Cloud-Based Attacks

&

Data Theft Attacks

Presented by :

Boumezbeur Aya

Dib Maria

What is cloud computing?

- **cloud computing :** is the on-demand delivery of IT resources over the Internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centers and servers, you can access technology services, such as computing power, storage, and databases, on an as-needed basis from a cloud provider like Amazon , Google , Microsoft.

Cloud computing is a big shift from the traditional way businesses think about Information Technology resources , So the top benefits of cloud computing are :

Cost savings :

- This is because cloud computing eliminates the capital expense of buying hardware and software.
- the racks of servers, the round-the-clock electricity for power and cooling.
- the IT experts for managing the infrastructure.

Security :

- Set of policies and procedures helping protect your data, apps, and infrastructure from potential threats.

Deploy globally in minutes:

- you can expand to new geographic regions and deploy globally in minutes.

- so you can deploy your application in multiple physical locations with just a few clicks.

Elasticity :

- that means you can scale these resources up or down to instantly grow and shrink capacity as your business needs change.

Types of cloud service :

1

Software as a Service (SaaS)

SaaS provides a full application stack as a service that customers can access and use. SaaS solutions often come as ready-to-use applications, which are managed and maintained by the cloud service provider.

2

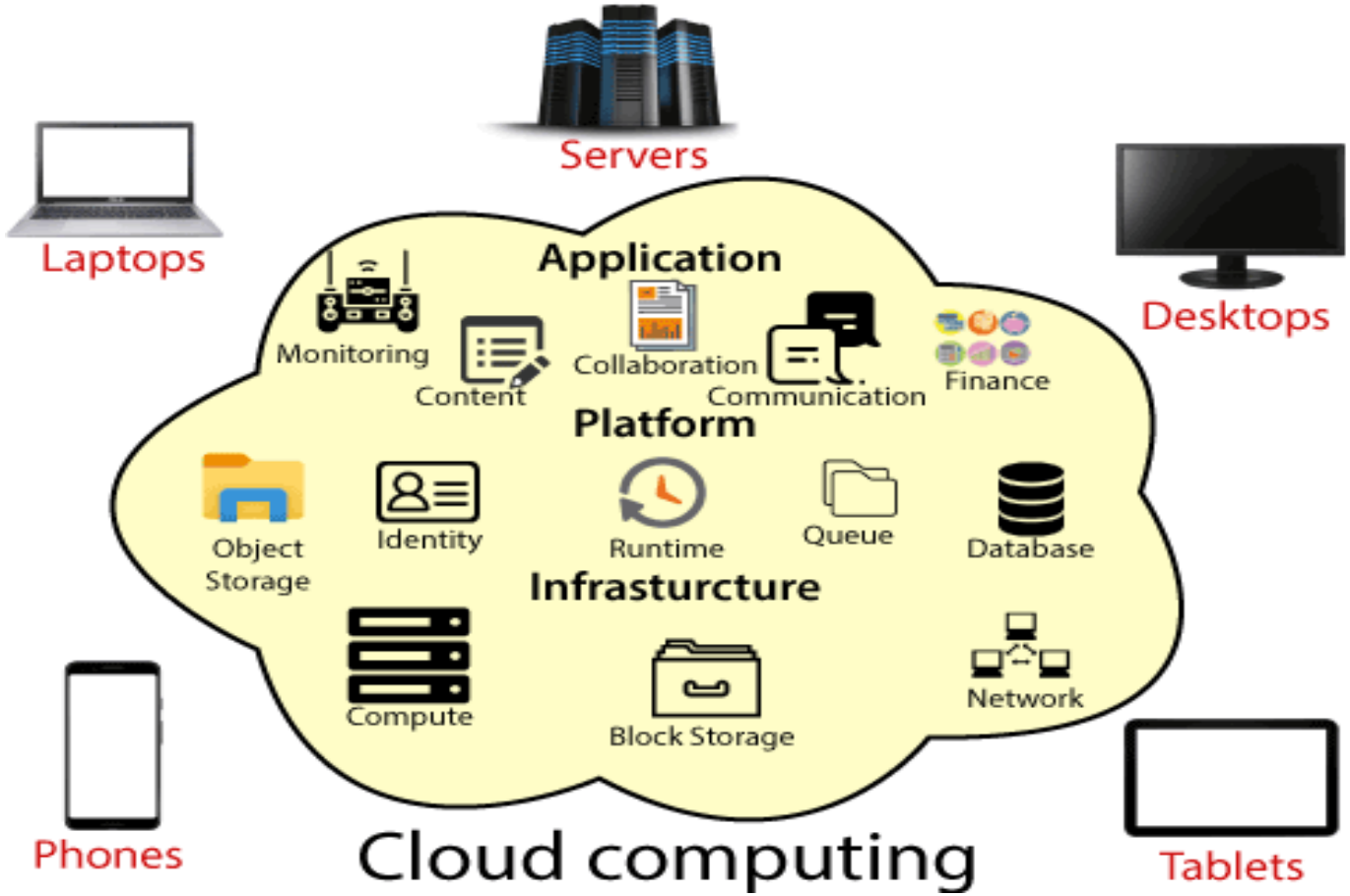
Platform as a Service (PaaS)

PaaS delivers and manages hardware and software resources for developing, testing, delivering, and managing cloud applications. Providers typically offer middleware, development tools, and cloud databases within their PaaS offerings.

3

Infrastructure as a Service (IaaS)

IaaS delivers on-demand infrastructure resources, such as compute, storage, networking, and virtualization. With IaaS, the service provider owns and operates the infrastructure, but customers will need to purchase and manage software, such as operating systems, middleware, data, and applications.


Servers
Laptops
Desktops
Application
Monitoring
Content
Collaboration
Communication
Finance
Platform
Object Storage
Identity
Runtime
Queue
Database
Infrasturcture
Compute
Block Storage
Network
Phones
Tablets
Cloud computing

Cloud-Based Attacks

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.

8 Types of Cloud Computing Attacks

Denial-of-Service Attacks

Account Hijacking

User Account Compromise

Cloud Malware Injection Attacks

Insider Threats

Cloud Cryptomining

Cookie Poisoning

Security Misconfiguration

1. Distributed Denial of Service (DDoS)

Overwhelming a cloud service with traffic to make it unavailable to legitimate users.

2. Account Hijacking

For example, attackers can use phishing attacks or password cracking techniques such as brute force attacks or dictionary attacks to guess or steal login credentials and gain access to a cloud account.

3. User Account Compromise

Weak password protocols are a leading cause of compromised user accounts. Many users who work with cloud services do not have strong password protection, as they either use weak passwords, reuse older passwords or don't change their passwords regularly.

4. Cloud Malware Injection Attacks

Introducing malicious software such as viruses or ransomware into cloud environments to compromise data or disrupt services, Using phishing attacks.

5. Insider Threats

Malicious activities carried out by individuals within an organization such as employees or contractors who have authorized access to cloud resources.

6. Cookie Poisoning

an attacker, by poisoning cookies with malicious content, can exploit vulnerabilities in the cloud application's security and gain unauthorized access to user accounts or sensitive data.

7. Security Misconfiguration

Organisations have to configure these deployments according to their requirements to ensure more robust cybersecurity.

8. Cloud Cryptomining

when someone uses someone else's cloud computing resources from a cloud service (like Amazon Web Services, Microsoft Azure, or Google Cloud) without their permission to mine cryptocurrency like Bitcoin,leading to unexpected costs for the victim.

Cloud Security Testing

What is Cloud Security Testing?

- Cloud Security Testing is a special type of security testing method in which cloud infrastructure is tested for security risks and loopholes that hackers can exploit.

- Cloud security testing, or cloud security assessment, is the process of evaluating the security of cloud-based services, applications, and infrastructure to identify and mitigate vulnerabilities and threats. It is essential for maintaining the confidentiality, integrity, and availability of data and services in the cloud.

Why is Cloud Security Testing important?

Cloud security testing is one of the most important things you need to ensure your cloud infrastructure is safe from hackers. As the cloud computing market is growing rapidly, there is a growing need for application security solutions for the cloud to ensure that businesses are protected from cyber-attacks.

3 Different Approaches to perform Cloud Security Testing

Cloud security testing is performed in three different approaches:

- **Black Box:** No external information about the cloud infrastructure
- **Gray Box**: Limited information about the cloud infrastructure
- **White Box:** Complete information about the cloud infrastructure

What are the advantages of Cloud Testing Security?

Compliance

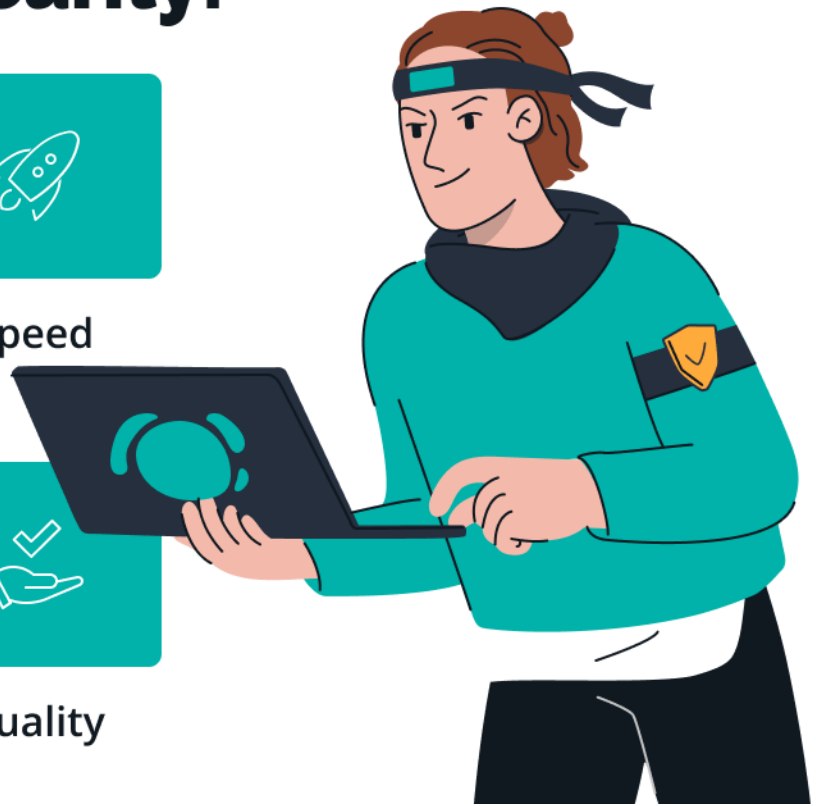
Financial Resilience

Speed

Scalability

Minimizing Risks

Quality



Methods for Cloud Security testing

1. Vulnerability Assessment

Checking for Weaknesses , use special tools to look for any "holes" or weaknesses in the way your cloud system is set up.

2. Penetration Testing

Testing Like a Hacker, pretend to be a friendly hacker and try to break into your own cloud system.

3. Configuration Review

Looking at Settings , check the settings of your cloud services to make sure they are set up in the safest way.

4. Identity and Access Management (IAM) Assessment

Checking Who Can Access, make sure only the right people have access to your cloud stuff. This means checking who has keys to your "digital house.“

5. Data Encryption and Privacy

Protecting Information , make sure your important information is hidden and protected, like putting it in a secret code.

6 . Incident Response Testing

Practice for Problems , pretend bad things are happening (like someone trying to break in) and see how well your system can handle and stop these problems.

7. API Security Testing

Checking How Things Talk to Each Other, look at how different parts of your cloud system and application communicate and interact with each other.

8. Continuous Monitoring

Making Sure Everyone Follows the Rules ,check if your cloud system follows the rules and laws about keeping information safe and private.

9. Compliance Audits

Watching for Problems All the Time, use special tools that keep an eye on your cloud system all the time, looking for any signs that something might be wrong.

10. Training and Awareness

Teaching Everyone to Be Safe ,teach everyone who uses the cloud system how to be safe and not do things that might cause problems.

Do Cloud Services Providers allow cloud security testing?

The cloud services providers, such as Amazon Web Services, Google Cloud Platform, and Microsoft Azure, allow their customers to perform testing, but with some limitations. Above all, these services have their own cloud security providers their security teams that perform testing using various methods.

Case studies

Facebook

In April 2021, Facebook reported a vulnerability affecting hundreds of millions of user records, which were exposed on servers hosted by Amazon Web Services (AWS). Facebook said the problem was identified and quickly fixed.
The incident was sparked by the disclosure of records by two third-party developers employed by Facebook. The exposed databases contained personal information that could be used for social engineering and targeted phishing attacks.

Microsoft—2019

On January 22, 2020, Microsoft announced that one of their cloud databases was breached back in December 2019, resulting in the exposure of 250 million entries, including email addresses, IP addresses, and support case details.
According to the computing giant, the cause of this data breach was a misconfigured network server that was hosting the critical information. While this is not the biggest, it was one of the most shocking cyber attacks due to the high-profile nature of the target.

Prevention and Protection

1. Encrypt All Data in the Cloud : There are typically three stages at which data needs to be encrypted:

- 1. At-rest encryption
- 2. In-transit encryption
- 3. In-use encryption

2. Use Strong Authentication:

Implement multi-factor authentication (MFA) to add an extra layer of security for user accounts.

Regularly review and update access controls and permissions to ensure that users have the minimum necessary privileges.:

3. Employee Education

4. Security Tools : like

1. Cloud Security Posture Management (CSPM) Tools:

CSPM tools are specifically designed to assess and manage the security posture of cloud environments. They can identify misconfigurations in cloud services such as storage, compute, and networking. Examples include Palo Alto Networks Prisma Cloud, AWS Config, and Microsoft Azure Security Center.

2. Vulnerability Scanning Tools:

Examples include Nessus, OpenVAS, and Qualys

3.Network Security Tools:

Network security tools focus on monitoring and securing the network infrastructure, helping to identify and prevent unauthorized access or unusual network patterns. Examples include intrusion detection systems (IDS and IPS) like Snort.

3. Penetration Testing Tools:

Penetration testing tools simulate attacks on your infrastructure to identify weaknesses and potential exploits. Examples include Metasploit, OWASP Amass, and Nmap.

4. Compliance Monitoring Tools:

Compliance monitoring tools help ensure that your cloud infrastructure adheres to regulatory requirements and industry standards. Examples include CloudCheckr and Dome9.

What is Data theft ?

- **Data theft :** theft is the act of stealing digital information stored on computers, servers, or electronic devices to obtain confidential information or compromise privacy.

- The data stolen can be anything from bank account information, online passwords, passport numbers, driver's license numbers, social security numbers, medical records, online subscriptions, and so on. Once an unauthorized person has access to personal or financial information, they can delete, alter, or prevent access to it without the owner’s permission

Type of Data theft

- A **data leak** occurs when sensitive data is accidentally exposed, either on the internet or through lost hard drives or devices. This enables cybercriminals to gain unauthorized access to sensitive data without effort on their part.

- A **data breach** is a calculated assault on digital fortifications, where malicious actors intentionally infiltrate systems, exploiting vulnerabilities to gain illicit entry. Both acts, whether accidental or deliberate, compromise the sanctity of data security, posing significant threats to the confidentiality and privacy of the exposed information.

How does data theft happen?

- **1.** Social engineering
- **2.** Weak passwords
- **3.** System vulnerabilities
- **4.** Insider threats
- **5.** Human error
- **6.** Compromised downloads
- **7.** Physical actions
- **8.** Database or server problems
- **9.** Publicly available information

Targets of data thefts

Any information stored by an individual or organization could be a potential target for data thieves. For example:

1. Customer records
2. Financial Data such as credit card or debit card information
3. Source codes and algorithms
4. Proprietary process descriptions and operating methodologies
5. Network credentials such as usernames and passwords

HR records and employee data

6. Private documents stored on computer computers

Impact of data theft :

1. **Reputational damage -** Brands with a history of becoming data theft victims will have a bad reputation and find it difficult to attract new customers.

2. **Regulatory fines -** Depending on your industry, you can face steep fines from regulatory bodies such as HIPAA and GDPR for failing to meet their security mandates.

3. **Ransomware demands -** Attackers sometimes use ransomware to hold their victim's information and demand a hefty fee to give back the data. Even so, paying the ransom to get back the data isn't a guaranteed solution.

Impact of data theft :

4 **Lawsuits -** Organizations that mishandle their data or have poor security practices can be subject to legal action from the affected customers.

5 **High recovery costs -** Patching systems and recovering data following a data breach can be expensive.

6 **Downtime -** An organization may be unable to use an existing system following a data breach until it is corrected. The downtime can negatively impact employee productivity, consequently hurting an organization's bottom line.

7 **Loss of customers -** When your business becomes a data theft victim, the chances are that existing customers will leave because they don't feel safe.

How to keep data safe and secure

- 1.Use secure passwords
- 2.Multi-factor authentication
- 3.Limit social media sharing
- 4.Keep systems and programs up to date

- 5.Avoid using the same password for multiple accounts
- 6.Be cautious when sharing personal information
- 7.Close unused accounts
- 8.Monitor your accounts
- 9.Be wary of free Wi-Fi

Case studies

Equifax

In 2017, Equifax became a victim of data theft. In this attack, the personal data of 143 million customers was compromised. What's more, approximately 209,000 people had their credit card data exposed.

Yahoo

In September 2016, Yahoo revealed that 500 million users had been compromised in a 2014 breach. Yahoo claimed that the data theft came about due to an unauthorized party forging cookies to gain access to user accounts without needing a password.