|  |  |
| --- | --- |
| Course | Information Security |
| Assignment | Assignment 3-Cloud Security |
| Student ID | 100899259 |
| Student Name | Maisha Khatoon |

# Write a summary of the key concepts and principles of the AWS shared Responsibility Model.

The security responsibilities of AWS and its clients are defined by the model of split responsibility used by AWS. According to this paradigm, AWS is responsible for the security of the cloud infrastructure, which includes the real security of server farms, systems management, storing, and hypervisor. Customers are responsible for the safety of their data, working frameworks, and applications.

The following are the main ideas of the AWS shared responsibility model:

* Cloud security: Amazon is responsible for the equipment, software, and system administration that make up the cloud architecture.
* Customers are responsible for the security of their data, applications, and working frameworks that are hosted in the cloud.
* Shared responsibility: When it comes to protecting client data and applications, AWS and clients share security responsibilities.

The AWS shared responsibility model's guiding principles are as follows:

* Responsibility of AWS: AWS oversees protecting the infrastructure that powers all of the services offered by the AWS Cloud. This includes acquiring the hardware, software, systems management, and offices needed to run AWS Cloud services.
* Client Responsibilities: Customers are responsible for ensuring the security of their data, applications, and operational frameworks while they are using the AWS Cloud.
* Shared Responsibility: Security and consistency of uses, information, and frameworks are shared responsibilities between clients and AWS. The use of the AWS administration affects the separation of responsibilities.

# Review two AWS services.

## AWS EC2

### What is AWS EC2?

A web service offered by Amazon Web Services (AWS) called Amazon Elastic Compute Cloud (EC2) offers flexible computation capacity in the cloud. It enables users to launch, manage, and customize virtual machines (also known as occurrences) that can run a variety of operating systems, including Linux and Windows, as needed.

AWS EC2 offers a wide range of event kinds that are optimized for different types of tasks, such as compute-upgraded, memory-improved, capacity-streamlined, and GPU scenarios. Clients can choose a case type based on the requirements of their application and pay only for the amount of the limit that they really utilize.

Moreover, EC2 offers additional components and tools for managing and automating the sending and scaling of events, including Auto Scaling, Elastic Burden Adjustment, and AWS CloudFormation. Moreover, EC2 can work in conjunction with other AWS services like Amazon Elastic Block Storage (EBS), Amazon Simple Capacity Administration (S3), and Amazon Virtual Confidential Cloud (VPC) to provide a comprehensive cloud computing setup.

In general, AWS EC2 is a flexible, reliable, and useful cloud computing administration that enables users to efficiently organize and scale compute resources in the cloud.

### Customer Security Responsibility

Customers are responsible for the security of their services, data, and functioning frameworks that are hosted on Amazon Elastic Compute Cloud under the AWS shared responsibility model (EC2). It is possible to classify the client security obligations for EC2 into three categories:

* Setting up the EC2 instances: Customers are responsible for setting up the operating system and software on their EC2 instances. This includes setting up firewalls and access controls, managing client information and consents, and introducing and maintaining working framework upgrades and fixes.
* Information security: Customers are responsible for protecting the data sets, log files, and other application information they store on EC2 occasions. This includes encrypting information that is in motion or that is very still, monitoring access restrictions, and taking reinforcing and disaster recovery procedures.
* Consistency and administration: Customers are responsible for ensuring that their services and information running on EC2 instances comply with administrative requirements and industry standards. This includes implementing security controls, keeping an eye out for security incidents to detect and address them, and managing routine security assessments and reviews.

Customers who use AWS EC2 generally need to adopt a comprehensive approach to security management, including implementing security best practices, monitoring their frameworks for security events, and continuously improving their security posture to reduce risks and protect their applications and data.

### AWS’s Security Expectation

AWS (Amazon Web Services) offers a concept of shared responsibility for security that outlines the responsibilities of AWS and its clients with regard to security. According to this paradigm, customers are responsible for the security of their applications, data, and working frameworks that are operating on AWS administrations, such as Amazon Elastic Compute Cloud, while AWS is responsible for the security of the fundamental framework and administrations (EC2).

For example, AWS has implemented a variety of security mechanisms to ensure the security of the EC2 platform. These are as follows:

* Physical security: Access is tightly restricted and AWS server farms are purchased.
* Network security: Amazon offers several levels of organizational security, including firewalls, security groups, and records for organization access control.
* Host security: AWS obtains the EC2 instances by disconnecting them from various occurrences and approving firmware for safe booting.
* Information security: AWS offers a variety of encryption options for information that is still and moving, including SSL/TLS encryption for network traffic, Amazon EBS encryption, and Amazon S3 encryption.
* Consistency: Amazon ensures compliance with several industry standards and regulations, including PCI DSS, HIPAA, and SOC 2.

## AWS S3

### What is AWS S3?

A fully supervised object storage service is provided by Amazon Web Services under the name Amazon Simple Storage Service (S3) (AWS). It provides a highly adaptable, secure, and robust storage system that can store and restore any volume of data from anywhere on the internet.

In cans, which are containers for objects stored in S3, users can store and retrieve information objects like records, photos, recordings, and archives. Clients have control over access restrictions and the arrangements made for the items stored in containers. They can also create, edit, and delete containers.

S3 provides various features and tools for managing information, such as

* Forming: S3 may keep different iterations of an article, allowing users to track changes and, if necessary, recover earlier iterations.
* Lifecycle arrangements: Due to S3's ability to change objects' storage classes based on their entrance designs, storage costs are reduced.
* Encryption: S3 offers SSL/TLS encryption for information in transit as well as server-side and client-side encryption for information that is quite still.
* Fine-grained access controls are provided for objects by S3, such as container techniques, access control entries (upper leg tendons), and Identity and Access The executives (IAM) schemes.
* Combination: To create a comprehensive cloud-based information processing and research setup, S3 can be used with other AWS services like Amazon CloudFront, AWS Lambda, and AWS Paste.

AWS S3 is an incredibly flexible and reliable storage service that gives users a resourceful and adaptable storage base for their information storage needs.

### Customer Security Responsibility

Customers are responsible for the security of the data they store on Amazon Simple Storage Service under the AWS shared responsibility model (S3). Three categories can be used to comprehensively classify the customer security responsibilities for S3:

* Information security: Clients are responsible for protecting their records, photos, and archives that are stored in S3. This includes implementing encryption for information both at rest and in transit, managing access restrictions, and taking backups and disaster recovery precautions.
* Clients are responsible for enforcing access controls on their S3 containers and items. In addition to managing Personality and Access The board (IAM) strategies to manage client access, this includes establishing can arrangements and access control records (upper leg tendons).
* Consistency and administration: Clients are responsible for ensuring that the information they store in S3 complies with administrative requirements and industry standards. This involves implementing security controls, keeping an eye out for and responding to security-related events, and managing routine security assessments and reviews.

### AWS’s Security Expectation

The Amazon Simple Storage Service (S3) is a fully supervised service with a few built-in security features and tools to protect user data. Customers are responsible for getting their data stored in S3, while AWS is responsible for the security of the basic infrastructure and the S3 service itself. Some of the security requirements for AWS S3 include:

* Encryption: S3 offers SSL/TLS encryption for information in transit as well as server-side and client-side encryption for information that is quite still. Moreover, Amazon provides AWS Key Administration Service (KMS), a supervised service that streamlines the creation and management of the encryption keys required to scramble data.
* S3 provides several options for gaining access to controls, including pail techniques, access control records (upper leg tendons), and Character and Access the Executives (IAM) ways. These restrictions allow customers to monitor who accesses the S3 pails and items they own.
* Logging and watching: S3 offers detailed access logs that users can use to track client behaviour and spot unauthorized access attempts. Moreover, AWS provides Amazon CloudWatch, a monitoring and logging service that provides continuous visibility into resource utilization and system health.
* Consistency: Amazon warrants that S3 complies with several industry standards and regulations, including HIPAA, PCI DSS, and GDPR. Customers can use AWS's consistency reports, such as SOC 1, SOC 2, and ISO 27001, to demonstrate their compliance with these standards.
* Recovery from failure: S3 is designed to provide great sturdiness and accessibility, with several copies of each content stored across different accessible zones. Customers can also create reinforcement and disaster recovery plans using Amazon features like cross-locale replication and lifecycle arrangements.

# Description for the following cloud security acronyms

## CSPM

Cloud Security Posture Management is referred to as CSPM. It relates to several tools and processes that help organizations maintain a secure and consistent posture in their cloud environments. CSPM arrangements provide automated security audits and consistency evaluations for all cloud assets, including the infrastructure, software, and data.

The main goal of CSPM is to identify security flaws and vulnerabilities in cloud environments and provide useful information to fix them. In order to continuously check cloud conditions and identify security vulnerabilities, CSPM arrangements routinely coordinate with the APIs of cloud suppliers.

## CWPP

Cloud Workload Protection Platform is referred to as CWPP. It alludes to a number of security tools and processes, such as virtual machines, compartments, and serverless capabilities, that protect workloads operating under cloud settings.

CWPP configurations provide automated threat location and response capabilities, as well as perceivability and control over workloads in multi-cloud environments. CWPP setups frequently operate with the APIs of cloud providers and employ AI calculations to continuously evaluate workloads and gradually detect security risks.

## CNAPP

CNAPP stands for Cloud Native Application Protection Platform. An arrangement of security known as a Cloud Native Application Protection Platform (CNAPP) was created specifically to protect cloud-native applications. Applications that are built using cloud-native innovations like holders, microservices, and serverless calculating are referred to as cloud-native apps since they are designed to function on cloud infrastructure.

The goal of CNAPPs is to provide security throughout the whole application lifecycle, from development through deployment and beyond. In order to continuously detect and address security risks and weaknesses, they use a combination of automated and manual cycles.

## CIEM

Cloud Infrastructure Entitlement Management is referred to as CIEM. It relates to a number of tools and processes that support organizations in managing access and consents to cloud resources.

The use of CIEM configurations enables automated verification and analysis of rights across cloud environments, including client and administrative accounts, jobs, gatherings, and consents. The primary goal of CIEM is to identify and address security risks associated with entitlements, such as excessive or unsightly authorizations that could result in data breaches or consistency violations.

## CASB

The Cloud Access Security Broker abbreviation is CASB. It makes reference to a security arrangement that helps organizations spread their security policies and procedures to the cloud.

CASB configurations provide visibility and control over cloud apps and data, enabling organizations to monitor and control cloud use and approve security measures. Addressing security risks associated with cloud reception, such as information loss, consistency infringement, and unauthorized access, is the primary goal of CASB.