Strathmore
UNIVERSITY

SCHOOL OF COMPUTING AND ENGINEERING SCIENCES (SCES)

BACHELOR OF SCIENCE IN COMPUTER NETWORKS AND CYBER SECURITY

END OF SEMESTER EXAMINATION – MARKING GUIDE

CNS 4105: CLOUD COMPUTING AND SECURITY

DATE: 25th **July 2024** Time: **15:30-17:30 Hours**

Instructions

1. This examination consists of **FIVE** questions.
2. Answer **Question ONE (COMPULSORY)** and any other **TWO** questions.

Question One [30 Marks]
SECTION A:

Read the Attached Case on XYZ Corp then answer the questions that follow

a) How did XYZ Corp. address the challenge of managing user access across multiple cloud platforms? **[2 Marks]**

b) What strategies did XYZ Corp. employ to enhance its compliance with industry-specific regulations while migrating critical workloads to the cloud? **[4 Marks]**

c) Discuss the benefits of continuous monitoring and real-time threat detection in XYZ Corp.'s cloud security strategy. **[2 Marks]**

d) What role does encryption play in XYZ Corp.'s cloud security strategy, and how does it contribute to data protection? **[4 Marks]**

e) AWS has provided XYZ Corp with a Service Level Agreement (SLA) for the provisioned IT resources. As a cloud practitioner advise XYZ Corp on any **FOUR** issues the SLA should address. **[8 Marks]**

SECTION B

a) What is one method that a company could use to ensure high availability during a security attack? **(Select ONE)** **[1 Mark]**

i. Access Control
ii. Resource Monitoring
iii. Automatic Scaling
iv. Regular Audits
v. All of the above

b) In the AWS shared responsibility model, AWS is responsible for providing what **(Select the best answer)** **[1 Mark]**

i. Security of the cloud
ii. Security to the cloud
iii. Security for the cloud
iv. Security in the cloud

c) Which statement about AWS Identity and Access Management (IAM) is true? **(Select ONE)**

[1 Mark]

i. IAM provides enhanced security by prohibiting federation from corporate systems such as Microsoft Active Directory
ii. With IAM, you can grant principals granular access to the console
iii. IAM provide auditing of who performed an action, what action they performed, and when they performed it
iv. IAM provides encryption for data at rest and data in transit

d) Which statements are true for a Virtual private cloud (VPC)? **(Select Three)** **[3 Marks]**

i. Uses network access control lists (ACLs) as the only layer of security
ii. Belongs to multiple AWS regions and only one Availability Zone
iii. Gives you control over your virtual networking resources including selecting the IP address range, creating subnets, and configuring route tables and network gateways
iv. Provides the ability to customize your network including creating a public subnet for your webservers that can access the public internet
v. Acts as firewall to control traffic in and out of one or more subnets
vi. Is a logically isolated section of the AWS cloud where you can launch AWS resources in a virtual network

e) Which AWS service can be used to generate encryption keys that are protected by FIPS 140-2 validated hardware security modules (HSMs)? **(Select ONE)** **[1 Mark]**

i. AWS Secrets Manager
ii. AWS Key Management Service (AWS KMS)
iii. AWS Certificate Manager (ACM)
iv. AWS Certificate Manager Private Certificate Authority

f) A web application uses a fleet of Amazon EC2 instances for both dynamic and static assets. The EC2 instances are in a private subnet, behind a load balancer that is in a public subnet inside the VPC. Which service logs would provide the MOST insight into how users are using the web application? **(Select ONE)** **[1 Mark]**

i. AWS Trusted Advisor logs
ii. Amazon VPC flow logs
iii. Amazon S3 access logs
iv. Elastic Load Balancing (ELB) access logs

g) An Administrator wants to improve their vulnerability management. They would like to use a service that continuously scans Amazon EC2 instances for software vulnerabilities and unintended network exposure. Which AWS service would meet their need? **(Select ONE)** **[1 Mark]**

i. Amazon Macie
ii. AWS shield
iii. Amazon Inspector
iv. Amazon Detective

h) An Administrator wants to implement a level of protection against distributed denial of service (DDoS) attacks. Which AWS service would meet their need? **(Select ONE)** **[1 Mark]**

i. Amazon Detective
ii. Amazon Inspector
iii. AWS shield
iv. AWS Firewall Manager

Question Two [15 Marks]

A European Sports Television network is reconciling its usage accounts for cloud and On-premises. The following is a monthly summary of both the up-front and ongoing costs

Cost	Amount
Hardware Purchase	Kes. 11,000
Salary	Kes. 45,500
S3 bucket provisioning	Kes. 4,000
EC2 instance provisioning	Kes. 10,000
LAN Network set-up	Kes. 9,170
VPC	Kes. 7,300
Software Patch	Kes. 5,200
Hardware Maintenance	Kes. 1,200
Cloud Subscription Fee	Kes. 3,692
Cloud Architect fee	Kes. 80,000
Perpetual Software Licenses	Kes. 30,000

a) Classify the costs as being on-going or up-fronts costs in either cloud environment or on-premises environment. **[5 Marks]**

b) Compute the Total Cost of Ownership over a three-year period and advise on what approach you would have the firm to take. **[10 Marks]**

Question Three [15 Marks]

Health-e-MedRecord (HEMR) is a patient-centered, cloud-based healthcare platform that enables all stakeholders – patients, physicians, first responders, and facilities – to deliver the best possible health care. HEMR offers a suite of applications that address major workflows and integrations between various provider teams and administrators. After receiving a Well Architected Review, Health-e-MedRecord decided to move forward with making many important changes to its cloud infrastructure. The company wants to utilize cloud services to help address security vulnerabilities, achieve cost optimization, and implement cloud best practices.

a) HEMR experienced the threat described below, identify it and explain how it is launched**.**

[4 Marks]

Description

There were Suspicious amounts of traffic originating from a single IP address or IP range. There was also a flood of traffic from users who share a single behavioral profile, such as device type, geolocation, or web browser version as well as an unexplained surge in requests to a single page or endpoint. Lastly, there were odd traffic patterns such as spikes at odd hours of the day or patterns that appear to be unnatural (e.g. a spike every 10 minutes)

b) Explain the four fundamental components of cloud data transmission they should consider when reviewing the architecture from a security standpoint. **[6 Marks]**

c) Beyond the Well Architecture Review, identify five recommendations to make HEMR's cloud infrastructure more secure and scalable. **[5 Marks]**

Question Four [15 Marks]

a) An efficient and bespoke load-balancing algorithm should include different metrics that are relevant to the application it supports. Consider the design of the interactive three-tier web application load-balancing algorithm in Figure 1. Discuss the following areas of improvement in relation to the load-balancing algorithm and architecture. **[12 Marks]**

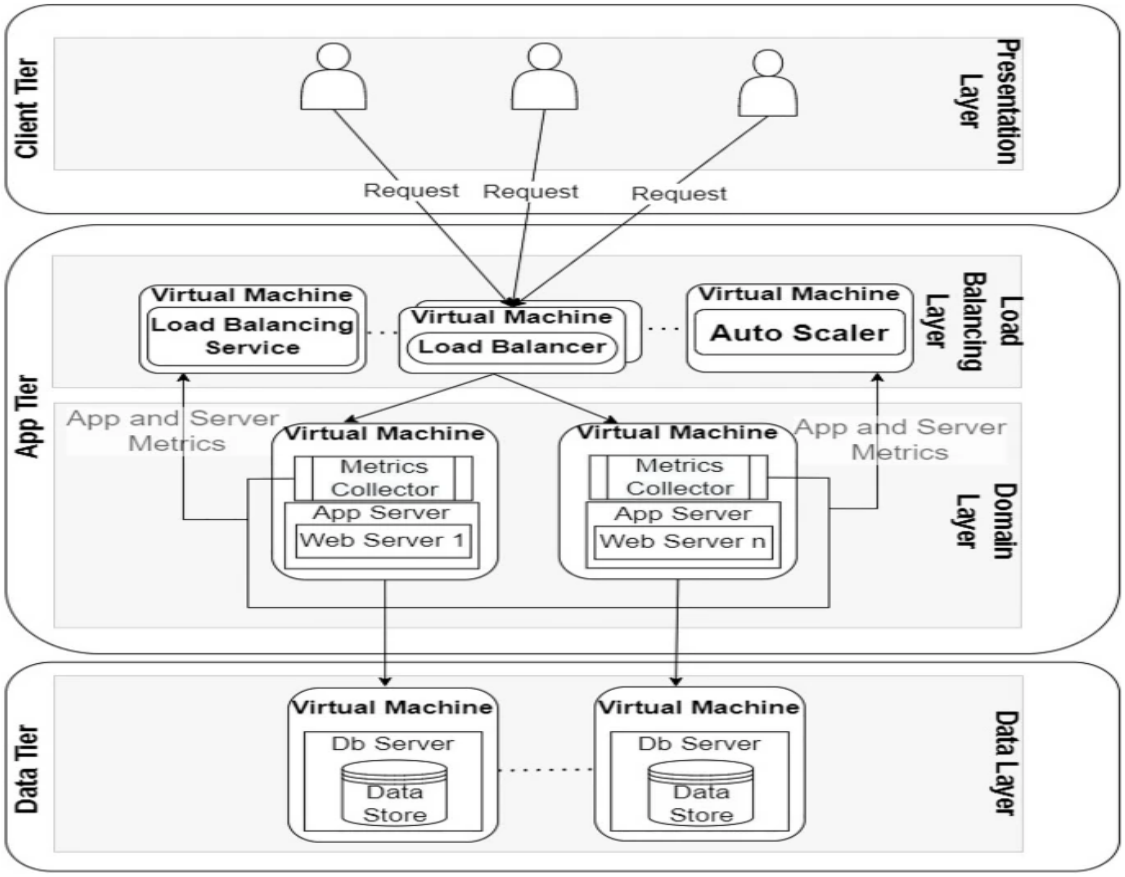

Figure 1: Load Balancing Layered Architecture

a. Scalability
b. Fault Tolerance
c. Reduced Overhead and Latency
d. Server Metrics

b) Provide common examples of the cloud deployment models – Platform as a Service, Software as a Service, and Infrastructure as a Service. **[3 Marks]**

Question Five (15 marks)

a) Consider the AWS Identity and Access Management (IAM) deployment in Figure 3. Explain any four IAM role characteristics. **[8 Marks]**

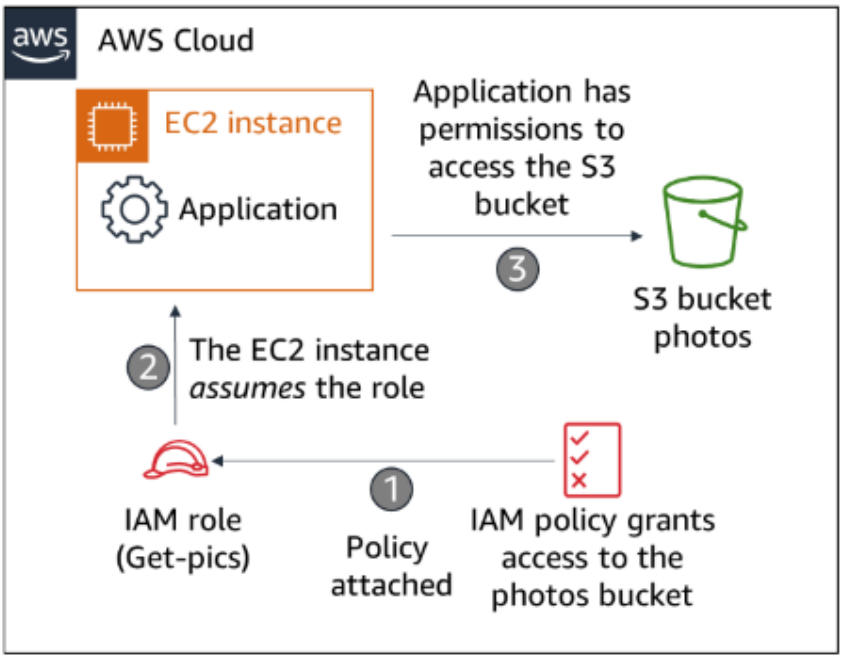

Figure 2: IAM Deployment

b) Figure 4 below illustrates the Cloud server-side encryption. Explain the three types of S3 server-side encryption offered by Amazon Web Services. **[7 Marks]**

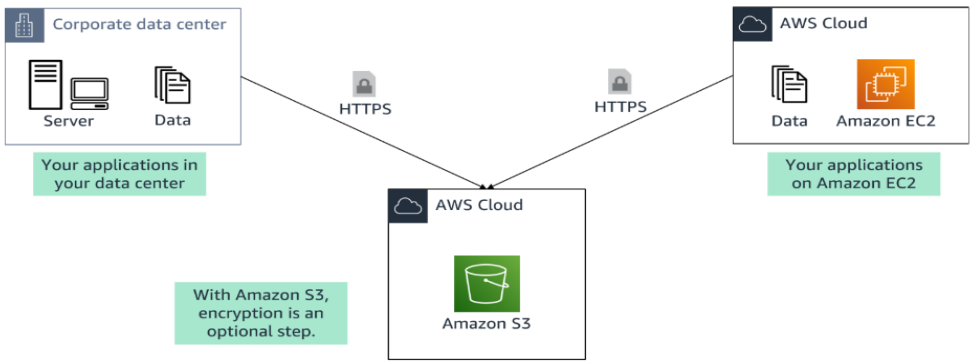

Figure 3: Server-Side Encryption

Case Study: Enhancing Cloud Security, XYZ Corp

Introduction:

In an era where digital transformation is omnipresent, cloud computing has emerged as a fundamental enabler for organizations seeking scalability, flexibility, and cost-efficiency. However, alongside its benefits, cloud adoption brings inherent security challenges. This case study delves into the journey of XYZ Corp., a multinational enterprise, in fortifying its cloud security posture.

Background:

XYZ Corp. operates in a highly regulated industry, necessitating stringent data protection measures. As the company migrated its critical workloads to the cloud, concerns regarding data integrity, confidentiality, and compliance surfaced. Recognizing the imperative to bolster its security framework, XYZ Corp. embarked on a comprehensive cloud security initiative.

Challenges Faced:

1. Data Protection: Safeguarding sensitive information across multiple cloud environments while ensuring compliance with diverse regulatory standards.
2. Access Management: Managing user access across decentralized cloud platforms without compromising agility or security.
3. Threat Detection: Detecting and mitigating evolving cyber threats in real-time to preempt potential breaches.
4. Compliance: Demonstrating adherence to industry-specific regulations and standards to mitigate legal and reputational risks.

Strategies Implemented:

1. Multi-layered Encryption: Implemented end-to-end encryption mechanisms to protect data at rest, in transit, and during processing, leveraging industry-standard encryption algorithms.
2. Identity and Access Management (IAM): Deployed centralized IAM solutions to govern user access, enforce least privilege principles, and enable seamless authentication across cloud environments.
3. Continuous Monitoring: Leveraged AI-driven threat detection and monitoring tools to proactively identify anomalies, unauthorized access attempts, and suspicious activities.
4. Compliance Automation: Automated compliance checks and audits using cloud-native tools to ensure adherence to regulatory requirements, thereby streamlining compliance efforts.

Outcomes and Benefits:

1. Enhanced Security Posture: Strengthened resilience against cyber threats through robust encryption, access controls, and proactive threat detection mechanisms.
2. Improved Compliance: Achieved and maintained compliance with industry-specific regulations and standards, bolstering trust among stakeholders and mitigating legal risks.

3. Operational Efficiency: Streamlined security operations and compliance workflows through automation, freeing up resources for innovation and strategic initiatives.

4. Scalability and Flexibility: Built a scalable security architecture capable of adapting to evolving business needs and dynamic cloud environments.

Conclusion:

By prioritizing cloud security as a strategic imperative, XYZ Corp. transformed its security posture from a potential liability into a competitive advantage. Through a holistic approach encompassing encryption, access management, threat detection, and compliance automation, the organization fortified its defenses, enabling secure and compliant cloud adoption. As the digital landscape continues to evolve, XYZ Corp. stands poised to navigate future challenges with confidence, leveraging its resilient cloud security foundation.