Terna Engineering College

Computer Engineering Department
Program: Sem VI

Course: Cloud Computing Lab(CSL605)

PART A
(PART A: TO BE REFFERED BY STUDENTS)

Experiment No.7

A.1 Aim:
To study Security as a Service on AWS

A.2 Prerequisite:
Knowledge of Access Control, Authentication and Authorization

A.3 Objective:
To understand the Security practices available in public cloud platforms and to study various Threat detection, Data protection and Infrastructure protection services in AWS.

A.4 Outcome: (LO 4)
After successful completion of this experiment student will be able to understand the Security practices available in public cloud platforms.

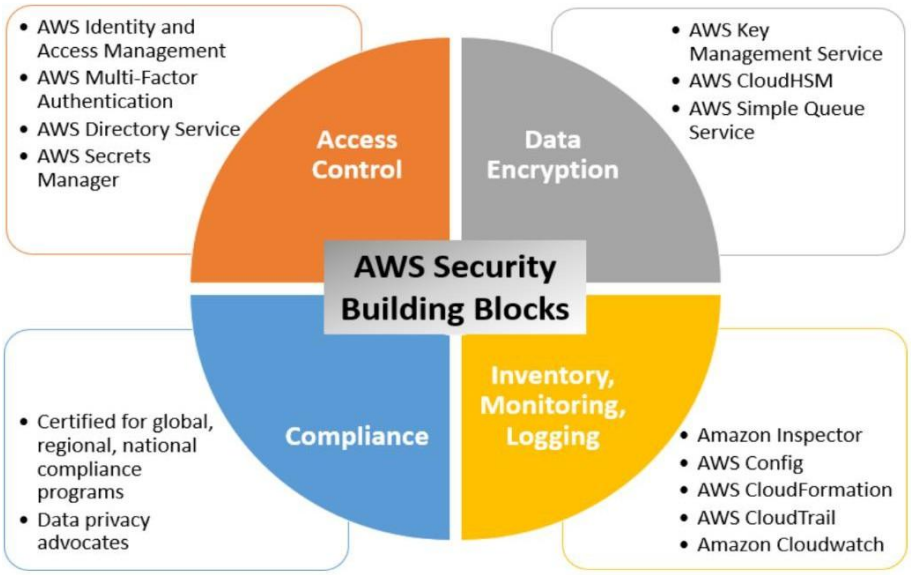
A.5 Theory:

Amazon Web Services (AWS) enables organizations to build and scale applications quickly and securely. However, continuously adding new tools and services introduces new security challenges. According to reports, 70 percent of enterprise IT leaders are concerned about how secure they are in the cloud and 61 percent of small- to medium-sized businesses (SMBs) believe their cloud data is at risk.

AWS provides many different security tools to help customers keep their AWS accounts and applications secure.

What are the benefits of Security Services?

1. **Keeps Data Safe**: Infrastructure incorporates strong safeguards to help protect privacy. All data is processed in highly protected data centres.
2. **Meets Compliance Requirements**: Manages dozens of compliance programs in its infrastructure. Organizations meet compliance effortlessly
3. **Saves Operational Cost**: Operational cost reduces as organizations don't have to maintain on-premise facilities.
4. **Scales Quickly**: Security scales with the organization's usage of Amazon Web Services Cloud. The architecture is built to keep data secure, no matter the size of the enterprise.



AWS provides a number of security tools and services to help make your life easier when it comes to securing your cloud.

Data protection: AWS recognizes the importance of securing data and making sure it is not lost in transfer. Their services help you meet core security, confidentiality, and compliance requirements. Features include things encryption, data duplication and data monitoring. An example of a data protection service provided by AWS is Amazon Macie.

Identity & Access Management: AWS recognizes the need for managing Identities so they provide an extensive list of tools and services to help you manage identity in the cloud. Overall, the goal is to control the resources and actions identities can use and manipulate.

Infrastructure Protection: Infrastructure protection is a critical component of information security and helps ensure that everything within your workload is safe from vulnerability exploitation or unintended access. While infrastructure is largely managed by AWS itself, they also provide some additional resources for managing the security of configurable infrastructure, e.g. AWS WAF.

Threat Detection: When in the cloud, you need constant reassurance that your security posture is strong and you have all the right configurations in place to optimize security. AWS provides services that increase visibility into your deployment and operations and also monitor identity behavior to help detect threats. An example is Amazon GuardDuty.

PART B

(PART B: TO BE COMPLETED BY STUDENTS)

(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the ERP or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no ERP access available)

Roll No.B30	Name: Pranjal Bhatt
Class :TE B COMPS	Batch :B2
Date of Experiment:	Date of Submission:
Grade :	

B.1 Question of Curiosity:

Q.1. What are AWS security monitoring and logging evaluation tools? Explain each.

Ans: Amazon CloudWatch: A monitoring and observability service that provides data and actionable insights for AWS resources, applications, and services. CloudWatch collects and tracks metrics, monitors log files, sets alarms, and responds automatically to changes in system performance or resource utilization.

AWS CloudTrail: A service that records API calls and activity within an AWS account, enabling users to track user activity, resource changes, and troubleshoot operational issues. CloudTrail logs provide visibility into actions taken by users, applications, or AWS services, aiding in compliance auditing, security analysis, and incident response.

Amazon GuardDuty: A managed threat detection service that continuously monitors AWS accounts and workloads for malicious activity and unauthorized behavior. GuardDuty analyzes VPC flow logs, CloudTrail event logs, and DNS logs to identify potential security threats such as compromised instances, unauthorized access attempts, or suspicious network activity.

AWS Config: A service that assesses, audits, and evaluates the configuration of AWS resources, providing a detailed inventory of resource configurations and changes over time. AWS Config helps users maintain compliance, track resource relationships, and identify configuration drift, enabling proactive security measures and ensuring adherence to security best practices.

Amazon Inspector: An automated security assessment service that helps users identify security vulnerabilities and compliance issues within AWS deployments. Inspector performs automated security assessments against predefined rulesets and best practices, providing detailed findings and recommendations to improve security posture and reduce risk.

Q.2 Explain cloud security.

Ans:
Cloud security refers to the set of policies, technologies, and controls deployed to protect data, applications, and infrastructure associated with cloud computing. In AWS, cloud security includes:

- Data encryption at rest and in transit
- Identity and Access Management (IAM)
- Threat detection
- Network security
- Compliance monitoring Cloud security ensures confidentiality, integrity, and availability of cloud-based systems and data.

Q.3 What are AWS Security use cases?

Ans: Identity and Access Management (IAM): Controlling user access to AWS services and resources.

Network Security: Securing network traffic and controlling access to VPCs, subnets, and instances using security groups and NACLs.

Data Encryption: Encrypting data at rest and in transit using AWS Key Management Service (KMS) and SSL/TLS.

Security Monitoring and Logging: Monitoring AWS resources, detecting security threats, and logging activity using services like CloudWatch, CloudTrail, and GuardDuty.

Incident Response and Forensics: Investigating security incidents, conducting forensics, and responding to security breaches.

Compliance and Governance: Ensuring compliance with regulatory requirements and implementing governance policies using AWS Config, AWS Organizations, and AWS Audit Manager.

Application Security: Implementing security best practices for application development and deployment on AWS, such as secure coding practices and container security.

Infrastructure Security: Hardening AWS infrastructure, securing APIs, and managing secrets using services like AWS WAF, AWS Shield, and AWS Secrets Manager.

B.3 Conclusion:

Hence, we understood Security as a Service (SECaaS) on AWS provides a comprehensive suite of tools and features to protect data, applications, and infrastructure in the cloud. Leveraging AWS's advanced security capabilities, organizations can implement proactive measures such as identity and access management, threat detection, and encryption, ensuring robust protection against cyber threats while maintaining scalability and flexibility.