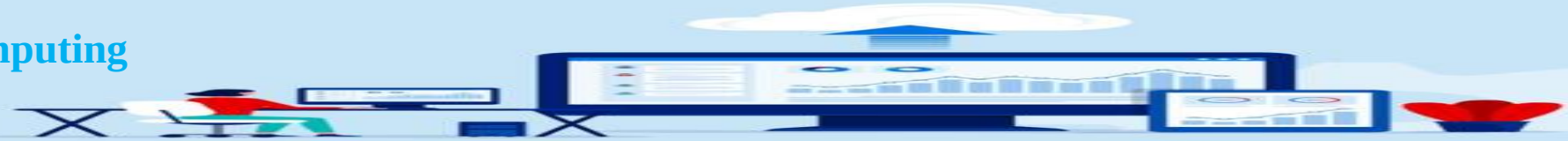


What is Cloud Computing Attack?

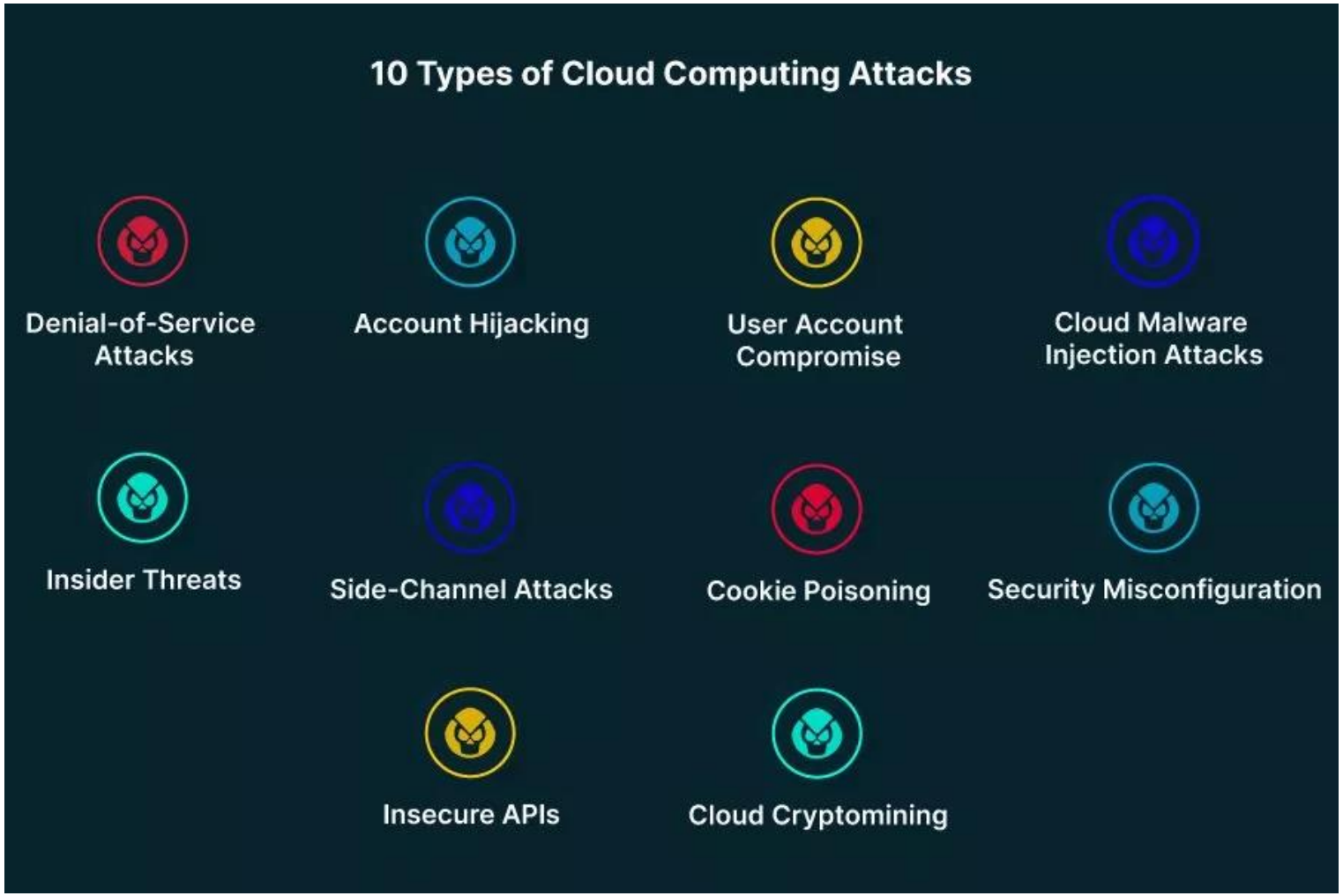
- As more organizations and individuals rely on cloud computing for storing and processing data, there is a corresponding increase in the number of potential targets for attackers.
- Many organizations may not be aware of the risks and vulnerabilities associated with cloud computing, or may not have sufficient measures in place to protect against these threats.
- To protect against these vulnerabilities and risks, it is important for organizations to implement appropriate security measures and to regularly monitor and review the security of their cloud assets.
- This may include implementing access controls, encrypting data, implementing backup and recovery processes, and regularly updating and patching systems and applications.

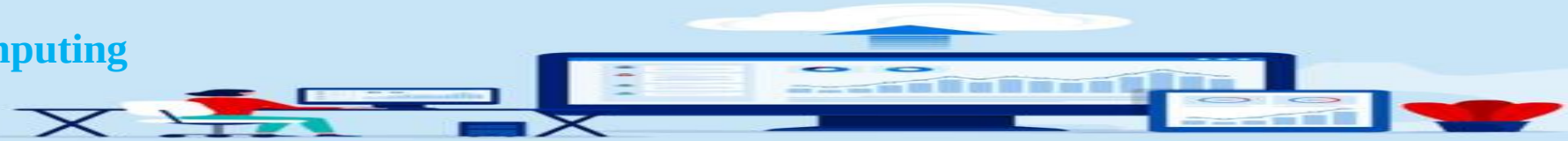
Data encryption is a security method where information is encoded and can only be accessed or decrypted by a user with the correct encryption key. Encrypted data, also known as ciphertext, appears scrambled or unreadable to a person or entity accessing without permission.

Backup and recovery describes the process of creating and storing copies of data that can be used to protect organizations against data loss.



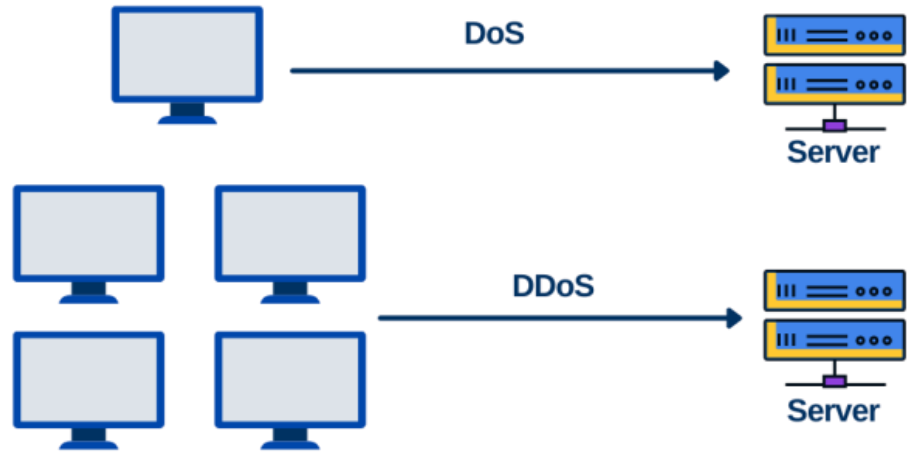
What is Cloud Computing Attack?





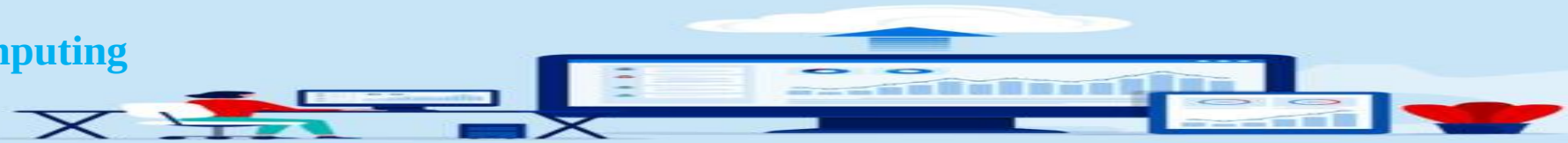
Cloud Computing Attack: Denial-of-Service Attacks (DoS)

- A Denial-of-Service (DoS) attack is a type of cyber attack that aims to make a computer or network resource unavailable to its intended users.
- DoS attacks typically involve flooding a cloud service with a large volume of traffic, which can overwhelm the system and make it unable to process legitimate requests.
- DoS attacks can have serious consequences, including disrupting the availability of critical services, causing financial losses, and damaging an organization's reputation.
- Cloud-based DoS attacks can be particularly challenging to defend against, as the scale and complexity of cloud environments can make it difficult to identify and mitigate the attack.



Cloud Computing Attack: Account Hijacking

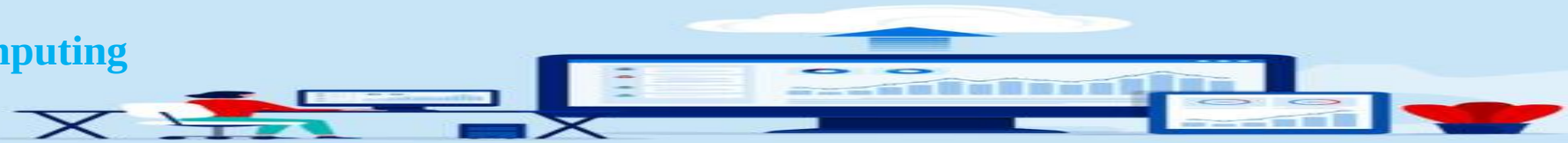
- Account hijacking in the cloud refers to the unauthorized access or control of a cloud computing account by an attacker.
- This can allow the attacker to use the associated resources for their own purposes, or to steal or manipulate data stored in the cloud.
- For example, attackers can use password cracking techniques to guess or steal login credentials and gain access to a cloud account.
- Account hijacking can lead to financial losses and damage to an organization's reputation.



Cloud Computing Attack: User Account Compromise

- User account compromise typically involves an attacker gaining access to an account through the actions of the account owner, such as by tricking the user into revealing their login credentials or by exploiting a vulnerability in a system or application used by the user.

- This differs from account hijacking, which involves an attacker gaining unauthorized access to an account through means such as password cracking or exploiting vulnerabilities in the cloud infrastructure.

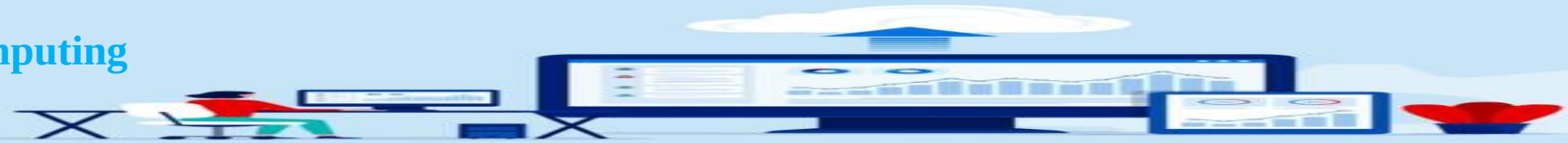


Cloud Computing Attack: Cloud Malware Injection Attacks

- Cloud malware injection attacks are a type of cyber attack that involves injecting malicious software, such as viruses or ransomware, into cloud computing resources or infrastructure.

- This can allow the attacker to compromise the affected resources and steal or destroy data, or to use the resources for their own purposes.

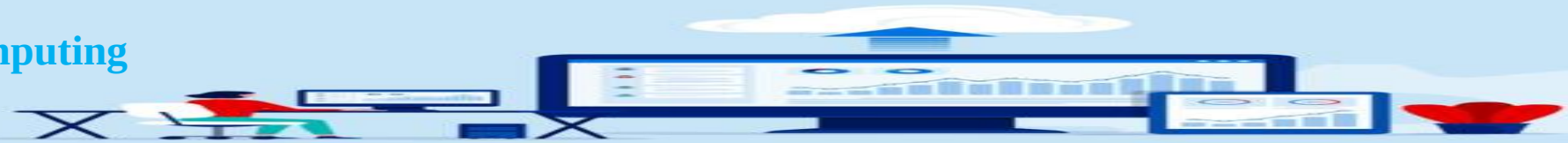
Ransomware is a type of cryptovirological malware that permanently block access to the victim's personal data unless a ransom is paid. While some simple ransomware may lock the system without damaging any files, more advanced malware uses a technique called cryptoviral extortion.



Cloud Computing Attack: Cloud Malware Injection Attacks

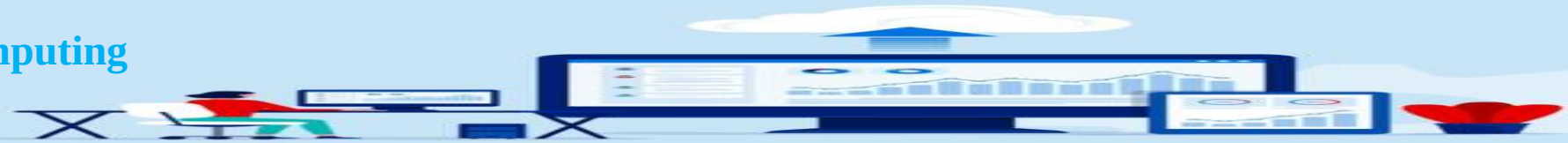
- There are several ways in which attackers can inject malware into cloud resources, including:

- Exploiting vulnerabilities in the cloud infrastructure or in the systems and applications running on the cloud.
- Adding a malicious service module to a SaaS or PaaS system, or an infected VM to an IaaS system, and diverting user traffic to it.
- Using phishing attacks to trick users into downloading and installing malicious software.
- Gaining unauthorized access to cloud accounts and injecting malware through the use of malware-infected files or links.



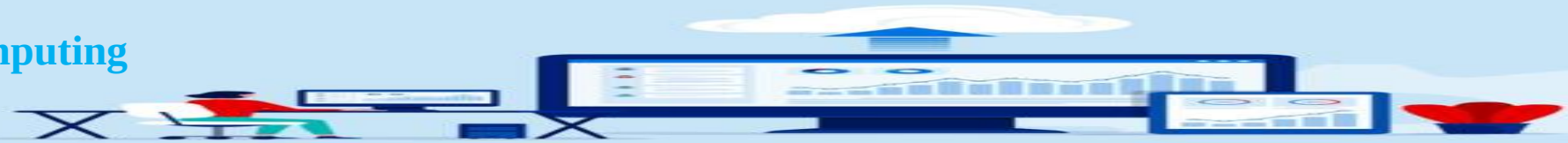
Cloud Computing Attack: Insider Threats

- Insider threats in a cloud environment refer to the risk of unauthorized access or misuse of cloud computing resources by individuals within an organization, such as employees or contractors.
- These individuals may have legitimate access to the cloud assets, but may misuse or abuse that access for their own purposes, or may accidentally expose the assets to risk through their actions.
- Insider threats can be particularly challenging to detect and prevent because they often involve individuals who are authorized to access the cloud assets and who may not be acting maliciously.
- They can also be difficult to mitigate because they often involve a high level of trust and access within the organization.



Cloud Computing Attack: Side-Channel Attacks

- A side-channel attack involves exploiting information that is leaked through the physical implementation of a system, rather than through its logical interfaces.
- This information can include details about how the system is implemented or about the data being processed by the system.
- In a cloud environment, attackers can perform side-channel attacks by placing a malicious virtual machine on a legitimate physical host used by the cloud customer. This gives the attacker access to all confidential information on the victim machine.
- Side-channel attacks can be used to extract sensitive information from a system, such as passwords, encryption keys, or other sensitive data. They can also be used to disrupt the operation of a system or to manipulate its behavior.

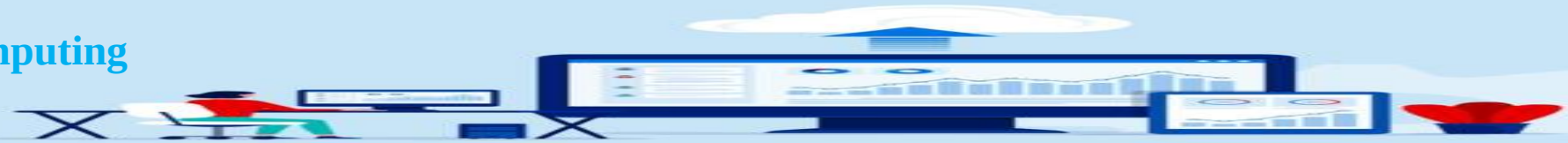


Cloud Computing Attack: Cookie Poisoning

- Cookie poisoning in cloud applications refers to the unauthorized modification or injection of malicious content into a cookie, which is a small piece of data that is stored on a user's computer by a website or web application.

- Cookies are used to store information about a user's preferences and browsing history, and are often used to personalize the user's experience or to track their activity.

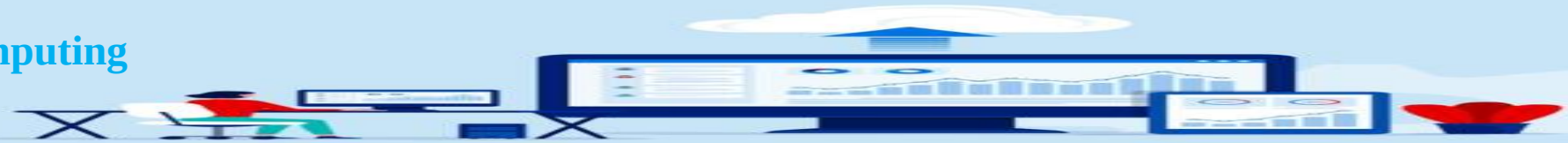
- In SaaS and other cloud applications, cookies often contain credential data, so attackers can poison cookies to access the applications.



Cloud Computing Attack: Security Misconfiguration

- Security misconfiguration refers to the failure to properly configure cloud computing resources and infrastructure to protect against cyber threats.

- This can include failure to properly set access controls, failure to properly configure and secure systems and applications, and failure to regularly update and patch systems and applications.



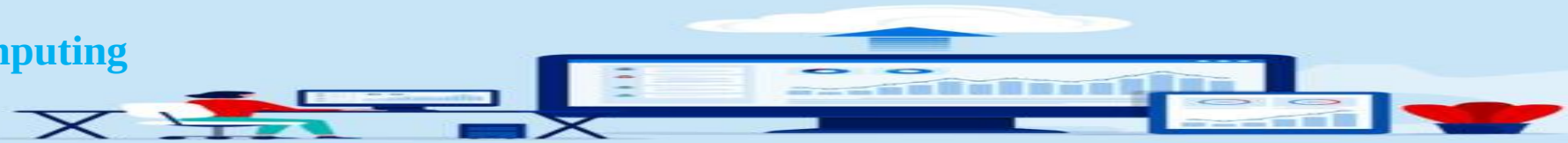
Cloud Computing Attack: Insecure APIs

- Insecure APIs have vulnerabilities that can be exploited by attackers to gain unauthorized access to systems or data, or to disrupt the operation of the API.

- Examples include:

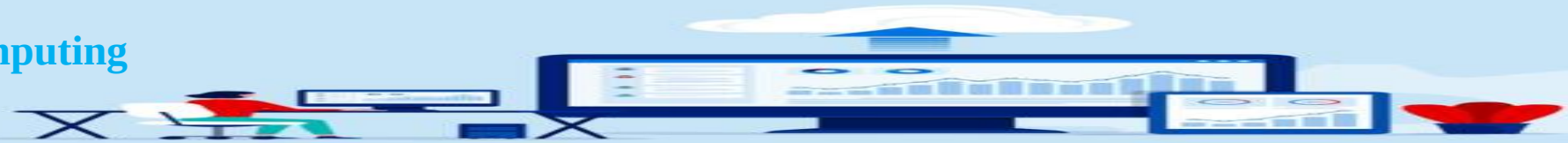
  - ✓ Shadow APIs: APIs that are not properly documented or authorized, and may not be known to the organization that owns the API. These APIs can be created by developers or other users within the organization, and can expose sensitive data or functionality to unauthorized parties.

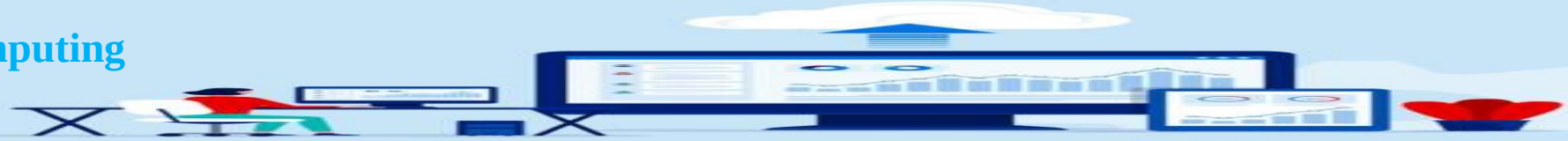
  - ✓ API parameters: The inputs and outputs of an API, which can be vulnerable to injection attacks if they are not properly validated and sanitized.



Cloud Computing Attack: Cloud Cryptomining

- A cloud cryptomining attack is a type of cyber attack in which attackers use cloud computing resources to perform cryptomining without the knowledge or consent of the cloud provider or the owner of the resources.
- Cryptomining is the process of using computing resources to solve complex mathematical problems in order to verify and validate transactions on a blockchain network.
- In a cloud cryptomining attack, the attackers use stolen or compromised credentials to access and exploit cloud computing resources, such as virtual machines or containers, for the purpose of performing cryptomining.
- They may also use malware or other techniques to gain unauthorized access to cloud resources.





Cloud Computing