Name: Keegan Vaz **SEC:** TE CMPN B **Roll No.:** 28 **PID:** 192120

Experiment 7

Aim

Study and Implement of Security as a Service (SECaaS)

Theory

1. What are different security issues in cloud computing.

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

   1. 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 don't have full control over our database. So if the security of cloud service is to be breached by hackers then it may be possible that hackers will get access to our sensitive data or personal files.

   2. 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. An 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.

   3. 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.

   4. 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 face various problems 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.

5. Lack of Skill – While working, shifting to another service provider, needing an extra feature, how to use a feature, etc. are the main problems caused in IT companies who don't have skilled employees. So it requires a skilled person to work with cloud Computing.

6. 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.

2. Explain Server and Data Security is cloud computing.
   Ans: A cloud server is a computer server that has been virtualized, making its resources accessible to users remotely over a network. Cloud servers are intended to provide the same functions, support the same operating systems (OSes) and applications, and offer similar performance characteristics as traditional physical servers that run in a local data center. Cloud servers are often referred to as virtual servers, virtual private servers or virtual platforms.
   Types of cloud servers:
   1. Public cloud servers. The most common expression of a cloud server is a virtual machine (VM) or compute "instance" -- that a public cloud provider hosts on its own infrastructure and delivers to users across the internet using a web-based interface or console. This model is known as IaaS.
   2. Private cloud servers. A cloud server may also be a computer instance within an on-premises private cloud. In this case, an enterprise delivers the cloud server to internal users across a local area network (LAN) and, in some cases, also to external users across the internet. The primary difference between a hosted public cloud server and a private cloud server is that the latter exists within an organization's own infrastructure, whereas a public cloud server is owned and operated outside of the organization. Hybrid clouds may include public or private cloud servers.
   3. Dedicated cloud servers. In addition to virtual cloud servers, cloud providers can supply physical cloud servers, also known as bare-metal servers, which essentially dedicate a cloud provider's physical server to a user. These dedicated cloud servers -- also

called dedicated instances -- are typically used when an organization must deploy a custom virtualization layer or mitigate the performance and security concerns that often accompany a multi-tenant cloud server.

Data Security:

As there is a higher emphasis on ensuring everything is safe and secure, and that there is no risk of data hacking or breaches, still as the Cloud is often shared between a lot of users, security becomes an immediate and primary concern for Cloud owners. If you are online you are at risk of data breaching or hacking, that is an undeniable fact. CSPs have a wide variety of security tools and policies in place but problems may still incur, usually originating in human error. The possible potential challenges include data breaches, data hacking, Cryptojacking, data loss, DDoS, and Insider threats.

3. Explain various Threat detection, Data protection and Infrastructure protection services in AWS.

   Ans: **Threat Detection -** Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.

   Data Protection - AWS earns the trust by working closely with you to understand your data protection needs, and by offering the most comprehensive set of services, tooling, and expertise to help you protect your data. To do this, we provide technical, operational, and contractual measures needed to protect your data. With AWS, we are able to manage the privacy controls of your data, control how your data is used, who has access to it, and how it is encrypted.

   Infrastructure protection - Infrastructure protection encompasses control methodologies, such as defense in depth, that are necessary to meet best practices and organizational or regulatory obligations. Use of these methodologies is critical for successful, ongoing operations in the cloud. It is a key part of an information security program. It ensures that systems and services within your workload are protected against unintended and unauthorized access, and potential vulnerabilities. For example, you'll define trust boundaries (for example, network and account boundaries), system security configuration and maintenance (for example, hardening, minimization and patching), operating system authentication and authorizations (for example, users, keys, and access levels), and other appropriate policy-enforcement points (for example, web application firewalls and/or API gateways).

Activity

- How is SSL Certificate provided in cloud computing?

  Ans: SSL Security for Cloud Computing has proven to be of great help in several aspects. It is considered as the best security protocol for Cloud users. As we know, an SSL certificate is used to create a safe channel between a web browser and web server for avoiding any type of data tampering in between. Even in the case of cloud computing, an SSL certificate effectively secures data stored or shared by establishing an encrypted session.

  Data Monitoring: If an SSL certificate is used to encrypt the stored data by Cloud providers, they can assure the customers that their data is closely monitored, even during the transmission. Also, trusted certificate issuing authorities will avoid issuing an SSL certificate to the servers located in banned countries like Iran, North Korea, etc.

  Regulatory Compliance: Any enterprise intending to secure data on the cloud is required to comply with certain rules and regulations that are set by the government and trusted industry authorities like Sarbanes-Oxley (SOX) Act, Payment Card Industry Security Standard (PCI-DSS), Health Insurance Portability & Accountability Act (HIPAA). And before outsourcing and trusting cloud providers with all sensitive data, enterprises must also ensure that the providers seek some compliance with industry standards. Here, SSL encryption helps in avoiding any type of disclosure of private data to third parties trying to intercept or steal it.

  Ensure Data Segregation & Encrypted Access: In Cloud Computing, the storage location of all data coming from users across the world, and the respective server location remains unknown to the users. It is controlled by cloud providers. And the shared environment in cloud storage may not guarantee the segregation of that data and the subsequent multi-tenancy. However, using an SSL certificate can easily secure the data on the cloud.

  The cloud provider needs to ensure this by providing:

  - **Encryption:** Cloud-users should ensure they are being provided the industry-standard levels of encryption, the minimum session encryption strength of 128-bit or the preferable 256-bit encryption.
  - **Authentication:** There should be an authentication of the server's ownership before the data is transferred. It is advisable to rely on certificates issued by trusted third party CAs as in that case, the servers are already authenticated by them.

- **Certificate Validity:** An SSL certificate comes with certain validity periods. In case of an unlikely event where the certificate is compromised a fail-safe check needs to be there to make sure the certificate has not been revoked since its issuance. At present, Online Certificates Status Protocol (OCSP) and Certificate Revocation List (CRL) are the two standards popularly used to check the certificate validity.

Securing Back-Up Repositories: Almost all users store their data on the cloud with an intention to retrieve it later when needed. However, if there occurs an unlikely event of the cloud experiencing a total crash for some unforeseen reason, then providers should be able to recover users' data from their backup repositories. An SSL certificate assures the legitimacy of the duplicate servers that are used to retrieve the backup and also provides an encrypted channel for its transfer.

An SSL certificate is chosen by many providers for establishing cloud security. Cloud users should also be vigilant while selecting a cloud provider based on the security they furnish. Along with other attributes like space being provided, users should also consider security aspects that are opted by the providers. To avoid security breaches or data loss, cloud providers should use SSL certificates that are issued after undergoing rigorous vetting procedures conducted by trusted authorities and offer encryption strength of 128- to 256-bit for exceptional security.

- What is key pair in AWS

  Ans: Key Pair in AWS -

  a. A key pair is a combination of a public key that is used to encrypt data and a private key that is used to decrypt data.

  b. Key-pairs are secure login information for your instances/virtual machines.

  c. To connect to the instances we use key-pairs that contain a public-key and private-key.

Conclusion

Why cloud computing security is important.

Ans: Importance of security in Cloud Computing –

Fast: Use cloud service provider native accelerators that enable security capabilities and controls to be deployed in minutes or hours, rather than months.

Frictionless: Embed security into existing solutions, business processes and operational teams.

Scalable: Apply automation and self-healing processes to reduce manual steps and break the resourcing model of adding headcount to enable organizations to scale.

Proactive: Establish pre-emptive controls to block accidental or malicious security incidents from happening in the first place.

Cost effective: Bake-in security from the outset to avoid the additional costs incurred by having to re-do work.